"To do it over again, I would have made the argument that training be mandatory for all users," she testified. "I can't mandate training, but it's the one thing, if I could do over, I would do."

The problems with the Phoenix pay system are at the centre of a labour tribunal hearing into whether the federal government is breaking the law by not paying thousands of public servants properly and on time.

As departments drilled down into the issues, Di Paola said, they found two "root causes" - the information public servants were plugging into the system was wrong or untimely, and the processing times of transactions at the Miramichi, N.B., pay centre were slower than expected.

There are "pieces" of pay administration that are not working, she said, but Phoenix "as a technology is working."

Di Paola said the 80,000 people backlogged awaiting extra pay are not considered Phoenix problems.

They ended up not getting paid what they are owed because information was not put into the system properly.

Her comments, however, have sparked a backlash from federal employees.

Chris Aylward, president of the Public Service Alliance of Canada, said Di Paola was trying to shift blame to the workers.

"We're talking 80,000 people who didn't input their information properly?" Aylward asked after her testimony. "I find that hard to believe. And there is no system problem or problem with the pay system? I find that extremely hard to believe.

"It's embarrassing when we have a manager responsible for the implementation of a new pay system who blames everyone else but the pay system itself ... and (she's saying) 'It's either your HR people or employees themselves who are not inputting data properly', " Aylward added.

DND employees who provided the Citizen with the internal message about Phoenix training echoed Aylward's criticism.

Military managers of the department's civilian employees do not currently have access to the Phoenix pay system, a situation that has also created problems in the department.

But they are still expected to complete what is called the "Phoenix Self-Service for Military Managers" course, the internal message noted.

Phoenix was designed to integrate payroll and human resources systems.

The government bought off-theshelf software and "reconfigured" and "customized" it to handle the 80,000 pay rules and rates of pay for public servants.

Motherboard Blog
Canada's CIA Had No Policy for Collecting and Using Massive Amounts of Data
Saturday, 01 October 2016
Byline: Jordan Pearson

Ottawa- The Canadian Security Intelligence Service (CSIS), the country's CIA equivalent, used large datasets to track and identify persons of interest without a policy to guide their collection, retention, or use, according to a new report from Canada's intelligence watchdog.
CSIS is tasked with tracking terror suspects within and outside of Canada, and the investigation was undertaken in the context of new, and incredibly broad, powers bestowed upon the spy agency by the controversial Bill C-51.

Canada has recently ramped up its efforts to identify people connected to pro- terror ideologies. In August, the Royal Canadian Mounted Police (RCMP) arrested 24-year-old Ottawa man Tevis Gonyou-McLean who was later released on a peace bond that restricts his movement, communication, and online activities. The RCMP's national security unit frequently receives intelligence from CSIS.

A report published on Thursday by the civilian Security Intelligence Review Committee (SIRC) notes that CSIS uses large databases to find out more information about suspects, develop leads, and even to "identify previously unknown individuals of interest by linking together types of information which have mirrored threat behaviour."

According the SIRC report, CSIS had "no comprehensive governance framework guiding the collection, retention and use of bulk datasets." The investigation, which began last year, recommended that CSIS have a policy in place by February of 2016, and CSIS suspended bulk data collection upon SIRC's recommendation until a policy could be implemented.

The Communications Security Establishment, CSIS' sister organization and Canada's answer to the NSA in the US, stopped sharing metadata with foreign spying partners under similar circumstances last year when an internal review concluded that the agency had handled data improperly.

The new report also suggests that CSIS employed overly generous interpretations of the law in order to collect more data than it was supposed to.

So-called "referential" datasets--defined by CSIS as already being publicly available, such as a phone book--are not considered to be "collected" by the agency under the CSIS Act, and thus do not need to meet the legal threshold of being "strictly necessary" for a particular investigation.

However, the watchdog "found instances where [it] felt the criteria for inclusion in the 'referential' category--data that is publicly available and openly sourced--were not met." Indeed, SIRC "found no evidence to indicate that CSIS had appropriately considered the threshold."

In other words, CSIS collected large datasets that the watchdog considered to be more invasive than, say, a phone book or a map, but was miscategorizing them and in the process bypassed legal safeguards governing sensitive data.

CSIS has not responded to Motherboard's request asking for clarification on what types of datasets would be considered referential and non-referential.

As a remedy, SIRC recommended that before engaging in bulk data collection, "a clear connection to a threat to the security of Canada" must be established, alternatives to bulk data collection must be considered, and an assessment of how likely the bulk data collection is to produce intelligence of value must be undertaken.

Overall, however, the watchdog was bullish on CSIS' use of its new powers despite these failures on the part of the spy agency.

CBC News
Canada plays catchup as wireless providers create emergency alerts for cellphones
Monday, 03 October 2016
Byline: Staff reporter

A new emergency alert system that transmits messages directly to cellphones, whether people want the alerts or not, is in the works for Canada.
The alerts would be transmitted to cellphone users regardless of their wireless providers. A similar system has been in place in the United States for years.

Once a message is sent out, it would be received by every cellphone in a geographic area, said Marc Choma, spokesman for the Canadian Wireless Telecommunications Association.

The association represents wireless service providers and businesses that develop products for the wireless industry.

The emergency messages would be used to alert Canadians to serious concerns like dangerous storms and possible terror threats.

System tested in Ontario

The system could use an emergency radio channel that is picked up by cellphones, and enables the system to reach people even if the servers that handle cellphone calls and text messages are overwhelmed.

"If there is going to be an emergency, the best way to reach people is with something that almost everybody has in their pocket right now, and that would be their cellphone," said Choma.

He said the alerts can also contain pictures and text.

This "cell broadcast system" has already been tested in the Durham Region of Ontario, according to Choma.

Public Safety Canada is working with the wireless industry to test the system. It's the federal department's mandate to keep Canadians safe from a long list of potential dangers, like crime, natural disasters and terrorism.

System could cost $25M

The Department of Public Safety said the wireless alert system pilot project will be completed in 2017. Choma said setting up the system could cost wireless providers about $25 million. Despite the cost, he said, wireless carriers support adopting the system.

The Canadian Radio-television and Telecommunications Commission (CRTC) launched a full public consultation on the emergency alerts in March.

The CRTC refused to comment on the system. However, the comments Canadians made about the proposed system have been made public. Those comments are mixed, but some people don't like the idea of being automatically included in the program.

"Only implement such a system if it can be disabled by the end user so that it is not forced upon them," wrote David Cole from Toronto. "That way, if it is poorly implemented, it can be turned off. Enough intrusion already."

"No, unless the CRTC prevents the wireless service providers from charging a fee to provide the service," wrote Ernest Price from St. Catharines, Ont.

'Take it to a higher level'

In Nova Scotia, the emergency management office supports the system. Paul Mason, director of emergency services, said the province currently uses TV and radio alerts to let the public know about emergencies.

"People spend a lot of time on their cellphones, and the alerts that would go out would have a loud noise that would get their attention ... I think bringing cellphones in would take it to a higher level."

Mason expects the CRTC will make a ruling on the system by December. If the alerts get the go ahead, he expects it to take at least a year or two before the system is brought online.

Public Safety Canada said it will work with all levels of government to make sure the alerting system is successfully implemented across the country.

Cell emergency alerts already in U.S.

A similar federal cellphone alert system already exists in the United States. It can only send a 90-character text message that can't contain any pictures or videos.

Ben Krakauer, director of watch command with New York City's Office of Emergency Management, said people cannot opt out of the program. "A national program that works regardless of whether you live in the city, whether you have a New York City phone number or if you're visiting us from across the country or around the world, is fantastic," he said.

In total, Krakauer said, they've only used the federal emergency alert system eight times. He believes it has saved lives.

Most recently, his office sent out a text message informing people of the search for Ahmad Khan Rahami, he Afghan-born U.S. citizen charged in last month's explosives incidents in New York City and New Jersey.

Metro News Vancouver
China flag ceremony at Vancouver City Hall raises red flags for some
Monday, 03 October 2016
Byline: David P. Ball

Local politicians touted a Chinese independence anniversary event in Vancouver this weekend as a way to celebrate Canada's relationship to the People's Republic of China.
But the celebration -- at which City Coun. Kerry Jang raised the Chinese flag on a City Hall flagpole alongside Richmond East MP Joe Peschisolido, both wearing red scarves -- isn't being celebrated by everyone in the Chinese-Canadian community.

"I myself and my family lived through the (Chinese) Cultural Revolution," said Meena Wong, former mayoral candidate for the Coalition of Progressive Electors. "The flag and red scarf represent oppression to me.

"My family was raided by the Red Guards wearing those red scarves. I'm very disgusted and disappointed."

The ceremony also sparked an online petition by a group of Chinese-Canadians who have protested outside pro-Communist Party of China events, including this summer in Richmond at a birthday party for late dictator Mao Zedong, infamous for overseeing the killings of at last 60 million people.

"We know how (Chinese authorities) treat people and how they use their influence to brainwash people," said Louis Huang, chair of the Alliance of the Guard of Canadian Values.

"We wanted to live a better life there and to change our country, but the (1989) Tiananman Square massacre completely destroyed everything of our dreams ... that's one reason I left China."

Huang added that it's not just human rights in the dictatorship which he finds worrying, but also concerns about allegations that Chinese officials are attempting to influence affairs in Canada. Those concerns have even been raised by the Canadian Security and Intelligence Service (CSIS), our spy service.

"The Chinese government is extending its influence into our society and into Canadian governments -- municipal, MLAs and MPs," Huang alleged. "Lots of people are worried about this ... We worry about our economy, our society, and our national security."

But Jang, who attended the event as the city's Acting Mayor, lashed out at critics -- asking why no one protested City Hall's recent Mexican or Slovenian flag- raising events.

"To me, this is just racism pure and simple," he told Metro. "Why pick on the Chinese?

"I'm getting tired of putting up with this bulls---, these types of comments, my whole life. I'm 64, I figured we should have come somewhere by now as Canadians."

Asked what he'd say to Chinese-Canadians criticizing the event, Jang said, "Leave the war at home."

"We have raised our concerns about human rights and the death penalty and we're affecting change in China," he said. "We don't get that change by just yelling or being mean. They're changing."

Peschisolido concurred, arguing that "engaging" with the Chinese government was the best way to achieve democratic reform.

He told Metro that his speech at City Hall, and other recent independence events, "talked about the importance of human rights, freedom of speech, of religion freedoms and freedom of the press."

Friends of Hong Kong organizer Fenella Sung told Metro she "was totally shocked" to see photos from the event, arguing that "even Hong Kong under the sovereignty of China would not do a flag-raising with Communist Party of China" representatives in attendance.

The red scarves especially caught her eye, because they're "the uniform of one of the Communist Party's hierarchies ... Do they really know what it means to wear that?"

Jang replied that the scarf has been a Chinese cultural symbol "since time immemorial" and predated the current regime. But Sung was unsatisfied with the explanation, nor claims it would help push China towards reform.

"How could they think that by raising the flag of Communist China, Canada would help anything to do with human rights in China?" she asked.

"Would prisoners being tortured be able to get freedom because we raised the flag on our City Hall? Would prisoners of conscience have their prison terms shortened?"

Washington Post
Freer rein for law enforcement hackers
Saturday, 01 October 2016
Byline: Ellen Nakashima & Rachel Weiner

Washington - When the FBI searched Andrew Workman's computer, they say they found pornographic videos of girls as young as 3 years old. A federal judge in Colorado ruled in September that the computer hack that helped the bureau uncover the videos should never have been allowed.
Why? The search warrant permitting the hack was issued by a magistrate judge in Virginia - outside the judicial district in which Workman lived - and in an apparent violation of federal criminal rules.

But a shift in federal rules set to go into effect in December says that a judge in one district can approve a warrant to hack computers outside that district in cases in which the computers' locations are shielded.

The change would aid the government in its sweeping national investigation into child pornography on the "dark Web," a universe of sites that are off Google's radar, where pedophiles using special technology can operate in anonymity.

The government contends that the change - which was approved by the Supreme Court in April and will go forward unless Congress opposes it - is necessary to clear up a loophole created by technology. Because investigators cannot know in advance where a target computer is physically located if a suspect

is using tools to mask his or her location, it is impossible to seek a search warrant in the district in which the target is located, officials say. They add that the change does not create any new authority and would still require a showing of probable cause before a warrant is issued.

"It really just gives us the ability to go in front of a [single] judge and get a warrant to do a search," Assistant Attorney General Leslie Caldwell said. "Otherwise we could find ourselves in a situation where we knew child-exploitation activity was happening in a lot of different places, but we wouldn't know exactly where the computers were located and we wouldn't have a judge to go to."

But privacy advocates and some lawmakers contend that the amendment to Rule 41 of the Federal Rules of Criminal Procedure would legally sanction mass hacking, in which federal law enforcement, with one warrant, can hack thousands of computers whose locations are unknown. And they argue that the rule change would allow prosecutors to seek out judges they feel would be more sympathetic to their warrant application.

If the rule change goes through, and if the government can show probable cause, "the FBI gets the authority to hack anywhere in the world," said Christopher Soghoian, principal technologist for the American Civil Liberties Union. "We desperately need to have congressional hearings and investigations into the use of this technology before it becomes the tool of choice of law enforcement."

Google, PayPal and several other technology companies have also lobbied against the change to the rule, calling it "dangerously broad."

In the case that ensnared Workman, the FBI took over a child- pornography site called PlayPen and surreptitiously installed software on it that enabled investigators to identify computers of users who went to the site. Since then, the government has obtained Internet protocol addresses of at least 1,300 computers in the United States, identified at least 38 children subject to sexual abuse, and brought about 200 cases.

Critics say that allowing the government to use such hacking software potentially endangers the computers of law-abiding citizens who have nothing to do with pedophiles.

"A bungled government hack could damage systems at hospitals, on the power grid, in transportation or other critical infrastructure," said Sen. Ron Wyden (D-Ore.), who is part of a bipartisan, bicameral group of lawmakers seeking to block the Rule 41 change.

Caldwell dismissed such assertions, saying that investigators work closely with private-sector computer security experts. "We do a lot of testing to make sure that the software we're using is not going to have harmful, unintended consequences," she said.

She also noted that the proposed rule change is the result of three years of extensive review and public testimony involving two committees consisting of academics, judges and defense attorneys.

The change to Rule 41, the government says, will help settle what has become a confusing area for judges and prosecutors.

Since the warrant used to hack Workman's computer was issued in February 2015, there have been 24 challenges to it. Nineteen judges who reviewed the warrant concluded it was not properly issued on venue grounds. Of those, four, including the judge in Colorado, threw out the evidence as a result. The other 15 ruled that the violation was not serious enough to suppress the evidence. And the remaining five found the warrant was properly issued.

Any change to Rule 41 would not automatically apply to the pending cases. But the Justice Department could request that each individual court apply the new rules.

Even if the change goes through, defense lawyers say they will continue to challenge the hacking warrants on other grounds. For instance, they have argued that the hacking constitutes a violation of the Fourth Amendment.

Judge R. Brooke Jackson, who decided to suppress the evidence in Workman's case, said he was aware that his ruling might free a guilty man.

"This is particularly difficult to stomach where the crime at issue is something as reprehensible as the possession of child pornography," he wrote in his decision. "On the other hand, this ruling might serve as a reminder to ... be attentive to 'something as basic as who can issue a warrant.'"

Kashmir Observer
Over 70% terrorists using cyber space: PMO Cyber Coordinator
Saturday, 01 October 2016

New Delhi - Over 70 percent of terrorists and terror groups across the globe are using various cyber medium tools to spread the evil of terrorism and further their goals, Gulshan Rai, the National Cyber Security Coordinator in the Prime Ministers Office (PMO) has said.
Speaking at the India Conference on Cyber Security & Internet Governance organised by Observer Research Foundation in New Delhi, Rai said 70-75 percent of terrorists are using tools like voice over internet telecom, social media and even encryption to spread the menace of terrorism and further their goals.

He said that post the controversy surrounding whistle-blower Edward Snowden, users and nations have become worried about the security of their data and are now using various encryption techniques and policies that has led to interruptions in seamless flow of data and information.

Former Central Intelligence Agency (CIA) employee Snowden copied and leaked classified information from the National Security Agency (NSA) in 2013 without prior authorisation.

Stressing on the need for finding a fine balance between the security and seamless flow of data, Rai said India is coming out with the national encryption policy with the focus on multi-stake holder model.

Based on public private partnership, the model, will have the government, industry, academia and the civil society working together to ensure a perfect balance between security and smooth flow of data.

The three-day international conference that began on September 28, was inaugurated by Union Minister for Information Technology & Law and Justice, Ravi Shankar Prasad.

New York Times
Hate Speech Bounded by Character Limit Alone
Monday, 03 October 2016
Byline: Jim Rutenberg

Column - If you go by what some Twitter users have to say, it's a wonder I can string together a sentence. I don't know how I ever manage to get myself to the office given what a "dumb ass" I am -- a Jew, no less, and someone who soils his pants out of fear of a Trump presidency. And if you don't believe that last bit, someone using a pseudonymous Twitter account was kind enough to provide a graphic photograph of the supposed soiling, but not his or her actual name, because it's just so much easier to hurl bile while cowering behind anonymity.
Then again, I don't know what it's like to be really savaged by Twitter. No one has threatened to rape me or kill me (unless being advised to kill myself counts). No one has relegated me to a gas chamber. And no one has hit me with anything like the sustained racist and sexist barrage that forced the "Saturday Night Live" and "Ghostbusters" star Leslie Jones to temporarily leave Twitter in disgust.

Now that Twitter is contemplating putting itself up for sale, we can only wonder what lucky suitor is going to walk away with such a charming catch.

Twitter is seeking a buyer at a time of slowing subscriber growth (it hovers above the 300 million mark) and "decreasing user engagement," as Jason Helfstein, the head of internet research at Oppenheimer & Company, put it when he downgraded the stock in a report last week.

There's a host of possible reasons for this, including new competition, failure to adapt to fast-changing media habits and an "open mike" quality that some potential users may find intimidating.

But you have to wonder whether the cap on Twitter's growth is tied more to that most basic -- and base -- of human emotions: hatred.

It courses through Twitter at an alarming rate, turbocharged by this year's political campaigns and the rise of anti- immigration movements that dabble in racist, sexist and anti-Semitic tropes across the globe. And this is to say nothing of its use by terrorist recruiters.

It's a lamentable turn that Twitter says it is urgently working to address.

Soon after Twitter took its place in the tech-driven media revolution a decade ago, it proved to be a forceful amplifier of ideas and personalities, one that could be a political game changer. Its role in enabling the Arab Spring movements remains inspirational. It helped foster bottom-up movements like the Tea Party and Black Lives Matter here in the United States. And, of course, it helped make possible the outsider candidacy of Donald J. Trump, who continues to use it, er, aggressively.

The back-and-forth over his candidacy, and the news media's coverage of it, have added a new cache of material to the uglier side of Twitter's oeuvre.

More often than not, the venom comes from pseudonymous accounts -- the white hoods of our time.

Just take a gander at @Bridget62945958, who published a series of anti-Semitic posts against my colleague Binyamin Appelbaum. One message showed a series of lampshades. Its caption read: "This is your family when Trump wins. Get your Israeli passport ready."

Twitter suspended the account after Mr. Appelbaum brought it to the attention of Twitter's co-founder and chief executive, Jack Dorsey, by way of his own Twitter feed. A new account sprang right up to continue the vitriol, prompting Jeffrey Goldberg, a national correspondent for The Atlantic, to write a post asking Mr. Dorsey, "How does it feel to watch Twitter turning into an anti-Semitic cesspool?"

Mr. Goldberg says he is torn about what Twitter should do, given that its cause -- openness and free speech -- is a reason he and so many other journalists are drawn to the service. "That's the fundamental problem," he told me. "At a certain point I'd rather take myself off the platform where the speech has become so offensive than advocate for the suppression of that speech."

Twitter clearly wrestles with the same fundamental problem. It warns users they may not "threaten other people on the basis of race, ethnicity, national origin, sexual orientation, gender" and various other traits. Yet it often fumbles the enforcement. Charlie Warzel of BuzzFeed News unearthed a doozy last week.

After a user who identified herself as Kathleen posted a tweet criticizing the Trump campaign, a Twitter member going by Adorable Deplorable directed a message back at her featuring a photograph of a beheaded man -- apparently an ISIS victim -- and the words, "Your [sic] heading for a deep hole."

Twitter forced the photo's removal after BuzzFeed's inquiries, but it initially told Kathleen that the post did not violate its policies. This is apparently common. In a BuzzFeed survey of Twitter users, about 90 percent of those who said they had reported abuse said their complaints went unheeded.

So-called trolls are a problem for all social media -- even Facebook, which keeps a tidier, more contained system. (To wit, the Facebook message a local New Jersey politician wrote to the Daily Beast writer Olivia Nuzzi after she posted something about Mr. Trump that he did not like: "Hope. You. Get. Raped. By. A. Syrian. Refugee.")

But the openness of Twitter, and the sheer speed and volume of information that moves through it, present a particularly hard challenge that executives there say they are rushing to meet.

"Everyone on Twitter should feel safe expressing diverse opinions and beliefs," the company said in a statement it sent me on Saturday. "But behavior that harasses, intimidates or uses fear to silence another person's voice should have no place on our platform."

In a letter to shareholders, Mr. Dorsey said the company was putting in place technology enabling it to more readily detect abusive accounts, make it easier for users to report them and even prevent them in the first place.

It's all a bit tricky for a company founded with an absolutist ethos, once calling itself "the free speech wing of the free speech party."

Some of its moves to curtail abuse have drawn accusations that it is applying a double standard aimed at conservatives. After Twitter placed the Breitbart News editor Milo Yiannopoulos on permanent suspension for his role in the Twitter campaign against Ms. Jones, he accused it of declaring "war on free speech," specifically against "libertarians, conservatives and anyone who loves mischief."

Another banned Twitter provocateur, Charles C. Johnson -- whom my predecessor David Carr once called a "troll on steroids" -- says he is planning a lawsuit to fight his suspension.

In an interview, Mr. Johnson said he respected Twitter's right to ban patently offensive speech but argued that it needed to set a consistent, uniformly applied standard. Still, he said, "the problem of trolls" might be unsolvable.

"It might just be a human nature problem," he said. "Maybe we don't like each other that much -- and that's what Twitter has revealed."

We didn't need Twitter to reveal that. And in the previous two media revolutions -- radio and television -- the country managed to strike some sort of accommodation between the right to free speech and the greater civic good.

That happened because there was an immediate national recognition that these media could have tremendous power to shape culture, politics and government for good and for ill.

As Herbert Hoover moved to establish basic standards for radio, he acknowledged that it had "great possibilities of future influence" but was also of "potential public concern."

He declared radio should be developed with public interest in mind, an idea that carried over to television. What followed were standards that forced broadcasters to devote at least some of their hours to civic affairs while avoiding obscene and "grossly offensive" content. At times, the efforts have wandered dangerously into censorship. But at least there was a big national discussion about what should beam into American living rooms.

There was no similarly robust discussion at the start of this, the latest media revolution, and we can only hope that the political mistrust isn't so great that we can't have a constructive one now.

Each new media development has served as a mirror for the society that spawned it. It sure seems time for a good, hard look.

But what does this dumb, pants-soiling Jew know?

London Times
Google diverts would-be jihadists away from radical websites
Monday, 03 October 2016
Byline: Anthony Cornish

London - Hundreds of thousands of people seeking information about Islamic State on Google have been diverted to anti-extremism search results, as part of a drive to stop Muslims becoming radicalised online.
The pioneering project directed people searching for particular Isis-related terms to YouTube videos that confront jihadist propaganda.

The under-the- radar scheme, which has been praised by government ministers, made use of Google's AdWords service, which allows organisations to pay to have their results at the top of searches.
Keywords targeted included the Isis slogan baqiya wa tatamaddad (remaining and expanding), the deferential term al dawla al islamiya (supporters of Islamic State), and the organisation's media sources Al-Furqan, Al-I'tisam, Al-Hayat, Amaq news agency and Ajnad.

Names of buildings in Isis-controlled areas known to host recruits, such as the Ninawa International Hotel in Mosul, in northern Iraq, were included.

The project, known as Redirect Method, was launched in a pilot scheme by Jigsaw, a technology incubator formerly known as Google Ideas. It was operated by the London-based tech business Moonshot CVE (Countering Violent Extremism).

The initiative comes amid growing criticism of the failure of technology giants to prevent online radicalisation.

The scheme has escaped the hostility aimed at the British government's Channel and Prevent anti-radicalisation strategies, which go further in identifying and challenging potential jihadi youngsters but have been attacked by some groups for perceived stigmatisation of Muslims.

Redirect Method's first task was to work out which words might interest a potential fighter. Former extremists, researchers and online advertising specialists helped to choose terms which could identify searchers at risk of radicalisation.

"Amaq News" was added in March when Isis used the outlet to claim responsibility for the Brussels bombings which killed 32 people.

Moonshot did the English-language version of the scheme while Quantum Communications, with offices in Lebanon and Washington, produced an equivalent in Arabic.

Users were invited on their screens to watch specially created YouTube channels with playlists of anti-Isis videos. The clips chosen were available online.

The videos included real footage from the self-styled caliphate's de facto capital in the Syrian city of Raqqa, first-hand accounts of what life is like under Isis, and imams challenging the group's interpretation of Islam.

In English, there were 30 campaigns covering more than 1,000 keywords. The Arabic campaign was more extensive. The Redirect Method's pilot claimed to reach 320,000 online users in eight weeks. Engagement was quantified in terms of "click-through rate" and effectiveness was judged by how long users spent watching the content.

Baroness Shields, minister for internet safety and security and a former managing director at Facebook, said: "Global technology companies play a vital role in addressing this challenge posed by terrorists and extremists using their platforms to radicalise, recruit and inspire."

Analysis: Search engine could class anyone as extreme

The Redirect Method may threaten anti-establishment groups and could damage trust in the Google search engine, according to Arun Kundnani, former researcher at the Institute of Race Relations.

He says that it sets a dangerous precedent for the future of ideas online.

"Once we have accepted this for people we call jihadis, it will be easier to accept it for all sorts of other radicals. There is a danger that Jigsaw will end up identifying individuals who express dissenting or unpopular opinions, classify them as extremists, and then opaquely engineer their information environment -- what we would normally call propaganda.

"There will be growing distrust of [Google's] search algorithm and people will choose to rely on other information sources that more closely match their world view."

Ian Pearson, a futurologist, said: "Superficially it looks like a good thing. If someone's in the early stages of radicalisation then redirecting them along a safer path and stopping them from being radicalised would seem to be a good idea.

"On the other hand, you do wonder why Google is this great moral arbiter of our time -- where does that mandate come from? Why do they think that they're the people who should be making such decisions? Surely we have governments that do that."

Financial Times
Lauri Love on US extradition and how hackers can help companies
Monday, 03 October 2016
Byline: Maija Palmer

London - If businesses are serious about reducing the risk of cyber attacks, they must work closely with hackers, says Lauri Love, the UK computer security expert who is facing extradition to the US, accused of computer crimes.
Mr Love, who lost his appeal against extradition in September, says more should be done to ensure young people with computer skills learn to use their talents in a positive way working for companies, rather than engaging in crime. The transition to cyber vandalism and worse often starts when a bright but socially awkward teenager is drawn into the wrong circles, he says.

"A lot of the mental make-up that can make you quite good at analysing computers and information systems tends to manifest with problems of social adaptiveness. People can find that they have trouble concentrating at school or problems with behaviour and authority," Mr Love adds. "They don't have the availability and means of getting into doing cyber security and developing their skills in the appropriate safe environment in a constructive way.

"The underworld doesn't care how well- dressed you are or whether you can maintain eye contact. They just care if you have the skills. There is a perverse sense in which the criminal underworld is more meritocratic than society. Sadly, their agenda is different."

Until last month, Mr Love was part of a social enterprise, Hacker House, which aims to give young computer enthusiasts a place to practise their hacking skills without causing damage -- and to put them to use helping, rather than harming, businesses.

"We want to provide a place where people who have started down the path to being a little bit naughty can come. We can say, 'OK, we will teach you how to hack, you can have all the fun, but you won't be interfering with someone's business and you won't find yourself on the end of a difficult conversation with people with badges,'" he adds.

Companies could learn a lot from hackers, Mr Love says. Most businesses severely underestimate their risk from cyber crime. Hackers often penetrate their defences in very basic ways.

"There is a lot of code running on computers -- some of it is kept up to date and patched against security vulnerabilities, some of it is not," Mr Love says. "Hacking is mostly a case of persistence; it is not always a case of spectacular ability -- just determination to keep looking until you find the one thing that wasn't up to scratch."

He compares looking at the back end of corporate systems to looking back in time. "Sometimes you end up going back to the 1990s and finding levels of security that we ought to have moved past," he says. "You see the same mistakes over and over again."

There is a tradition of ex-hackers going to work in corporate security. Kevin Mitnick, who was imprisoned in the US in the 1990s for hacking, runs his own corporate security consultancy. George Hotz, a hacker who faced litigation by Sony in 2011 for hacking the PlayStation 3 games console, has since worked for Facebook and Google.

Companies can also tap into the hacker community more broadly by setting up so-called "bug bounty" programmes, where hackers are rewarded if they discover and report serious security flaws.

"We can shape the rules of the game so people who find these things out have a way to come to the [company] and say, 'I have found out this is insecure,' without being afraid of being prosecuted or sued," Mr Love says. "We can create an incentive structure to bring people onside. These are bug bounty programmes and people are just learning to do them."

With a mischievous smile, Mr Love, who is accused of breaking into US military computers, adds: "In fact the Pentagon just ran its first bug bounty system. And so whereas some people in the world are in trouble for allegedly hacking the Pentagon, now the Pentagon is asking sometimes the same people to come and hack it."

The FBI and US Department of Justice allege Mr Love stole thousands of files from the Pentagon and Nasa, as well as from other bodies, including the Federal Reserve and Environmental Protection Agency.

Mr Love's lawyers have argued that he should face legal proceedings in the UK rather than the US, where they say his health could be affected by a lengthy jail term. Mr Love has Asperger syndrome, which his lawyers say could deteriorate and lead to a mental breakdown or even suicide.

In any case, Mr Love feels the current approach by the police and criminal justice system is not deterring hackers.

"The issue is that there are 7bn people connected to the internet and not all of them are in legal jurisdictions where computer crimes will be prosecuted. Even if you can scare all the people in the UK into not testing your security, that doesn't affect the people that live somewhere where you don't have extradition arrangements," he says.

He is not arguing that computer breaches should be decriminalised, but he says there should be more differentiation between cases where hackers are going in to steal money or information, and cases where people are merely testing the system's defences.

"When you damage a system, when you trespass, when you interfere with business operations -- that is a crime and should remain defined as a crime. But the priority of the state shouldn't be to try to frighten people into not testing security, we need security to be tested," he says.

"I don't think we should be heavy-handed with people, not when they haven't adopted a criminal mindset. I'm hoping law enforcement can start taking more of a harm-reduction approach rather than this kind of traditional drugs-war approach of being very hard on it and trying to scare the kids straight -- because the kids aren't being scared straight."

Mr Love's case is due to considered by Amber Rudd, the UK's home secretary, in mid-November. If she decides to authorise the US's extradition request, Mr Love will have 14 days to appeal against the ruling.

SC Magazine (UK)
National Cyber Security Centre HQ operational
Monday, 03 October 2016

London - The UK's new National Cyber Security Centre (NCSC) officially opens for business today as a public-facing part of GCHQ that acts as a focal point for the government to deliver authoritative advice on tackling cyber-security issues. It will be based in the Nova office and shopping complex near Victoria Station in London, not in Cheltenham at GCHQ, as originally announced last year, though it will also have offices there..
While this operational centre will focus on defensive work, it will be able to call on offensive capabilities developed by GCHQ and the Ministry of Defence.

According to Evening Standard reports, the NCSC will have a staff of 700, more than half of whom will be based in the new HQ, moving in to the building later this year and in early 2017. It will have specialist teams for the City, Whitehall, intelligence and security services, energy, telecoms and other parts of the critical national infrastructure.

It is led by CEO Ciaran Martin who was director general cyber at GCHQ, with Dr Ian Levy, former technical director of cyber-security at GCHQ, becoming technical director at the NCSC. The NCSC's website is scheduled to go live tomorrow (4 October).

The launch of the organisation was announced by the former Chancellor George Osborne last year then confirmed by Matt Hancock, minister for the Cabinet Office and Paymaster General. Its remit is to ensure the online safety of the general public, both public and private sector organisations as well as the UK's critical national infrastructure. Objectives include raising awareness of government intent; undertake genuine dialogue that shapes service delivery; demonstrate serious commitment to listen; and develop sustainable engagement channels to provide structured consultation with the private sector.

One of its first tasks is to work with the Bank of England to produce advice for the financial sector to manage cyber-security effectively.

Minister for the Cabinet Office and Paymaster General, Matthew Hancock commented: "In establishing the National Cyber Security Centre we are creating a body devoted to cyber-security and this will transform the UK's approach to an issue that affects us all.

"This important work with the Bank of England is paramount to ensuring that businesses of all shapes and sizes understand the threats and what they can do to mitigate them.

"We'll do this by informing the entire business community and public sector about emerging threats, providing support when attacks happen and educating everyone on how best to stay safe online."

In an official statement Robert Hannigan, director GCHQ said: "Given the industrial-scale theft of intellectual property from our companies and universities, as well as the numerous phishing and malware scams that waste time and money, the National Cyber Security Centre shows that the UK is focusing its efforts to combat the threats that exist online.

"Ciaran will be an excellent Chief Executive who will ensure that the NCSC will continue the outstanding work done by all of the existing organisations to protect national security and our economic success."

Ciaran Martin stated: "I'm very pleased to have the privilege of leading a world class team to get ahead of one of the most important threats of our time." Echoing Osborne's comments last year, he told ES, "Our role is helping t make the UK the safest place to live and do business online," noting that this would range from tackling hostile states, criminal gangs, to smaller scale attacks.

In an email to SCMagazineUK.com, David Damato chief security officer, Tanium

Offered his advice for the new NCSC: "The new National Cyber Security Centre will provide an important bridge between business and government, but it cannot succeed if it does not urgently address the accountability gap that sees board members and executives too often without the information and tools they need to take responsibility for cyber security.

"Discussions on cyber-security rarely reach corporate boardrooms, leaving many of the UK's biggest businesses dangerously exposed. Only a third of the leaders of UK's top 350 companies say they understand the threat of a cyber-attack and even fewer are regularly updated about security threats.

"If the UK wants to stem the tide of cyber-crime, the National Cyber Security Centre must make closing the corporate accountability gap its first order of business."

According to its prospectus, The National Cyber Security Centre will have four key objectives:

. To understand the cyber security environment, share knowledge, and use that expertise to identify and address systemic vulnerabilities. The NCSC will be the centre of government expertise on what is happening in cyberspace, combining the knowledge gathered from incidents and intelligence with that shared through the close relationships with industry, academia and international partners. That knowledge will be used to provide best practice advice and guidance, and to tackle systemic vulnerabilities to enhance cyber security for all.

. To reduce risks to the UK by working with public and private sector organisations to improve their cyber security. The NCSC will support the most critical organisations in the UK across government and the private sector to secure and defend their networks. It is planned that this will include the provision of bespoke advice and guidance, help to design and test networks, and exercise response arrangements.

. To respond to cyber- security incidents to reduce the harm they cause to the UK. It is recognised that despite all the efforts made to reduce the risks and enhance security, incidents will still happen. When a serious cyber incident occurs, the NCSC will work with victims to minimise the damage, to help with recovery, and to learn lessons to reduce the chance of recurrence and minimise future impact. Often this will entail helping by connecting victims with commercial companies known to be excellent at cyber incident response. At the same time the NCSC will ensure that the wider response of government and law enforcement is well co-ordinated. And in the case of very serious incidents this might mean communicating publicly about consequences and the steps people and businesses should take to protect themselves.

. To nurture and grow our national cyber security capability, and provide leadership on critical national cyber security issues. Cyber security and information technology continues to develop and evolve at a rapid pace. As the Centre within government for cyber-knowledge, the NCSC will have the best possible

visibility of what is happening today - in terms of threats, vulnerabilities and technology trends. This means cutting edge technical research teams, combining the best of government, industry and academic expertise, scanning the horizon and helping plan for what could challenge us tomorrow. The NCSC will lead the UK's thinking across the range of initiatives and developments, ensuring that the UK Government, organisations and the public can harness the advantages that new technologies bring in a safe and secure manner.

Boston Globe
Hackers now have wider choice of weapons
Monday, 03 October 2016
Byline: Hiawatha Bray

Boston - Over the past two weeks, hackers launched two of the biggest digital attacks in Internet history, targeting a French Internet provider and one of the foremost computer-security journalists in the United States.
What's perhaps more unusual is not the size of the attacks, but their source: Internet-connected cameras and digital video recorders like those in home and office security systems.

Cyber-criminals hacked into thousands of these devices around the world and used them to bombard analyst Brian Krebs and the French company OVH with trillions of bits of meaningless data. The attack was severe enough to temporarily shut down Krebs's website.

The attacks raise questions about the security of the much-vaunted Internet of Things (IoT), in which everyday objects from home appliances to door locks, cars, and digital video recorders are connected over a network and can be controlled remotely. The research firm Gartner Inc. estimates there are about 6.4 billion IoT devices in the world, with many many more on the way--20.8 billion by 2020. Internet security analysts say that many of these devices are just as hackable as our home computers, but much harder to protect from attack.

"It's already a nightmare," Krebs said of the state of cyber-security for these Internet-connected devices. "They just keep shipping devices that are insecure by default, and it's been going on for a long time."

Most IoT devices offer some measure of security, but usually not enough. For example, many devices require a password to change software settings, but don't force the user to create one of his own. So many users stick with the default password installed at the factory. They might as well use none at all. The default passwords for hundreds of popular products are published online; hackers can just look them up on Google.

Once in control of the device, the hackers can install malware to steal data from other devices, pump out spam e-mails, or, as in Krebs's case, crush an Internet site under an avalanche of data.

Last year, Burlington-based data security company Veracode tested 10 such devices. Testers found that eight of the 10 devices had serious security flaws that could allow intruders to seize control.

Consumers are famously ill-equipped to protect their personal computers from malware attacks. But most people know enough to install antivirus software and download the latest security patches. Bruce Schneier, a fellow at the Berkman Klein Center for Internet & Society at Harvard University, said many IoT devices don't provide a way to update their software, and most people wouldn't know how anyway.

"We're moving down the chain to lower-cost embedded devices without upgrade paths, without patch systems, without security teams," said Schneier, who is also chief technology officer of Resilient, a data security company owned by IBM Corp. "There's going to be no way to fix this," said Schneier. "None."

The Xively business unit of Boston's LogMeIn Inc. makes software that helps manage the data generated by IoT devices. Ryan Lester, Xively's director of IoT strategy, said that most IoT device makers put good security features into their products.

But he acknowledged, "for many organizations the race to get an IoT product to market is a fast and furious one and it can be tempting to cut corners - especially in areas that can be complex and time consuming like security."

Lester said that his company has a set of security standards that all clients must meet. "We have turned a few prospective customers away that did not," he said.

But Roland Dobbins, principal engineer at computer security company Arbor Networks Inc. of Burlington, said that it's not enough to rely on the security policies of individual companies. He called for IoT companies to band together and set industrywide policies, to make their products harder to hack.

"Vendors who write code for these devices must be given very, very specific guidance on security standards," he said. But up to now, the industry's efforts in this area have mostly been "lip service," he said.

Even if such standards are drawn up, Dobbins said it might be necessary for the federal government to ensure compliance. "Something's going to have to change," Dobbins said, "and it's just a question of whether industry is going to get its act together or government is going to have to intervene."

The National (UAE)
WhatsApp case reveals India's need for law to protect data privacy
Monday, 03 October 2016
Byline: Rebecca Bundhun

New Delhi - India needs new data privacy laws, experts say, as a court case with WhatsApp has brought the issue into sharp focus.
WhatsApp last month revised its privacy policy to allow the Facebook-owned messaging app to share data with Facebook and permit targeted adverts.

Two students filed a public litigation in the Delhi High Court to try to get the policy reversed. The court ruled that because the policy would only come into effect on September 25, all data before that should be deleted. It also resulted in the court asking India's telecom regulator, Trai, to look at bringing WhatsApp and other messaging services under the statutory regulatory framework. But the students did not succeed in winning the case to get the WhatsApp policy reversed.

"In addition to laws for data privacy and security, what is required to be done on priority is to educate the end user of the implication of such usage," said Srividya Kannan, the founder and director at Avaali Solutions, based in Bangalore.

India is a key market for Facebook and WhatsApp given the rapid growth of smartphone and internet use. WhatsApp in its defence has said that users are under no obligation to use the app.

The number of internet users in India is estimated to have reached 402 million by the end of last year, meaning that India has passed the United States with the second-largest number of internet users in the world. Only China is ahead, according to the Internet and Mobile Association of India and the research group IMRB International.

"Data privacy is an intrinsic risk to the usage of any of the social media applications," says Ms Kannan. "User data including perhaps the phone number could be compromised for commercial marketing, advertising. For enterprises, while social media is a great means of customer service, this is a double-edged sword and must be designed to prevent leakage of business sensitive information."

Bloomberg
U.S. spies finally embracing iPhones, wireless connections
Sunday, 02 October 2016
Byline: Nafeesa Syeed

Washington - U.S. spies are catching up to the masses in their gradual embrace of 21st-century technology, from installing wireless connections in secure facilities to wielding iPhones and tablets, according to an official with the U.S. National Geospatial-Intelligence Agency.
"We'd be cutting off our noses to spite our faces by denying us those kinds of tools," Matt Conner, deputy chief information security officer of the agency, said in an interview.

The NGA provides intelligence to other parts of the government from battlefield maps to satellite imagery of national disasters. It's among agencies that are working with the Director of National

Intelligence to study how to maximize the use of secure wireless networks and devices, while still maintaining the cover that spies need.

Already, NGA has secure wireless for its senior leaders in its mammoth headquarters in Springfield, Virginia, outside of Washington, Conner said. Protective equipment needed to make a wireless system secure can be costly and "there are people who are skeptical that there's value there," he said.

Conner, 41, a former information security officer with General Dynamics Corp., and others at the NGA migrated last year from BlackBerry devices to iPhones, although they aren't allowed to use them in the agency's building. The agency is also "moving swiftly" toward cloud services with Amazon Web Services on both its encrypted classified network and its unclassified network, as well as working with Microsoft on other cloud-based resources, he said.

In addition, it has developed internal mobile apps for workers as well as a few that are available to the public in Apple's App Store and on Google Play. Its Mobile Awareness GEOINT Environment app helps first responders in natural disasters by letting them geotag field reports and to record photos, videos and audio to share with others.

The agency also has opened an outpost in Silicon Valley. Its staff is trying to learn from startups and tech companies, which are making sophisticated yet widely available commercial geospatial tools, such as Google Earth.

NGA, which operates under the Defense Department, built the model of al-Qaida leader Osama bin Laden's compound in Pakistan that the military used for training before the 2011 raid that killed him. This year, NGA provided intelligence to authorities during the Olympics in Rio.

Conner oversees the cybersecurity of vast digital archives and the transmission of intelligence data. NGA uses encryption for long-haul communication between agencies as well as for the images and products resting in its libraries, he said. His team of a few hundred civilian employees and contractors also has to "sanitize" data that teams collect from social media and other open-source streams, screening for malware.

As with other military agencies, NGA's computer networks are targeted by other nations, according to Conner, who wouldn't name countries but said "they're probably the ones you think they are." The FBI has high confidence recent hacking attacks on U.S. political groups and election systems were orchestrated by Russia, according to a person familiar with the agency's probe. President Vladimir Putin has rejected the accusations.

The high-profile reports of hacking have "absolutely raised the visibility" of his work, Conner said. "I've joked often that it's a good problem to have -- we have more senior-level attention on our cybersecurity program that I'm aware of," he said.

The agency also takes threats from within seriously after the leaks by Edward Snowden, who worked for a National Security Agency contractor.

"We're conscious of the insider," Conner said. "We have a very robust program to manage our insider threat, at least bolstered by the Snowden disclosures three years ago, and that is across the federal agency space."

Daily Telegraph
Cyber crime unit opens amid surge in online attacks
Saturday, 01 October 2016

London - Britain's first national centre for combating cyber criminals will open next week, amid rapid growth in the number of online attacks.
Terrorists, hackers and online gangs will be targeted by intelligence experts at the new National Cyber Security Centre in Victoria, central London. A team of around 700 people will help to advance the Government's war against cyber crime.

The threat is growing, with 200 major incidents a month, double the rate last year.

The centre will be led by Ciaran Martin, formerly the director general for cyber security at GCHQ.

At a cyber security conference in Washington DC earlier this month, Mr Martin outlined plans to create a firewall that could protect government agencies and internet users against cyber attacks. He said Britain was facing twice as many "national security level cyber incidents" as this time last year.

Mr Martin said that the centre would help make the UK "the safest place to live and do business online".

"We'll tackle the major threats from hostile states and criminal gangs. But we'll also work tirelessly to protect people automatically from those smaller scale and deeply damaging attacks." The creation of the agency was announced by George Osborne, the former chancellor, in November last year. GCHQ has said one of the centre's first tasks will be to work with the Bank of England to provide advice to the financial sector.

Motherboard Blog
Shadow Brokers' Whine That Nobody Is Buying Their Hacked NSA Files
Sunday, 02 October 2016
Byline: Joshua Kopstein

Washington - The hacking group responsible for stealing a large cache of National Security Agency hacking tools is very upset that no one seems to be bidding on their pilfered files.

Early Saturday morning, the person or group which calls itself "TheShadowBrokers" authored another bizarre rant, expressing their annoyance at the seeming lack of interest in ponying up bitcoins to release the full set of stolen files.

"Peoples is having interest in free files ... But people is no interest in #EQGRP_Auction," the mysterious hacker group complained in a ranting post on Medium, which seems to be purposely written in Borat-style broken English. "TheShadowBrokers is thinking this is information communication problem."

The message also blindly lashes out at hackers, foreign intelligence services, and basically anyone else who hasn't bid on the files.

"TheShadowBrokers ... is thinking peoples is having more balls, is taking bigger risks for to make advantage over adversaries," the group adds. "Equation Group is pwning you everyday, because you are giant fucking pussies."

So Shadow Brokers are implicitly criticising me for not buying their zero days, or what? Mustafa Al-Bassam October 1, 2016

TheShadowBrokers originally made headlines after posting a sample of the cache, which contained exploit code matching the names and functionality of several previously-revealed NSA hacking tools. The contents and organization of the files led experts to conclude that they were accidentally left behind on a compromised server once used as a staging area by an NSA-linked hacking entity called Equation Group.

That theory was reinforced last week, when Reuters reported that "four people with direct knowledge" of an FBI investigation into the leak had stated that the files were found by Russian hackers after NSA operatives "mistakenly" abandoned them on a remote server. There is still no conclusive evidence that TheShadowBrokers is associated with Russian intelligence services, however.

Motherboard reached out to the hackers and will post an update if we receive a response. However, the group stated in their Medium post that they would only agree to interviews if offered money.

Of course, it's not exactly surprising that no one is rushing to bid on the group's stolen files. While the tools are likely legit, the high profile of the leak makes it insanely risky, and the suspected age of the exploit code makes it unclear whether the hacks are even still effective.

At the time of this writing, TheShadowBrokers have only received bids for a total of 1.76 bitcoins--or about $1,082--far below the group's asking price of $1 million.

Engadget Blog
Hackers targeted voter registration systems in 20 states
Saturday, 01 October 2016

Washington - With the US presidential election just over a month away, a Homeland Security official says voter registration systems in 20 states were the targets of hackers. The Associated Press reports that an official from the department confirmed the activity over the the last few months and explained that it hasn't been determined if the threats were domestic or foreign. ABC News reported this week that Russian hackers targeted the systems of 20 states and successfully infiltrated four.
This news follows an FBI warning in August that hackers outside of the US took aim at systems in Illinois and Arizona. While it's important to note that these attacks are on the voter registration systems and not the actual voting systems themselves, it's still a major concern heading into the election. There are already concerns that foreign hackers may try to influence the results of the process and the FBI has said it's looking into Russian hackers that may try to do so.

As the AP notes, government officials say that accessing the polling systems to sway an election would be "nearly impossible" because they are decentralized and not connected to the internet in most cases. However, Engadget security columnist Violet Blue argues there's reason to be concerned about the issue for a number of reasons, including aging voting machines. Homeland Security Secretary Jeh Johnson told state election officials last month to take technical precautions and make sure that machines aren't connected to the internet for added security.

Associated Press
Iran says new attack drone modeled on captured US aircraft
Saturday, 01 October 2016

Tehran - Iran's Revolutionary Guard has built a new attack drone which is similar to a U.S. unmanned aerial vehicle captured five years ago, Iranian media reported Saturday.
The semi-official Tasnim news agency says the "Saegheh" (Thunderbolt) drone is similar to the RQ-170 Sentinel spy drone. Iran's state-run Press TV says the long-range drone can carry four precision-guided bombs. Neither report gave figures for the drone's range.

Iran claimed to have shot down an RQ-170 drone used by the Central Intelligence Agency in December 2011 and broadcast footage of the recovered aircraft. It also claims to have captured three American ScanEagle drones.

Iran said last year that it had successfully tested its replica of the RQ-170.

Also on Saturday, Tasnim published photos of what it said was a U.S.-made MQ-1C drone captured recently by the Guard. It did not say when or how the drone was captured.

Fox News
FBI files reveal how Clinton server was created in K Street lab
Saturday, 01 October 2016
Byline: Catherine Herridge & Pamela K. Browne

Washington - If Hillary Clinton's 'homebrew' server ever got the Mary Shelley treatment, IT specialist Bryan Pagliano would make a fine Dr. Frankenstein - FBI documents reveal new details about how he painstakingly created the machine over a series of months while working in a room along Washington's storied K Street.
According to files released last Friday evening, Pagliano worked to design and build the now-infamous server inside a room once used as part of Clinton's campaign headquarters. On the street known as Washington's power corridor, Pagliano even used computer remnants from Clinton's failed 2008 presidential bid, where he had worked as an IT specialist.

The story of how the server came into existence became clearer thanks to witness interviews known as 302s. Though they were highly redacted, the bureau files include new details Pagliano revealed in a June 24 interview with the FBI.

In that interview, Pagliano said it was longtime Clinton Foundation aide Justin Cooper who asked him to build the server "in the fall of 2008" and that Pagliano completed the work in early 2009. (Pages 155, 163)

After the server's completion in the makeshift lab on K Street, Pagliano stated that he "rented a minivan and drove to Chappaqua New York to install the email server in the Clinton residence."

Pagliano and Cooper were separately interviewed by the FBI five times during the bureau's investigation into Clinton's use of private server and private email for government business while secretary of state. According to the reviewed documents, Pagliano was interviewed first on Dec. 22, 2015 and again six months later on June 21, 2016.

Cooper was interviewed three times -- once in 2015 and twice in 2016 -- and appeared before Congress. Pagliano was one of five people who received limited immunity from the Justice Department, has taken the Fifth and refused to testify before Congress.

In his interviews with the FBI, Pagliano said that "he could not recall any existing computer systems at the Chappaqua residence other than the Apple server described previously to the FBI."

Widely published reports including one in the New York Times indicated that Clinton was informally announced as Obama's choice of secretary of state on Nov. 22, 2008, with her formal nomination on Dec. 1. After working in her 2008 presidential campaign, Pagliano joined Clinton in the State Department as an employee and IT specialist, but he also continued to work on the homebrew server he built.

Pagliano, though, insisted to the FBI that he "believed the email server he was building would be used for private email exchange with Bill Clinton aides."

In addition, it was during his second interview with the FBI in June, that Pagliano suddenly "recalled being given a list of user names and passwords that Cooper asked to be transferred from Cooper's Apple server to Pagliano's system." (Page 164)

The 302 continued, "Pagliano did not recall transferring an account for Hillary Clinton and does not know how her account was installed on the server he built."

Justin Cooper did not work for the State Department but stated in his March 2016 interview that he registered the domain, clintonemail.com, because he handled financial issues for the Clintons. Cooper continues to works for Clinton Foundation entities which include Teneo.

Despite handing out limited immunity deals to five people including Pagliano, FBI Director James Comey has stated that Clinton's actions with her email practices were "extremely careless" -- but not criminal. As a presidential candidate once again, Hillary Clinton continues to refer to the server and her use of private email as "a mistake."

Strikingly, Cooper also said in his March interview that Hillary Clinton "had Sensitive Compartmented Information Facilities (SCIF's) in both her New York residence as well as her residence in the District of Columbia (DC)."

In his last interview with the FBI in June, Cooper suddenly remembered there were also two identical iMac computers inside what were supposed to be tightly secured rooms used to review classified materials. The interview states, "Cooper recalled a personally-owned iMac computer in the Sensitive Compartmented Information Facility (SCIF) of both the Washington, DC and Chappaqua, NY residences of Hillary Clinton."

Cooper added he did not have the combination to open the SCIF and admitted: "The SCIF doors at both residences were not always secured." This on its face is a direct violation of security protocol.

Cooper added further insight into close aide Huma Abedin's access to the SCIFs by stating "Abedin was frequently there but did not know if Abedin could access the SCIF when it was secured."

Catherine Herridge is an award-winning Chief Intelligence correspondent for FOX News Channel (FNC) based in Washington, D.C. She covers intelligence, the Justice Department and the Department of Homeland Security. Herridge joined FNC in 1996 as a London-based correspondent.

Pamela K. Browne is Senior Executive Producer at the FOX News Channel (FNC) and is Director of Long-Form Series and Specials. Her journalism has been recognized with several awards. Browne first joined FOX in 1997 to launch the news magazine "Fox Files" and later, "War Stories."

Mail on Sunday
Inside China's Bif Brother HQ
Sunday, 02 October 2016
Byline: George Knowles

about their daily lives in airports, government buildings, sports stadiums, high streets and stations. Hikvision, a company controlled by the Chinese government, was recently revealed to be Britain's biggest supplier of CCTV equipment, raising fears its internet-linked cameras could be hacked from Beijing at the touch of a button.

Last week, undercover Mail on Sunday reporters posed as businessmen to infiltrate its headquarters in the 'surveillance city' of Hangzhou in eastern China, to investigate its activities.

What they found will raise fresh cause for concern about a company whose growing influence in the UK has already been questioned by former MI6 officers and Security Ministers. Far from being the independently run business it claims to be in its customer-friendly marketing, Hikvision is controlled by China's ruling Communist Party.

Hikvision is central to the government's Orwellian programme to spy on its 1.3 billion citizens, and is inextricably linked to the totalitarian crackdown on those considered 'enemies of the state'.

More worryingly, Hikvision vice-president Pu Shiliang, 38, is also technical leader of a key laboratory at the Ministry of Public Security, the feared body that has been accused of the extrajudicial arrest and detention of thousands of lawyers, activists and perceived government opponents within China every year.

Hikvision's high- tech CCTV systems can 'see in the dark', track vehicles, and count the number of people entering and leaving a building, as well as boasting unparalleled 'face-tracking' technology.

They are even able identify a person by their gait.

These capacities enable the Chinese authorities to track dissidents, activists and human-rights campaigners, who are routinely rounded up and detained.

Last night, Lord West of Spithead, a Security Minister under Labour, said: 'We know very well that the Chinese hack Western systems on a massive scale to get intellectual property, but this is even more

worrying. If these cameras were in an office, they could see all the paperwork and get names of employees.

'What I've been pushing for is for the Government to set up a group that looks at the implications of all these decisions, and that should include the security agencies.

'The Chinese are hacking on a massive scale and if people do that, it's only right that we look at the implications.

'Yes, we want to trade with them, but people have to play by certain rules.'

Hikvision has been bankrolled to the tune of billions of pounds from Beijing, using the funding to sell CCTV systems at what critics claim are below market prices, and enabling it to become the world's biggest video surveillance system company in under a decade.

But until now, no one has seen behind the darkened glass windows of its headquarters in Hangzhou.

The Mail on Sunday was shown surveillance systems capable of singling out 'targets' in crowds within seconds by studying their faces and gait. Officials candidly told us their cameras in cities across China are controlled by the government which used them to track wanted people on a vast database of 'bad guys'.

They also told us government officials used the G20 summit in Hangzhou last month, attended by Barack Obama, Angela Merkel and Theresa May, to test the system's latest people-watching capabilities.

The China-wide project using products made by Hikvision and other smaller technology companies is called Skynet - the same name as the malignant Artificial Intelligence system bent on destroying humanity in the Terminator films.

And while Hikvision tells customers Skynet is an anti-crime initiative, government policy documents declare that its primary aim is to prevent public protests and 'find and control hostile forces' threatening China's repressive one-party state.

The revelations raise uncomfortable questions over whether Hikvision - now the biggest security camera provider in Britain with 20 per cent of the market - should be allowed unfettered access to the UK, and why it has never been subjected to security checks.

Experts fear Hikvision's internet-linked surveillance systems could potentially be remotely hacked from China through so-called 'back door' loopholes and used to track dissidents and human rights campaigners seeking refuge in the UK.

Nigel Inkster, a former deputy chief of MI6, said: 'There's probably a good case for a government look at this - who controls or has access to significant amounts of our national infrastructure.'

The firm's systems are in use on the London Underground network and in city centre surveillance in Salford, Manchester, and Hammersmith and Fulham in London, including at Chelsea Football Club.

Managers at Hikvision agreed to give us a tour of the research and development facilities, apparently keen to drum up more orders from overseas clients. In a suite of showrooms, we were shown surveillance cameras capable of seeing through fog and dark, and systems that can read vehicle number plates. The systems' advanced technology can also give accurate estimates of a target's age, sex and height.

'We have many customers in Britain now,' a company official told us. 'It is one of our biggest overseas markets after the US.'

Hikvision, which has 17,000 employees, says its urban surveillance systems target criminals and terrorists. 'We call it our safe city project,' the official said. 'Our cameras help to make a better world, a better city. If someone has committed a crime and walks across this camera area they will be identified from the database and the information will be instantly sent to the police.'

But a government document on Skynet issued in 2005 stated that its main aim was not to prevent normal crime but to maintain 'social stability... find out and control hostile forces' and to 'prevent mass disturbances in public areas'.

In an attempt to address privacy concerns, the official added: 'We just provide the cameras. We do not use the database ourselves, so people's privacy is protected. It is the government that controls the cameras and the database.'

China's leader Xi Jinping - who has led a ruthless crackdown on dissidents since his appointment in 2013 - visited Hikvision's HQ last year, praising its work and applauding the company for having a workforce with an average age of just 28.

Despite claiming on its website to be 'an independent and publicly traded corporation', Hikvision is in fact owned by Chinese Electronic Technology Corporation, a government body tasked with developing electronic systems for military and civilian use, including developing software to collate data on the jobs, hobbies, consumption habits and other behaviour of citizens to identify 'terrorists'.

As it rapidly expands its global presence, Hikvision has been generously bankrolled by Chinese state banks, which critics say give it an unfair commercial edge. It received £2.4 billion from China Development Bank in December and a further £2.3 billion loan from the Export-Import Bank of China in August, both of which are controlled by the government.

Weeks before our visit, Hangzhou hosted the G20 summit and tens of thousands of Hikvision surveillance cameras were put in place on key road junctions and buildings. Every taxi and bus also had

miniature security cameras installed. Today, there are an estimated 600,000 CCTV cameras in Hangzhou - one for every ten residents - making it one of the world's most watched cities along with the capital Beijing, which state media boasts is now '100 per cent covered' by surveillance cameras.

'You can be watched anywhere you go in Hangzhou,' the company official told us, adding that the G20 was used to test the efficiency of the latest Skynet systems. 'It was like an experiment,' he said.

The Chinese government's bid to expand Skynet reflects its paranoid determination to wipe out any opposition to the Communist Party as its economy stutters.

In the north-eastern city of Changchun, there was an outcry in 2013 when hundreds of thousands of surveillance cameras failed to find any trace of a car stolen from outside a supermarket with a sleeping two-year-old baby boy in the back. The boy was later found murdered.

'Skynet is useless. It isn't for public protection - it is just for following dissidents,' one furious resident said on an online forum.

Last night, Sir Malcolm Rifkind, former chairman of Parliament's Intelligence and Security Committee, said: 'There's clearly going to be a series of these Chinese-related projects and some may or may not have national security implications. There's going to be a need for a more joined-up strategy.

'You can't automatically say all business with China is dangerous but the security agencies can give expert judgment on the technical possibilities of another government accessing systems.'

John Honovich, head of the surveillance industry monitor IPVM, said the systems developed by Hikvision gave the Chinese government 'a powerful means to monitor and suppress any opposition to the party'.

He said that Hikvision was being heavily funded by China's state banks in a push to give it global dominance, allowing it to undercut rivals and sell systems overseas at relatively low prices.

'The overall strategic goal is to maximise market share, even at the expense of losses,' he added.

Mr Honovich advised local and national governments not to use Hikvision products at all, arguing: 'The risks of using products manufactured by the Chinese government are simply too high.'

WE CAN SEE YOU...

Workers inspect a bank of monitors at Hikvision's headquarters in Hangzhou, the surveillance capital of the world with 600,000 cameras such as the one above. Its software - shown in action, right - can identify faces and even a person's gait. The Chinese authorities have used this technology to identify dissidents at a glance and place them in long-term detention.

Globe and Mail
How Ottawa revived Canada's most controversial privacy issue
Wednesday, 05 October 2016
Byline: Michael Geist
Section: oped

The controversial issue of lawful access rules, which address questions of police access to Internet subscriber information and the interception capabilities at Canadian telecommunications companies, has long been played down by Canadian governments.
When the policy proposals first emerged in the early 2000s, the Liberal government focused on the anti-terrorism and anti-spam benefits. Subsequent Conservative proposals promoted the ability to combat child pornography and, most recently, cyberbullying.

Yet when the Conservatives passed lawful access legislation in late 2014, it seemed that more than a decade of debate had delivered a typical Canadian compromise.

The new legislation eliminated liability concerns for Internet service providers that voluntarily disclose basic subscriber information and created a series of new police powers to require access to, and preservation of, digital data.

The law faced some criticism, but more contentious proposals involving mandatory warrant-less disclosure of personal information and government-prescribed surveillance capabilities for telecom networks were not included.

Moreover, the Supreme Court of Canada ruled in the R v. Spencer case in June, 2014, that there was a reasonable expectation of privacy in subscriber information such that a warrant is required for disclosure in most circumstances.

Notwithstanding the legislative resolution and renewed legal certainty, Public Safety Minister Ralph Goodale has quietly revived the lawful access debate with a public consultation that raises the prospect of new rules that would effectively scrap the 2014 compromise.

Ironically, the focus this time is the public's demand for amendments to Bill C-51, the Conservatives' anti- terrorism law that sparked widespread criticism and calls for reform during last year's election campaign.

In other words, the balance of Canadian privacy is being put at risk by a policy initiative the purports to fix privacy.

The Public Safety consultation skips over the years of lawful access debate by putting everything back on the table, acknowledging that the law was updated less than 24 months ago but suggesting that more change may be needed.

For example, it implies that the "lack of consistent and reliable technical intercept capability on domestic telecommunications networks" presents a risk to law-enforcement investigations.

Yet left unsaid is that the prior proposed solutions in the form of government- mandated interception capabilities were rejected because of the enormous cost, inconsistent implementation and likely ineffectiveness of standards that would exempt many smaller providers.

The consultation also renews the possibility of easier access to basic subscriber information. Even after the Spencer court decision, transparency reports from many of Canada's largest telecom companies indicate that law enforcement still regularly obtains access to subscriber information.

The current approach strikes a balance that reflects the need for access for investigative purposes and the privacy protections to which all Canadians are entitled.

The consultation hints that changes to the basic subscriber information access system are coming with an emphasis on "the needs of law enforcement and national security agencies and the impact of those measures on industry" before any reference to privacy law.

In fact, Mr. Goodale places another controversial issue on the policy table, noting that encryption technologies are "vital to cybersecurity, e-commerce, data and intellectual property protection, and the commercial interests of the communications industry" but lamenting that those same technologies can also be used by criminals and terrorists.

Given its widespread use and commercial importance, few countries have imposed decryption requirements. However, this year's controversy involving access to data on an Apple iPhone owned by one of the San Bernardino, Calif., shooters revived the debate over access to encrypted communications, and the consultation asks Canadians to comment on the circumstances under which law enforcement should be permitted to compel decryption.

The consultation remains open until Dec. 1, but the message from the government is clear: The cost of changing Bill C-51 comes with a significant privacy price.

The anti-terrorism provisions that sparked concern will be examined, but so too will be lawful access rules that have enormous implications for Canadian business, law enforcement and the broader public.

Michael Geist holds the Canada Research Chair in Internet and E-commerce Law at the University of Ottawa, Faculty of Law.

Ottawa Citizen
StatCan's new head likes move to SSC

Wednesday, 05 October 2016
Byline: Tom Spears

Ottawa - Canada's new chief statistician has only good things to say about his agency's move to Shared Services Canada, almost three weeks after the former chief statistician called the situation "really damaging" and quit.
In September, Wayne R. Smith said the centralizing of computer services by SSC threatens Statistics Canada's ability to do good work.

On Tuesday, Anil Arora, the new head of StatCan, said he looks forward to improved data protection once Shared Services provides the IT infrastructure for his department.

"We have partnerships with service providers and always have had, for decades," Arora said in an interview.

"This is another partnership. It's an important partnership for us" that requires robust and secure infrastructure to handle massive amounts of data.

"Look, there are all sorts of risks that we manage on a daily basis," and StatCan is good at adapting and making contingency plans, he said.

"That (the transfer to SSC) is one additional risk that obviously we have to manage, and I have got nothing but co-operation from Shared Services Canada in understanding what our business is like and in working with us. So we are working closely with them" to look at capacity demands and ensure the infrastructure will support growing future demands with safeguards on privacy, he said.

"We have to do our share, and they have to be held accountable to do their share.

"I've got nothing but positive feedback that we are going to be able to work collaboratively."

StatCan also stands to gain from the SSC changes because there will be one central computer system to keep safe and up to date, which is "a lot better protection than if we have to worry about 40 disparate systems."

"I have the utmost respect for Wayne," he said, adding that Smith deserves credit for "successfully turning the census back to its mandatory long form" and other work. The recent census "is probably the best collection (of data) that we have seen."

"Wayne has his views, and he has made them known publicly.

"My job is to ensure that we continue to move forward, and I have my own style, my own way of doing things ... To me, it's really about the energy of the people that work here and the collaborative nature in which we are going to move forward."

Arora said StatCan has an "exciting and an ambitious agenda" and staff there "are really pumped" about the future.

Arora spent 21 years at StatCan and was assistant chief statistician when he left 6½ years ago for Natural Resources Canada and later Health Canada.

NPR
Amid Deteriorating U.S.-Russia Relations, Questions Grow About Cyberwar
Wednesday, 05 October 2016
Byline: Mary Louise Kelly

Washington - Just when you thought U.S.-Russia relations couldn't get worse, diplomatic deals on both Syria and nuclear security fell apart this week.
Moscow went first, announcing that it was pulling out of a landmark agreement on plutonium. Russia's President Vladimir Putin blamed "unfriendly actions" by the United States.

Hours later, Washington said it was breaking off talks on a ceasefire in Syria. "This is not a decision that was taken lightly," State Department spokesman John Kirby wrote in a statement. "Unfortunately, Russia failed to live up to its own commitments."

Moscow and Washington aren't cooperating on much of anything these days. And that prompts a question: What might come next, in the way of cyberattacks?

Russia is suspect-in-chief for recent attacks on targets ranging from the Democratic National Committee to a former U.S. NATO commander to former Secretary of State Colin Powell.

Rob Knake, who until last year served as director of cybersecurity policy for the National Security Council, says the toxic atmosphere might open the door to the U.S. retaliating. Until recently, Knake says, "We would say we want Russia's help on Syria. We want Russia's help on nukes. We want Russia's help on North Korea. Now, we've taken at least two of those issues off the table."

His point: if Russia and the U.S. aren't cooperating anyway, there may be less of a downside to hitting back on the cyber front. On the flip side, Knake argues, Russia may also feel less constrained.

"If they don't have an interest in cooperating with the U.S. in Syria, they may feel free to unleash the kind of attacks that they have yet kept on hold," he says. He sees a real risk of tit-for-tat retaliation spiraling out of control.

Angela Stent, who's watched Russia for many years from perches at the National Intelligence Council and now at Georgetown University, takes a different view, though she agrees this marks an exceptionally dangerous period in U.S.-Russia relations.

"This is the lowest point -- it's the worst relationship -- since, I would say, before Gorbachev came to power," she says, meaning all the way back to the 1980s, before Mikhail Gorbachev took over as the Soviet Union's head of state.

But Stent is not persuaded this low point will translate to gloves-off, bare-knuckle fighting in the cyber arena. That's because Moscow and Washington still share common interests -- including Syria, where Russia and the U.S. are still working together to coordinate counterterrorism operations.

Still, Stent says, Russia will not stop trying to provoke the U.S. with cyber intrusions.

"I think the Kremlin concluded some time ago that this was a lame-duck administration," she says. "And that this was the time to get whatever advantages they can. Because they don't know what the next president's going to do."

Meanwhile, President Obama and his advisers continue to avoid publicly naming and blaming Russia. They cite the ongoing FBI-led investigation into recent hacks.

CIA director John Brennan went about as far as any administration official has, in front of a crowd last week at the Washington Ideas Forum.

Asked whether Russia is trying to hack the U.S. election, Brennan replied: "What we do at [the] CIA is to look at a country's capabilities, look at their intent, look at things that they have done in the past, and determine whether something that certainly looks like a duck, smells like a duck and flies like a duck, whether it's a duck or not."

The question now is whether -- and how -- Washington decides to hunt.

Washington Post
Yahoo scanned all of its users' incoming emails on behalf of U.S. intelligence officials
Wednesday, 05 October 2016
Byline: Andrea Peterson

Washington - Yahoo in April of last year began secretly scanning the incoming emails of its hundreds of millions of users to comply with an order from the U.S. intelligence community, a move that prompted at least two company officials to leave, according to a former Yahoo employee familiar with the matter.

The company's decision not to fight the order from intelligence officials caused Yahoo's then-chief information security officer Alex Stamos to resign last year -- and at least one other security staffer left the company -- due to ethical concerns about the surveillance program, according to the person, who spoke on the condition of anonymity because the matter was confidential. Reuters, citing unnamed former employees, first reported the news Tuesday.

The government's demand to scan email in real time alarmed privacy advocates, as did Yahoo's compliance with such a broad order. Patrick Toomey, a staff attorney with the American Civil Liberties Union, called the order "unprecedented and unconstitutional."

"It is deeply disappointing that Yahoo declined to challenge this sweeping surveillance order, because customers are counting on technology companies to stand up to novel spying demands in court," he said in a statement.

Google, which runs Gmail, said in a statement: "We've never received such a request, but if we did, our response would be simple: 'no way'." Microsoft, another major email provider, said, "We have never engaged in the secret scanning of email traffic like what has been reported today about Yahoo." Apple, in a statement said, "We have never received a request of this type. If we were to receive one, we would oppose it in court."

It was unclear which intelligence agency directed Yahoo to scan emails, the person familiar with the matter said. It's also unknown what the government officials were looking for and what, if any, data Yahoo turned over to the government, the person said. The Office of the Director of National Intelligence did not respond to a request for comment.

"Yahoo is a law abiding company, and complies with the laws of the United States," the company said in a statement.

The company has fought a previous government request for data. In 2007, Yahoo unsuccessfully argued as unconstitutional an intelligence community demand that it hand over user communications to and from foreign targets without individual search warrants.

The challenge was heard in the secretive Foreign Intelligence Surveillance Court and some details about the case have remained under seal. But documents declassified in 2014 showed that the government threatened Yahoo with a massive $250,000 per day fine if it did not comply.

But Yahoo chief executive Marissa Mayer's decision to obey the order last year upset Stamos and some other senior executives, according to Reuters. Instead of looping in the security team, Mayer turned to the Yahoo's email engineers to develop the software, Reuters reported. That decision led to a programming error that left all Yahoo email vulnerable to hackers, the former Yahoo employee said.

When reached via Twitter direct message, Stamos, who is now Facebook's chief security officer, said, "I'm not commenting at all."

New York Times
Federal Tactics in Data Pursuit Are Excessive, Tech Firms Say
Wednesday, 05 October 2016
Byline: Nicole Perlroth, Katie Benner

San Francisco - It has been six months since the Justice Department backed off on demands that Apple help the F.B.I. break the security of a locked iPhone.
But the government has not given up the fight with the tech industry. Open Whisper Systems, a maker of a widely used encryption app called Signal, received a subpoena in the first half of the year for subscriber information and other details associated with two phone numbers that came up in a federal grand jury investigation in Virginia.

The subpoena arrived with a court order that said Open Whisper Systems was not allowed to tell anyone about the information request for one year.

Technology companies contend that court-imposed gag orders are being used too often by law enforcement and that they violate the Bill of Rights. The companies also complain that law enforcement officials are casting a wide net over online communications -- often too wide -- in their investigations.

Justice Department officials, for their part, argue that these gag orders are necessary to protect developing cases and to avoid tipping off potential targets. The officials say that they are simply following leads where they take them.

Through a spokesman, the Justice Department declined to comment on the case.

The information request made of Open Whisper Systems is particularly sensitive, since its encryption app is used around the world, and it is often recommended to journalists and human rights activists.

Microsoft sued the Justice Department over the gag order practice in April, arguing that law enforcement was relying on these orders too often. Specifically, the software giant said the gag orders violate the Fourth Amendment right of its customers to know if the government searches or seizes their property and also the company's First Amendment right to speak to its customers.

Microsoft also complained that the orders often came without time limits, unlike the Open Whisper Systems order. Dozens of other technology, media and civil liberties groups filed briefs supporting Microsoft last month, and the case is pending.

Part of the gag order on Open Whisper Systems was lifted after a court challenge by the American Civil Liberties Union, and redacted versions of documents related to the information request were made public last week. But the small San Francisco company was still not allowed to tell specific account holders about the investigation.

The documents made public show that the government asked Open Whisper Systems to turn over data associated with two telephone numbers, including web browsing histories and data stored in the tracking "cookies" of the web browsers attached to those accounts. But one of Signal's biggest draws is that it does not collect most of that information.

"The Signal service was designed to minimize the data we retain," said Moxie Marlinspike, the founder of Open Whisper Systems. Mr. Marlinspike said Signal uses a technology called end-to-end encryption that kept the service from gaining access to the contents of its users' messages. The company also does not store information on those with whom its users are communicating.

Civil liberties lawyers argue the Justice Department request fell well outside the bounds of what is typically covered by a subpoena, including basic subscriber information. Additional information, such as computer logs or content, would require a search warrant under the 1986 Electronic Communications Privacy Act.

"The Justice Department is pushing the envelope," said Jennifer Granick, director of civil liberties at the Stanford Law School Center for Internet and Society. Big companies like Apple and Microsoft have the wherewithal to push back, she said. But smaller companies may cave, rather than risk an expensive fight.

The Justice Department came to Open Whisper Systems with a menu of information needs, including subscriber details, addresses, telephone numbers, email addresses and method of payment. The request went on to demand information on internet addresses, browsers and internet providers that the account holders could have used, according to court records.

One of the phone numbers the government was investigating was not a Signal user after all. For the other phone number, Open Whisper Systems turned over the only pieces of data it could: the time the user's account had been created and the last time it had connected to the service -- far less than the government sought.

In other circumstances, the government has tried to force companies via court order to re-engineer their services to collect missing pieces of information, as it did with Apple earlier this year and in a similar case in 2013 against Lavabit, a small encrypted messaging service used by the former defense contractor Edward J. Snowden.

The government did not make that request of Open Whisper Systems. "They need to pick those cases carefully," Ms. Granick said. "They are only picking cases where they think they're going to have the people on their side."

The Justice Department and F.B.I. tried to force Apple to break its own software security in the case of an iPhone used by a gunman in last year's San Bernardino terrorist attacks, she said.

Companies are having some success in getting courts to lift gag orders. Last year, Nicholas Merrill, the owner of a now-defunct internet service provider, got a gag order lifted, though it took more than a decade. After the court decision in Mr. Merrill's case, a federal judge in the Eastern District of New York denied gag orders in more than a dozen cases related to Facebook subpoenas last May. And in June, Yahoo was successful in getting a court to lift gag orders on a number of law enforcement information requests.

"Gag orders should be used in exceptional cases," said Brett M. Kaufman, the staff attorney with the A.C.L.U. who represented Open Whisper Systems. "This one demonstrates that the exception has become the rule in routine proceedings."

London Times
Cardiff man 'hid data on cufflink for use in terrorism'
Wednesday, 05 October 2016
Byline: John Simpson

London - A suspected member of Islamic State is accused of giving terror training on encrypted technology and secreting a computer program on a removable hard drive hidden in a cufflink in pursuit of its campaign of terrorism.
Samata Ullah, 33, was charged last night with six terror offences including membership of Islamic State -- a proscribed organisation -- and downloading books on missile guidance systems for terrorist purposes.

Mr Ullah, of Cardiff, was also charged with directing "an organisation which is concerned in the commission of acts of terrorism" and in relation to giving instruction on the use of encrypted technology on a blog.

The charges include the allegation that Mr Ullah had a "USB cufflink that had an operating system loaded on to it for a purpose connected with the commission, preparation or instigation of terrorism" and the possession of "a book about guided missiles and a PDF version of a book about advanced missile guidance" for the same purpose. All the charges relate to offences allegedly committed on or before September 22. Mr Ullah is expected to appear in custody at Westminster magistrates' court today.

Mr Ullah lives in the Grangetown area of Cardiff with his family, who run the Cardiff Commercial Cleaning company. Neighbours have said that he regularly works out at a gym.

Announcing the charges, a spokesman for Scotland Yard said: "The arrest, which took place in the street in Cardiff by officers from the Counter Terrorism Command was pre-planned and as a result of a pro-active investigation by the Counter Terrorism Command supported by the Wales extremism and counterterrorism unit."

New York Times
Assange Sets New Schedule of Disclosures
Wednesday, 05 October 2016
Byline: Melissa Eddy

Berlin - Julian Assange, the founder of WikiLeaks, promised on Tuesday to release "significant material" over the next 10 weeks about arms, Google, mass surveillance, oil, the United States election and war. Speaking via a video link at a news conference in Berlin to mark a decade since the inception of WikiLeaks, Mr. Assange vowed that his organization would continue to provide a platform for the release of classified documents held by the United States and by other governments and institutions in positions of global power.

"We hope to be publishing every week for the next 10 weeks, we have on schedule, and it's a very hard schedule, all the U.S. election-related documents to come out before Nov. 8," said Mr. Assange, who made his announcement from the Ecuadorean Embassy in London, where he has been living since 2012. "Our upcoming series includes significant material on war, arms, oil, Google, the U.S. elections and myself."

WikiLeaks used the occasion of its 10th anniversary to trumpet some of its prominent releases of information, including documents about the United States detention camp at Guantánamo Bay, Cuba; files about the wars in Iraq and in Afghanistan; United States diplomatic cables; and Democratic Party emails that were made public on the eve of the party's convention in Philadelphia.

The remarks from Mr. Assange disappointed many followers of WikiLeaks in the United States, who had stayed up hoping to hear information relevant to the presidential election.

Although Mr. Assange promised to release such documents before the election on Nov. 8, he said, "If we are going to make a major publication, we don't do it at 3 a.m." in the United States.

He dismissed speculation that the documents related to the United States election would contain information intended to damage the candidacy of Hillary Clinton, the Democratic nominee. The idea that "we intend to harm Hillary Clinton, or I intend to harm Hillary Clinton, or I don't like Hillary Clinton, all those are false," Mr. Assange said.

Mr. Assange laughed when he was asked whether he felt any personal affinity for her Republican rival, Donald J. Trump, saying that he felt "personal affinity for all human beings." He explained that he felt sorry for both Mrs. Clinton and Mr. Trump, given that "these are two people who are tormented by their ambitions."

Mr. Assange had been scheduled to make the announcement from the balcony of the embassy where he has been staying since Ecuador granted him political asylum, but he changed that plan at the last minute because of security reasons. He declined to give further details about those concerns.

Mr. Assange sought refuge after Sweden said it wanted him for questioning on allegations of rape, an accusation that he has denied. He feared that if he were sent to Sweden, he would then be extradited to the United States to face espionage charges.

Times of India
7,000 Indian sites hacked, claim Pak rookies
Wednesday, 05 October 2016
Byline: Chethan Kumar

Bengaluru - A group of Pakistani hackers has said they have hacked 7,070 Indian websites and released a list of names early on Tuesday. The hackers are no experts, say cyber security specialists, but are 'script kiddies' or those who don't write their own code and use existing scripts to hack into websites.
Each of the websites has the logo of the hacking group, Pakistan Haxors Crew, and a song "Ae watan tera ishara aagaya, ar sipahi ko pukar aagaya..." (Oh nation, we've received your signal, every soldier has got his call(ing)..." begins to play with a scroll that reads, "Tum ne socha tha, hum ne kar dikhaya" (You thought, we've done it). The group has in the past hacked websites of Tata Motors, AIADMK and Taj Mahal, and on Tuesday, said, "There is more to come."

While most of them are non-government websites, experts say this indicates how vulnerable Indian websites are to such threats. According to information from the communication and information technology ministry, 1,490 government websites have been hacked between January, 2010, and December, 2015. The data for this year is yet to be compiled.

"I've seen their post. They are not even proper hackers. They are what we call script kiddies, people who use existing computer scripts to hack into computers as they lack the expertise to write their own," says Mirza Faizan Asad, legal head, Global Cyber Security Response Team. And, if people who cannot write their own code are hacking into websites, the damage by real hackers would be greater.

One of the worst instances of the hacking of a government website was in August, 2013. The Electronics Corporation of India Ltd (ECIL) website was hacked by 'PhrozenMyst', who allegedly stole sensitive data pertaining to the Indian Space Research Organisation (Isro) and Bhabha Atomic Research Centre (Barc). The hacking of government websites saw a decline from 2013. However, in 2015, the number went up.

Aravind Prakash, associate professor at Binghamton University, US, said, "There is always a school of thought that will argue, 'why can't we buy software'? But one must understand that you cannot trust these companies that we buy from to provide a vulnerability- free software or system. Intrusion or hacking happens when there are vulnerabilities."

Reuters
Yahoo secretly scanned customer emails for U.S. intelligence - sources
Tuesday, 04 October 2016
Byline: Joseph Menn

San Francisco - Yahoo Inc last year secretly built a custom software program to search all of its customers' incoming emails for specific information provided by U.S. intelligence officials, according to people familiar with the matter.
The company complied with a classified U.S. government directive, scanning hundreds of millions of Yahoo Mail accounts at the behest of the National Security Agency or FBI, said two former employees and a third person apprised of the events.

Some surveillance experts said this represents the first case to surface of a U.S. Internet company agreeing to a spy agency's demand by searching all arriving messages, as opposed to examining stored messages or scanning a small number of accounts in real time.

It is not known what information intelligence officials were looking for, only that they wanted Yahoo to search for a set of characters. That could mean a phrase in an email or an attachment, said the sources, who did not want to be identified.

Reuters was unable to determine what data Yahoo may have handed over, if any, and if intelligence officials had approached other email providers besides Yahoo with this kind of request.

According to the two former employees, Yahoo Chief Executive Marissa Mayer's decision to obey the directive roiled some senior executives and led to the June 2015 departure of Chief Information Security Officer Alex Stamos, who now holds the top security job at Facebook Inc."Yahoo is a law abiding company, and complies with the laws of the United States," the company said in a brief statement in response to Reuters questions about the demand. Yahoo declined any further comment.

Through a Facebook spokesman, Stamos declined a request for an interview.

The NSA referred questions to the Office of the Director of National Intelligence, which declined to comment.

The demand to search Yahoo Mail accounts came in the form of a classified directive sent to the company's legal team, according to the three people familiar with the matter.

U.S. phone and Internet companies are known to have handed over bulk customer data to intelligence agencies. But some former government officials and private surveillance experts said they had not previously seen either such a broad directive for real-time Web collection or one that required the creation of a new computer program.

"I've never seen that, a wiretap in real time on a 'selector,'" said Albert Gidari, a lawyer who represented phone and Internet companies on surveillance issues for 20 years before moving to Stanford University this year. A selector refers to a type of search term used to zero in on specific information.

"It would be really difficult for a provider to do that," he added.

Experts said it was likely that the NSA or FBI had approached other Internet companies with the same demand, since they evidently did not know what email accounts were being used by the target. The NSA usually makes requests for domestic surveillance through the FBI, so it is hard to know which agency is seeking the information.

Reuters was unable to confirm whether the 2015 demand went to other companies, or if any complied.

Alphabet Inc's Google and Microsoft Corp, two major U.S. email service providers, did not respond to requests for comment.

CHALLENGING THE NSA

Under laws including the 2008 amendments to the Foreign Intelligence Surveillance Act, intelligence agencies can ask U.S. phone and Internet companies to provide customer data to aid foreign intelligence-gathering efforts for a variety of reasons, including prevention of terrorist attacks.

Disclosures by former NSA contractor Edward Snowden and others have exposed the extent of electronic surveillance and led U.S. authorities to modestly scale back some of the programs, in part to protect privacy rights.

Companies including Yahoo have challenged some classified surveillance before the Foreign Intelligence Surveillance Court, a secret tribunal.

Some FISA experts said Yahoo could have tried to fight last year's directive on at least two grounds: the breadth of the demand and the necessity of writing a special program to search all customers' emails in transit.

Apple Inc made a similar argument earlier this year when it refused to create a special program to break into an encrypted iPhone used in the 2015 San Bernardino massacre. The FBI dropped the case after it unlocked the phone with the help of a third party, so no precedent was set.

Other FISA experts defended Yahoo's decision to comply, saying nothing prohibited the surveillance court from ordering a search for a specific term instead of a specific account. So-called "upstream" bulk collection from phone carriers based on content was found to be legal, they said, and the same logic could apply to Web companies' mail.

As tech companies become better at encrypting data, they are likely to face more such requests from spy agencies.

Former NSA General Counsel Stewart Baker said email providers "have the power to encrypt it all, and with that comes added responsibility to do some of the work that had been done by the intelligence agencies."

SECRET SIPHONING PROGRAM

Mayer and other executives ultimately decided to comply with the directive last year rather than fight it, in part because they thought they would lose, said the people familiar with the matter.

Yahoo in 2007 had fought a FISA demand that it conduct searches on specific email accounts without a court-approved warrant. Details of the case remain sealed, but a partially redacted published opinion showed Yahoo's challenge was unsuccessful.

Some Yahoo employees were upset about the decision not to contest the more recent directive and thought the company could have prevailed, the sources said.

They were also upset that Mayer and Yahoo General Counsel Ron Bell did not involve the company's security team in the process, instead asking Yahoo's email engineers to write a program to siphon off messages containing the character string the spies sought and store them for remote retrieval, according to the sources.

The sources said the program was discovered by Yahoo's security team in May 2015, within weeks of its installation. The security team initially thought hackers had broken in.

When Stamos found out that Mayer had authorized the program, he resigned as chief information security officer and told his subordinates that he had been left out of a decision that hurt users' security, the sources said. Due to a programming flaw, he told them hackers could have accessed the stored emails.

Stamos's announcement in June 2015 that he had joined Facebook did not mention any problems with Yahoo. (bit.ly/2dL003k)

In a separate incident, Yahoo last month said "state-sponsored" hackers had gained access to 500 million customer accounts in 2014. The revelations have brought new scrutiny to Yahoo's security practices as the company tries to complete a deal to sell its core business to Verizon Communications Inc for $4.8 billion.

Le Monde
Le big data au secours de la lutte antiblanchiment
Wednesday, 05 October 2016
Byline: Sandrine Cassini

Paris - La Française des jeux et IBM vont s'appuyer sur l'analyse de données pour traquer la fraude Comment lutter contre le blanchiment d'argent sale? A l'image des banques, la Française des jeux (FDJ) est tenue à une obligation de vigilance. Car son réseau, ses jeux de grattage et ses paris sportifs n'échappent pas aux opérations frauduleuses. Chaque année, elle détecte dans ses 32 000 points de vente pour 10 à 12 millions d'euros d'opérations suspectes, et remonte une centaine d'opérations à Tracfin, le service de renseignement rattaché à Bercy et chargé de la lutte contre le blanchiment de capitaux.

Pour la FDJ, qui réalise 14 milliards d'euros de chiffre d'affaires et 4 milliards de transactions annuelles, lutter contre ces fraudeurs revient à chercher une aiguille dans une botte de foin. Elle a donc donné le coup d'envoi à un partenariat avec IBM le 28 septembre. Objectif : utiliser le big data, l'analyse de données à grande échelle, pour détecter de manière plus efficace les comportements suspects.

" La plateforme brasse entre 80 et 100 critères par jour. Elle analyse des lieux, la fréquence des transactions, leur montant " , explique Xavier Etienne, directeur général adjoint chargé des technologies au sein de la FDJ. En test depuis un an, la nouvelle plateforme permet déjà d'identifier 20 % à 25 % de nouveaux schémas de fraudes. " Nous voulons passer moins de temps sur la recherche et mieux remonter les informations " , dit-il.

Rachat de tickets gagnants Globalement, les fraudeurs utilisent deux artifices pour blanchir des fonds. Le premier consiste à racheter en masse des tickets gagnants avec de l'argent sale et à les échanger dans un point de vente contre de l'argent propre. Autre subterfuge, le recours aux jeux faisant moins appel au hasard, mais plus à une certaine adresse, à l'image des paris sportifs. " Il peut y avoir des sommes très importantes misées sur une équipe gagnante, dans le seul but de blanchir de l'argent " , précise le directeur général adjoint.

La lutte contre le blanchiment n'est qu'une première étape. " Nous faisons avec la FDJ la recherche et développement commune pour explorer la mise en place de nouveaux services " , assure Marie-Noëlle

Muller, directrice des pôles publics d'IBM France. Prochaine étape, l'identification en amont des points de vente en difficulté, à partir du comportement des joueurs.

Canadian Press
Call for rules on armed drones highlights Canadian debate over such weapons
Thursday, 06 October 2016
Byline: Lee Berthiaume

OTTAWA _ Canada has joined dozens of other countries in calling for clearer rules around the sale and use of armed drones, even as the government debates whether the military should acquire such weapons.
The U.S. State Department on Wednesday released a joint declaration, signed by Canada and 44 other countries, laying out five general principles on the export and use of armed unmanned aerial vehicles, or UAVs.

They include emphasizing the importance of international law, compliance with existing arms-control laws and transparency about the use of drones.

The declaration is expected to be a starting point for establishing clear and definitive rules and standards to govern what is an increasingly common weapon used by militaries around the world.

"Our participation in this initiative complements Canada's membership in all four of the export-control regimes and our overall efforts in the legitimate trade in military goods," Global Affairs Canada spokeswoman Jessica Seguin said in a statement.

Yet while Canada has added its name to the declaration, it remains unclear if it will actually buy armed drones. This is despite more than a decade of research and calls for such weapons from senior military commanders.

Defence Minister Harjit Sajjan's spokeswoman, Jordan Owens, said the question of whether to acquire armed drones is among the issues being considered in the government's defence policy review, the results of which aren't expected until next year.

"This is very much a decision that rests with the government of Canada, but no decision has been made at this time," Owens said by email.

"As we do with any procurement of equipment, we are doing our due diligence to ensure any decision that is made will meet Canada's defence needs, now and into the future."

The Canadian military has operated UAVs in the past. French- and Israeli-made drones were used during the war in Afghanistan and the government announced in August that it was spending $14.2 million to buy five U.S. unmanned aircraft. But those have all been unarmed and used for surveillance.

The military has been kicking the tires on larger drone systems since the early 2000s, but has yet to get government approval to move forward. In the meantime, senior commanders have made no secret of their desire to obtain armed UAVs.

Speaking to reporters in March, chief of the defence staff Gen. Jonathan Vance said surveillance is important, "but we also want to be able to contribute to the strike.

"So I think it's important for the military force to have a range of options available to it," he said. "In my view there's little point in having a UAV that can see a danger but can't strike if it needs to."

Other officers, such as retired lieutenant-general Charles Bouchard, who commanded NATO's air and sea campaign in Libya in 2011, have also highlighted the benefits of armed drones. Bouchard is now head of defence giant Lockheed Martin's Canadian office.

Earlier this year, National Defence asked interested companies to submit information about what drones they would be able to provide to Canada. Among the requirements was "a weapons carrying and delivery capability in support of (Canadian Armed Forces) operations worldwide."

But Royal Canadian Air Force spokeswoman Lt.-Col. Holly Apostoliuk said the requirement was listed as a "secondary mission," and that the focus is on surveillance and the ability to operate in different parts of Canada, including the Arctic.

An actual competition is not expected until 2019, at the earliest.

Any move to acquire armed drones for the Canadian military is likely to stir controversy. Aside from concerns about dehumanizing war, some have questioned the accuracy of drone strikes.

The White House says 116 civilians have been killed in 473 drone attacks since U.S. President Barack Obama took office in 2009. But some estimates say the number could be as high as 800. One strike alone in eastern Afghanistan last week killed 15 civilians and injured 13 more.

Owens acknowledged the legal questions associated with using armed drones, but said "any UAV system acquired by Canada would be compliant with our domestic and international legal obligations and employed in a manner that is consistent with these obligations."

Motherboard
The Canadian Government's Plan to Sell New Spying Powers to Citizens
Thursday, 06 October 2016
Byline: Jordan Pearson

Canada's government is taking a forum for citizens to sound off about its spying powers and flipping it into an opportunity to sell Canadians on new and overbroad police capabilities, according to a new watchdog report.
In September, Trudeau's Liberals made good on a promise to open a public consultation on national security and released two documents, a green paper and a background document, explaining the issues at stake to Canadians at a time when the government is ramping up its efforts to thwart domestic terrorists. These included hot topics such as the difficulties police face when dealing with encrypted devices and issues surrounding data retention.

However, according to the watchdog report, the government's framing of the issues is selling Canadians on a police power that has been shot down again and again by the courts and the public: warrantless access to subscriber information from telecom companies.

"Successive federal governments have sought to legislatively enshrine a state power to access subscriber identification data from telecommunications companies," Citizen Lab researcher Christopher Parsons and Canadian Internet Policy and Public Interest Clinic staff lawyer Tamir Israel write in their report. "Such legislative initiatives would have facilitated access to such data on an indiscriminate basis and without any judicial authorization or control."

"All of these attempts have proven controversial and each has fallen in the face of public resistance," they continue. In 2014, the Supreme Court of Canada ruled that accessing subscriber information without a warrant constitutes an illegal search.

In its green paper, the government describes subscriber information as being akin to a phone book. However, subscriber information includes IP addresses, name, home address, phone number, email address, and mobile devices' IMSI number--much more information than is contained in your average phone book.

"Our laws on how information can be properly collected and then used in court as evidence were mostly written before the rapid pace of new technology became a consideration," the government's green paper states. Now, police worry about "slow and inconsistent access to basic subscriber information to help identify who was using a particular communications service at a particular time," the report states.

The idea of giving Canada's police and spying agencies access to subscriber information without a warrant was first raised in a consultation document in 2002, and was defeated in 2012 after being included in the failed Bill C-30, also known as the "Protecting Children from Internet Predators Act."

Most recently, in 2015, the Canadian Association of Chiefs of Police passed a resolution at their annual conference to lobby for warrantless, "real time" access to subscriber information.

Now, it seems, the federal government has moved from paedophiles to terrorists in its bid to convince the public that warrantless access to subscriber information is a good idea.

New Zealand Herald
Spark seeks details on US email scans
Thursday, 06 October 2016
Byline: Nicholas Jones

Wellington - Kiwi telco Spark is seeking clarification from Yahoo as to whether any of its customers had email searched at the behest of United States intelligence agencies.
According to an investigation by Reuters, Yahoo last year used a software program to search its customers' incoming email for specific information provided by US intelligence agencies.

That happened after the Yahoo complied with a classified US government demand, it was reported.

Spark is seeking more information, including whether Spark's Xtra Mail customers could have been affected. Yahoo hosts more than 800,000 accounts on behalf of Spark.

"At this time we are still seeking clarification from Yahoo if any Spark Xtra email customers are involved," a spokeswoman told the Herald.

Privacy Commissioner John Edwards said Spark was right to be making its own inquiries. "I would be concerned if these kinds of arrangements were occurring without a clear legal authority. But we haven't seen enough in the Reuters report to know the basis of it."

Edwards said there was a big difference between an intelligence agency asking a provider to scan all email accounts, and seeking access to a particular communication when there were legitimate law enforcement reasons to do so.

"They have no reason to believe that any individual is a suspect. They are just going across everything."
Spark will soon migrate its Xtra email accounts back to New Zealand, to be hosted by cloud email provider SMX.

Edwards said the Reuters report would fuel such moves worldwide.

"It really undermines confidence in the digital economy."

Last month, Spark contacted 131,000 Xtra customers about another scare, after hackers accessed hundreds of millions of Yahoo accounts in late 2014. They were told their accounts were potentially affected and to change their password.

The Spark spokeswoman said Yahoo had since advised there was no evidence Xtra accounts had been used for malicious activity.

The Daily Beast
NSA Thief Worked With Elite Hacker Squad
Thursday, 06 October 2016
Byline: Multiple reporters

Washington - The retired Navy officer arrested for allegedly removing highly classified information from the National Security Agency worked with the organization's elite computer hackers, who specialize in using computer code to penetrate the systems of foreign nations, according to a former colleague and the man's online resume.
Harold Thomas Martin, III, who goes by Hal, was also enrolled in a PhD program at the University of Maryland Baltimore County. The university has a partnership with the NSA, in which the agency helps develop curriculum for the school and agency employees can take classes there.

Martin worked with NSA's Tailored Access Operations unit, sources with knowledge of his background told The Daily Beast. In his LinkedIn resume, Martin says he worked as a "cyber engineering advisor" supporting "various cyber related initiatives" in the Defense Department and intelligence community.

Allen was employed by NSA contractor Booz Allen Hamilton. "When Booz Allen learned of the arrest of one of its employees by the FBI, we immediately reached out to the authorities to offer our total cooperation in their investigation, and we fired the employee," Craig Veith, a vice president with the company, said in a statement. "We continue to cooperate fully with the government on its investigation into this serious matter."

Martin was charged with two counts of mishandling classified information and theft of government property. According to the New York Times, which first reported his arrest, the FBI is investigating whether Martin stole classified computer codes that the NSA uses to break into foreign networks. The FBI discovered the material at Martin's home in Maryland.

Martin's case immediately drew comparisons to that of Edward Snowden, who was also working as a contractor for Booz Allen Hamilton when he stole classified documents that he gave to journalists. The NSA put in place so-called insider-threat detection programs after Snowden's leaks to catch future unauthorized disclosures. But it wasn't immediately clear whether those systems failed to spot Martin or if he removed the classified material before they were put in place.

Martin's lawyer told the Wall Street Journal "There is no evidence that Hal Martin intended to betray his country." He has also not been charged yet with espionage or attempting to provide the classified information to a third party or a foreign government.

Former intelligence officials, who said they aren't familiar with Martin's case, suggested he may have brought the material home to use as research for his PhD studies. "It's conceivable given what he was

working on that he might have used the [classified] material for research," a former official said, speaking on condition of anonymity.

The university's director of communications, Dinah Winnick, confirmed to The Daily Beast that Martin, 51, is a PhD student in the Information Systems program but said the school had no further comment.

It's not known whether Martin's PhD work related to his work at NSA, which focused on offensive cyber operations. But his description at the school's Interactive Systems Research Center said Martin was looking at "new methods for remote analysis of heterogeneous & cloud computing architectures." He presented a paper on the topic with his dissertation committee chair at a conference in Seattle in 2014.

His dissertation, currently in its fourth draft, according to a file on his personal homepage, is not publicly available. Members of Martin's dissertation committee did not return The Daily Beast's requests for comment.

According to Navy records, Martin served for twelve years -- four of them in the active component and the rest as a reservist. The highlight of his career appears to be his service on the USS Seattle, from April 1989 to July 1992. The Seattle, a fast combat support ship, was one of the first ships to arrive after Iraqi leader Saddam Hussein's forces invaded Kuwait in 1990.

Wilbur Trafton, the commander of the Seattle during the war to liberate Kuwait, told The Daily Beast that he doesn't remember the then-Lt. Martin. A second shipmate also said he couldn't recall Martin.

Martin's title at the time, Surface Warfare Officer, is a broad job description that reveals little about his work on the ship. The Seattle was decommissioned in March 2005.

Martin's ex-wife, Marina, declined to discuss her former husband.

CNBC
NSA has lost some terrorists because of encryption, its top lawyer says
Wednesday, 05 October 2016
Byline: Harriet Taylor

Cambridge - The NSA has lost some terrorists because of their adoption of strong encryption, but the agency is supportive of the use of the technology, it's top lawyer said Wednesday.
Glenn Gerstell, general counsel of the National Security Agency, made the comments at the Cambridge Cyber Summit at MIT in Cambridge, Massachusetts.

"We are big supporters of encryption," said Gerstell. "Encryption is more of a law enforcement issue."

He said the NSA sees ISIS terrorists using end-to-end encryption, and that has prevented the agency from finding out the key information about those bad actors.

The widespread availability of encryption technology requires the government to employ additional resources to monitor terrorists, said Gerstell. He declined to elaborate on specific sources and methods.

Privacy advocate Cindy Cohn, executive director of the Electronic Frontier Foundation, listed some of the methods the government may use when encryption blocks access to information shared by suspects: They install key loggers on devices to discover passwords, stop computers on their way to being shipped and install backdoors or send fake messages masquerading as popular services like Facebook to trick suspects to divulging passwords.

"We know they purchase vulnerabilities and don't tell the companies their systems are vulnerable," she said.

About 90 percent of the vulnerabilities the government discovers are in fact disclosed, but at times they choose not to share that information for national security reasons, said Gerstell.

The NSA is in an excellent position to assess cyberthreats given its tech chops, but the anonymity enabled by end-to-end encryption -- whose adoption is growing -- allows some people to get away with "mischief" and the barriers to entry for the use of this technology are "extremely low," he said.

Cybersecurity is the biggest threat the NSA will face over the next couple of decades, and the agency is very focused on combating cybercrime. It takes a multifaceted approach -- working hand in hand with the FBI and Department of Homeland Security to share threat information, and issuing bulletins to reach the public where appropriate, Gerstell said.

The conference is sponsored by CNBC, MIT and The Aspen Institute.

South China Morning Post
Snowden biopic to illuminate situation of asylum seekers (Canada)
Thursday, 06 October 2016
Byline: Raquel Carvalho

Beijing - Oliver Stone's Snowden film, which opens in Hong Kong cinemas today, has raised some concerns about the public exposure that those who sheltered the former US intelligence contractor in Hong Kong in 2013 are facing.
"I haven't seen the portrayal ... but am aware of some of the reports of the persons sheltering Mr Snowden," human rights lawyer Mark Daly said. "I think in very general terms it may shed some light on the situation of refugees in Hong Kong but the 'light' may not be welcomed by all," he noted.

Daly said that "usually, genuine asylum seekers would not wish to reveal their identities as this could expose them, or their families, to danger if returned to their countries of origin".

But he noted: "The issues are complex and perhaps raise further questions and concerns."

It emerged last month that Edward Snowden, a former National Security Agency contractor who leaked classified documents detailing the extent of electronic spying by the United States and other governments, took shelter in asylum seekers' homes during his stay in Hong Kong in June 2013. Their identities, including names and photos, appeared in the news over the past weeks.

Justice Centre advocacy officer Victoria Wisniewski Otero said although it is hard to predict the impact on the families who sheltered Snowden, the film might highlight the broader situation.

Robert Tibbo, one of the lawyers who assisted Snowden in Hong Kong, said there was no option but to reveal the identities of those who sheltered the former US intelligence contractor. "There are exactly eight refugees identified in the media and who are portrayed in the film ... There was no choice about the fact that they existed and sheltered Snowden as it is in the film," he said.

Tibbo noted that they knew the media would try to locate the three refugee families. "We did not want my other asylum seeking clients being questioned and harassed by the media or other people or organisations ... I did not want the three families to be living in fear," the lawyer told the South China Morning Post.

Revealing their identities before the film's release also provided an opportunity for them "to have control over their story". According to the Canadian barrister, "the identification of the three refugee families ... will certainly provide greater protection to them".

Tibbo said the film will "reveal that the refugees who sheltered and cared for Snowden were ordinary people who did the extraordinary. It will also "dispel the negative opinions the Hong Kong government and officials have made" and "thus improve the -image of the refugee community", he said.

Wall Street Journal
Firms Brace for More Hacks After Code Reveal
Thursday, 06 October 2016
Byline: Robert McMillan, Drew FitzGerald

New York - Internet companies are bracing for more trouble after hackers released the code behind one of the most powerful online attacks ever, which harnessed as many as one million internet-connected devices to knock a blogger offline.
The malicious software takes advantage of weak security on video recorders, routers and other internet-connected devices, taking control of the systems and forming them into a collection of attacking

machines, called a "botnet." It can then disable a victim's internet servers by flooding them with internet traffic.

The botnet code was released Friday -- apparently after a dispute between developers -- and is now available for anyone to download, meaning more attacks are likely. By Tuesday, it had infected about 300,000 devices, along with nearly one million affected using an earlier version of the software, according to Level 3 Communications Inc. Some machines were hijacked by both strains.

That has made networking engineers around the world nervous, said Paul Vixie, chief executive of Farsight Security Inc., who has helped developed some of the internet's core protocols. "The people who keep the internet running are either at the bar with stiff drinks in their hands or they're tearing their hair out because there is nothing they can do to stop this," he said.

The botnet software remotely connects to video recorders and routers, and then tries out default usernames and passwords until it gains control of the device. With nearly one million devices, a botnet theoretically could pump out an unprecedented 4 terabits-per-second computer attack, equivalent to streaming 800,000 high-definition movies simultaneously, according Fastly Inc., a company that sells networking services.

Level 3 said last week that cameras and video recorders made by China's Dahua Technology Co. were responsible for a large portion of the previous attacks. Dahua couldn't be reached for comment Tuesday, but the company last week said the vulnerability applied to internet-connected cameras with firmware dated before January 2015. It also advised users to upgrade the software on their devices and set strong passwords.

Big software makers like Microsoft Corp. have spent billions of dollars during the past two decades securing their software from hackers. But security experts say the makers of many internet-connected devices don't have the resources to do so.

Politico
DHS official: Half of U.S. states have sought help to thwart election hackers
Thursday, 06 October 2016
Byline: Darren Samuelson

Washington - Hacking threats have prompted 25 states so far to seek out the Obama administration's help in assessing vulnerabilities and fending off attacks to their voting systems headed into Election Day, a Department of Homeland Security official told POLITICO on Wednesday.
DHS won't name the specific states that have reached out for federal aid -- that's up to each individual state to confirm, the agency said. But DHS has been providing a running total on the overall number of states. Last Friday, a department official said that 21 states had expressed an interest in its vulnerability scanning services.

"We hope to see more," DHS Secretary Jeh Johnson said in a statement on Saturday.

Concerns about a cyberattack on the nation's election system have grown in recent months, following a series of suspected Russian hacks targeting Democratic political offices, the Hillary Clinton campaign and state election networks. GOP nominee Donald Trump has also prompted concerns about the integrity of the election by repeatedly stating the outcome will be "rigged" and by calling for his supporters to volunteer in "certain areas" as poll watchers.

Federal and state election officials insist the country's balloting is secure from a widespread hacking attack -- they note the diverse nature of 50 different state jurisdictions, plus thousands more at the county and local level. In addition, voting itself doesn't involve any connections to the internet, officials insist.

But weaknesses do exist across the system, too. A DHS official last week confirmed that hackers had been detected seriously probing into state voter registration systems in more than 20 states, and they actually had varying degrees of success getting into the rolls in Arizona and Illinois.

In an interview last week, Colorado Secretary of State Wayne Williams confirmed he's met with officials from DHS, the FBI and the U.S. attorney office in Colorado and availed his state of the federal government's resources. "We do participate in that process," he said.

Georgia Secretary of State Brian Kemp also told POLITICO it was "great" that states had the opportunity to tap federal officials for help prepping for the election. But the Republican said he also wasn't bowled over by what the federal government was providing in the way of detection services.

"They're not offering anything we're not already doing in Georgia in regards to running penetration tests on our system," Kemp said.

Washington Post
NSA contractor charged with stealing top secret data
Thursday, 06 October 2016
Byline: Multiple reporters

Boston - A federal contractor suspected in the leak of powerful National Security Agency hacking tools has been arrested and charged with stealing classified information from the U.S. government, according to court records and U.S. officials familiar with the case.
Harold Thomas Martin III, 51, who did technology work for Booz Allen Hamilton, was charged with theft of government property and unauthorized removal and retention of classified materials, authorities said. According to two U.S. officials familiar with the case, he is suspected of "hoarding" classified

materials going back as far as a decade in his house and car, and the recent leak of the hacking tools tipped investigators to what he was doing.

Martin was arrested in August after investigators raided his home in Glen Burnie, Md., and found documents and digital information stored on various devices that contained highly classified information, authorities said.

The breadth of the harm Martin is alleged to have caused -- and what might have motivated it, if proven -- was not immediately clear, although officials said some of the documents he took home "could be expected to cause exceptionally grave damage to the national security of the United States."

Investigators are probing whether Martin, who had top secret clearance, was responsible for an apparent leak that led to a cache of NSA hacking tools appearing online in August, according to the officials familiar with the case, who spoke on the condition of anonymity because the investigation is ongoing.

The FBI and NSA are trying to figure out what drove Martin. The FBI's Behavioral Analysis Unit is working on a psychological assessment, officials said. "This definitely is different" from other leak cases, one U.S. official said. "That's why it's taking us awhile to figure it out."

The leaked NSA tools included "exploits" that take advantage of unknown flaws in firewalls, for instance, allowing the government to control a network. They were posted by a group calling itself the Shadow Brokers. Current and former federal officials said their disclosure could allow targets of NSA spying to determine they were hacked by the United States, and some foreign spy agencies might be able to repurpose the tools.

"This will embolden many to retaliate, likely leading to an escalation of an already costly exchange of cyberattacks between the U.S. and some of its adversaries," said Leo Taddeo, a former FBI agent and chief security officer at Cryptzone, a cybersecurity firm.

Martin's arrest, first reported by the New York Times, marks another humiliating lapse for both Booz Allen and the NSA. In 2013, contractor Edward Snowden, who also worked for Booz Allen, passed a massive trove of documents to journalists, shedding light on massive government surveillance programs that have drawn criticism since they were revealed.

Even before that, the federal government had made detecting and deterring leaks a high priority. In 2011, President Obama created the National Insider Threat Task Force to assist in that effort, and the Justice Department under his administration has prosecuted more leakers than all of its predecessors combined. And after the Snowden disclosures, the NSA doubled down, adopting new technical measures to control information.

For example, officials instituted new rules on downloading sensitive data and implemented audit trails and more frequent screenings of network access by system administrators.

Rep. Adam B. Schiff (Calif.), the ranking Democrat on the House Intelligence Committee, said in a statement that Martin's arrest made it "painfully clear that the Intelligence Community still has much to do to institutionalize reforms designed to protect in advance the nation's sources and methods from insider threats."

An NSA spokesman declined to comment on Martin's arrest. In a statement attached to an SEC filing, Booz Allen said that when it learned one of its employees was arrested, "we immediately reached out to the authorities to offer our total cooperation in their investigation, and we fired the employee. We continue to cooperate fully with the government on its investigation into this serious matter." The company said there had "been no material changes to our client engagements as a result of this matter."

White House press secretary Josh Earnest said Wednesday: "This is certainly a situation that the Department of Justice takes seriously, as evidenced by their complaint. This is also a situation that President Obama takes quite seriously. And it is a good reminder for all of us with security clearances about how important it is for us to protect sensitive national security information."

Military records and an online profile show that Martin was a former Naval officer and reservist with a broad interest in cyber issues. His attorney said he was a Navy lieutenant, and records show he served for more than a decade, spending some years on the USS Seattle before ending his military career in the inactive reserves.

According to his LinkedIn profile and school officials, Martin was in an information systems graduate program at the University of Maryland Baltimore County, and he had studied software and security engineering at George Mason University and economics at the University of Wisconsin. He wrote that his goal was "to advance state of the art in several areas of computing practices in the public/private sector."

Federal public defender Jim Wyda and first assistant federal public defender Deborah Boardman, who are representing Martin, said in a statement that the charges against Martin were "mere allegations" and that they had not yet seen prosecutors' evidence.

"There is no evidence that Hal Martin intended to betray his country. What we do know is that Hal Martin loves his family and his country," the attorneys said. "He served honorably in the United States Navy as a lieutenant and he has devoted his entire career to protecting his country. We look forward to defending Hal Martin in court."

Roy Rada, Martin's former mentor at the University of Maryland Baltimore County, said in an email that Martin was "highly motivated" and had an "intense personal and professional interest in the post-

traumatic stress disorder." Rada, who retired from the school earlier this year, said Martin believed the school had the technology to diagnose PTSD earlier and sought funding to support his research, though, at least when Rada was involved, he did not received any.

Rada said Martin eventually sought a new mentor, and the two lost touch. He said Martin was "thoughtful, sensitive, and dedicated," and the news of his arrest was unexpected.

"While he had a commanding physical presence, emotionally he suffered from the feeling that his relatively special situation was inadequately appreciated," Rada said.

When Martin was taken into custody on Aug. 27, a Saturday, neighbors could hear a boom from blocks away.

It was around 2:30 p.m., and Steve Cunningham, behind a house two doors down, was so startled that he dropped to the ground. Around the corner, Glen Bond had just cracked a Miller Lite and sat down to watch TV in his living room. He walked outside, suspicious that a neighbor had just set off a giant firework.

Federal agents dressed in tactical gear and toting drawn rifles were swarming around the small brick and vinyl-sided house. At least two federal vans and more than 20 vehicles shut down access to the area.

Murray Bennett walked out on his stoop just in time to see a dozen agents smash through Bennett's backyard fence.

"Get back in the house!" a man in an FBI jacket yelled at him.

Not long after, he saw Martin escorted outside in handcuffs.

"Next thing you know, he was gone," Bennett said.

Until well past midnight, neighbors watched as the investigators ransacked Bennett's aging purple Chevrolet Caprice -- still parked in the driveway -- and carried out black trash bags from his home. Bennett said he knew Martin as a "computer guy" who was well educated and decent.

"Unreal," said Bennett, who has known Martin for about a decade. "We passed out Halloween candy together."

Neighbors described Martin as friendly but quiet. They said they hadn't noticed any change in him leading up to the raid.

Around 3 p.m. on Tuesday, a woman who identified herself as Martin's wife pulled up in a black Nissan Rogue and unloaded her groceries.

"The only thing I can say is that it's a matter under investigation. I have no comment," she told reporters before stepping inside.

Prosecutors did not reveal in the criminal complaint how they were tipped to Martin or what precisely they recovered. The complaint alleged that Martin initially denied to investigators that he took documents home, but once confronted with specific examples, he admitted he did so and that he knew the materials were classified. The complaint alleged that Martin "stated that he knew what he had done was wrong."

If convicted, Martin would face a maximum of 11 years in prison. The U.S. attorney's office in Maryland said he appeared in court on Aug. 29 and remains detained.

New York Times
Yahoo Said to Have Aided U.S. Email Surveillance by Adapting Spam Filter
Thursday, 06 October 2016
Byline: Charlie Savage, Nicole Perlroth

Washington - A system intended to scan emails for child pornography and spam helped Yahoo satisfy a secret court order requiring it to search for messages containing a computer "signature" tied to the communications of a state-sponsored terrorist organization, several people familiar with the matter said on Wednesday.
Two government officials who spoke on the condition of anonymity said the Justice Department obtained an individualized order from a judge of the Foreign Intelligence Surveillance Court last year. Yahoo was barred from disclosing the matter.

To comply, Yahoo customized an existing scanning system for all incoming email traffic, which also looks for malware, according to one of the officials and to a third person familiar with Yahoo's response, who also spoke on the condition of anonymity.

With some modifications, the system stored and made available to the Federal Bureau of Investigation a copy of any messages it found that contained the digital signature. The collection is no longer taking place, those two people said.

The order was unusual because it involved the systematic scanning of all Yahoo users' emails rather than individual accounts; several other tech companies said they had not encountered such a demand.

News of the order has opened a new chapter in a public debate over the trade-offs between security needs and privacy rights that has cast a spotlight on the sometimes cooperative, sometimes antagonistic relationship between Silicon Valley companies and the United States government.

It comes six months after a standoff between the F.B.I. and Apple, in which the government obtained a federal magistrate's order to force the company to help it unlock an encrypted iPhone from one of the attackers in the December mass shooting in San Bernardino, Calif. The F.B.I. gave up the fight with Apple after it found a way into the iPhone without the company's help.

By contrast, Yahoo cooperated with the Foreign Intelligence Surveillance Court order, although the technical burden on the company appears to have been significantly lighter than the one the F.B.I. placed on Apple.

Details of Yahoo's cooperation with the court order come two weeks after the company reported that hackers had broken into its computer network, stealing the credentials of 500 million users. Yahoo engineers discovered the breach this summer, two years after it had occurred, and just weeks after Verizon Communications announced plans to buy the troubled internet company for $4.8 billion.

The two government officials familiar with the matter said the digital signature Yahoo was ordered to look for last year was individually approved in an order issued by a judge, who was persuaded that there was probable cause to believe that it was uniquely used by a foreign power.

Investigators had learned that agents of the foreign terrorist organization were communicating using Yahoo's email service and with a method that involved a "highly unique" identifier or signature, but the investigators did not know which specific email accounts those agents were using, the officials said.

The officials' description of the unusual surveillance operation carried out at Yahoo shed new light on a report by Reuters that has attracted widespread attention and provoked outrage among privacy and technology specialists.

The Reuters article reported that in response to a "broad demand" from the government, Yahoo had "secretly built a custom software program to search all of its customers' incoming emails for specific information provided by U.S. intelligence officials."

According to the government officials, Yahoo was served with an individualized court order to look only for code uniquely used by the foreign terrorist organization. Two sources, including one of the officials, portrayed it as adapting the scanning systems that it already had in place to comply with that order rather than building a brand-new capability. The other official did not comment on the technology. The officials did not name the terrorist organization.

Asked on Wednesday about the information obtained by The New York Times, Suzanne Philion, a Yahoo spokeswoman, said the company had nothing further to say. Earlier in the day, the company said in a statement that the Reuters article was "misleading."

"We narrowly interpret every government request for user data to minimize disclosure," the Yahoo statement said. "The mail scanning described in the article does not exist on our systems."

Richard Kolko, a spokesman for the Office of the Director of National Intelligence, declined in a statement to discuss specific foreign intelligence collection techniques, but referred to the Foreign Intelligence Surveillance Act, or FISA.

"Under FISA, activity is narrowly focused on specific foreign intelligence targets and does not involve bulk collection or use generic key words or phrases," he said. "The United States only uses signals intelligence for national security purposes, and not for the purpose of indiscriminately reviewing the emails or phone calls of ordinary people."

Technology companies like Yahoo, Google and Microsoft scan for child pornography and are required to report any discoveries to the National Center for Missing and Exploited Children. They similarly search traffic for malware and spam, which companies disclose in their terms of service.

There is no engineering limitation preventing technology companies from using their spam and child pornography filtering systems to search email traffic for other sorts of digital signatures, said Hany Farid, chairman of the computer science department at Dartmouth, who helped develop the child pornography scanning system with Microsoft.

But the use of that technology to carry out an order from the Foreign Intelligence Surveillance Court to search for a digital signature used by a foreign power is rare, and one of the officials portrayed it as innovative.

"This is another example of how the government is pushing secretly novel or innovative interpretations of surveillance law" to conduct wiretapping in broader ways than the public realizes, said Jennifer Granick, the director of civil liberties at the Stanford Law School Center for Internet and Society.

The government has not released any intelligence court opinion explaining how the judge interpreted FISA to authorize such surveillance. Although Congress in June 2015 enacted a law that required the government to make public novel and significant rulings by the court, the order to Yahoo appears to have predated that legislation, the USA Freedom Act, by several months.

Yahoo has an inconsistent record with meeting government data demands. In 2007, the company settled a lawsuit related to allegations that it helped the Chinese government crack down on journalists by passing along their Yahoo emails.

But that year, the firm fought a legal battle, then secret, before the Foreign Intelligence Surveillance Court, challenging a mandate that it turn over, without a warrant, emails from user accounts the F.B.I. and the National Security Agency said belonged to noncitizens abroad who had been targeted for surveillance.

That litigation became an important test of whether Congress could legalize the Bush administration's warrantless surveillance program through the Protect America Act and, later, the FISA Amendments Act. Ultimately, the intelligence court ruled against Yahoo, and after being threatened with a huge fine, the company cooperated.

Yahoo was not able to clarify details of the Reuters article on Tuesday because orders from the Foreign Intelligence Surveillance Court are secret by law, and an increasing number of other government requests come with gag orders that prohibit tech companies from even acknowledging they exist.

Tech companies complain that such gag orders make it impossible for them to explain to customers what sort of data they do and do not turn over. Twitter and Microsoft have separately sued the Justice Department over the gag order practice, and both cases are pending.

Dozens of other companies have filed briefs in support of Microsoft. In its brief, Apple said it had received about 590 gag orders, of unlimited or indefinite durations, in the first eight months of 2016.

London Daily Telegraph
Yahoo investigated by Irish watchdog over email 'scanner'
Thursday, 06 October 2016
Byline: Cara McGoogan

Dublin - Yahoo is under investigation in Europe over claims that it monitored millions of emails at the request of the US government.
The Irish privacy watchdog said it would examine whether Yahoo had broken EU data protection law as a "matter of considerable concern". It had been reported Yahoo had built a tool to scan every email sent or received for certain phrases that could signal criminal activity on behalf of the National Security Agency and FBI.

"Arising from media reports, the Office of the Data Protection Commissioner is making enquiries into this matter," said the Dublin-based watchdog. As Yahoo's European headquarters is based in Ireland, the Irish office is responsible for determining whether it complies with laws across the EU.

Yahoo last night called reports of its surveillance "misleading". A spokesman said: "The mail scanning described in the article does not exist on our systems. We narrowly interpret every government request for user data to minimise disclosure."

London Times
TalkTalk fined £400,000 for mass hacking breach
Thursday, 06 October 2016
Byline: Robin Pagnamenta

London - The information commissioner has given TalkTalk a record fine after the personal details of hundreds of thousands of customers, including addresses and bank account details, were stolen by hackers last year.
The £400,000 penalty was imposed after the commissioner's office said that TalkTalk, which supplies broadband services to four million households, had failed to take rudimentary steps to safeguard its customers' privacy and security. The regulator said that hackers had been able to access the information "with ease", leading to the theft of the details of 156,959 customers -- or 4 per cent of the total -- in October last year.

In most cases, names, addresses, dates of birth, phone numbers and email addresses were stolen. However, of these, more than 15,600 customers also had their bank account details and sort codes stolen.

Elizabeth Denham, the information commissioner, said: "Today's record fine acts as a warning to others that cybersecurity is not an IT issue, it is a boardroom issue. TalkTalk's failure to implement the most basic cybersecurity measures allowed hackers to penetrate its systems with ease. Yes, hacking is wrong, but that is not an excuse for companies to abdicate their security obligations. TalkTalk should and could have done more to safeguard its customer information."

TalkTalk, which said that the hacking incident cost about £60 million to resolve, was "disappointed" by the decision to impose the fine for breaches of Britain's Data Protection Act.

The company said it had "cooperated fully with the ICO at all times and, whilst this is clearly a disappointing decision, we continue to be respectful of the important role the ICO plays in upholding the privacy of consumers". It added: "During a year in which government data showed nine in ten large UK businesses were successfully breached, the TalkTalk attack was notable for our decision to be open and honest with our customers from the outset. This gave them the best chance of protecting themselves and we remain firm that this was the right approach for them and for our business.

"As the case remains the subject of an ongoing criminal prosecution, we cannot comment further at this time."

The ICO said that TalkTalk was to blame because the hackers used a common technique known as "SQL injection" to hack three vulnerable and out-of-date web pages. The data was contained in "inherited infrastructure" that formed part of the acquisition of Tiscali's UK operations by TalkTalk in 2009.

The watchdog said that TalkTalk should have been aware of the technique and should have had systems in place to prevent such a cyberattack.

The company had also been given two warnings that it appeared unaware of. The first was a successful cyberattack on July 17 last year that exploited the same vulnerability in webpages. A second attack was launched between September 2 and 3 last year.

A 19-year-old man and a 17- year-old youth have been charged in relation to the alleged hack.

CNBC website
The Aspen Institute's Walter Isaacson Interviews Admiral Michael S. Rogers from the Cambridge Cyber Summit Today
Wednesday, 05 October 2016
Byline: Walter Isaacson
Section: Interview transcript

The Following is the unofficial transcript of an EXCLUSIVE interview with Admiral Michael S. Rogers, Commander, U.S. Cyber Command; Director, National Security Agency; Chief, Central Security Service, live from the Cambridge Cyber Summit hosted by The Aspen Institute, CNBC and MIT on Wednesday, October 5th.
WALTER ISAACSON: Thank you. Thank you very much, Michael, for being with us today. The latest of these is Yahoo, in which supposedly a lot was just read because they were ordered to do so. I just got a statement from them, an email, saying, no, no it wasn't really that way. We did not open up all of the emails. It was a much narrower complying with orders. Talk to us about the type of things you need to do and have industry cooperate with you, why that's legal and where you think we have to draw the line.

ADMIRAL ROGERS: So clearly we have a legal framework in this nation that enables the government under specific -- for specific reasons, under specific conditions, to make a case before a judge in which we're able to show a judge we have reason to believe that there is threat here to the United States associated with specific individuals and a judge grants, simplistically, authority for a specific purpose for a specific period of time to access data. And the court order is then given to the private sector to execute. This is done -- phone records, bank records, this is a long- standing mechanism in our nation for how does the government access information using a lawful mechanism to do that. Cyber and intelligence, in this aspect, is no different then.

WALTER ISAACSON: Let me make sure I heard you correctly. That means you couldn't get one that would just blanket look at all emails.

ADMIRAL ROGERS: No. I was going to say, that would be illegal. We don't do that, and no court would ever grant us the authority to do that. We have to make a specific case. And what the court grants is specific authority for a specific period of time for a specific purpose. It's not a blanket, A, just everything.

WALTER ISAACSON: So we shouldn't believe the stories that we read?

ADMIRAL ROGERS: I've read this real quickly and I thought, well, this is a little speculative.

WALTER ISAACSON: Now, do you need cooperation from the big companies, in Silicon Valley, especially on encryption, and are you getting that cooperation?

ADMIRAL ROGERS: I think particularly on the defensive side, as a nation, is we're trying to figure out, so how are we going to ensure that our systems, our data, are secure. The sweet spot to me is how do we create a partnership between the private sector and the government where the best of both are brought together for a unified purpose. Because I don't think asking the private sector to do this by themselves -- I don't think it's particularly realistic and is not going to generate the outcomes we want. I would argue, as well, turning to the government and saying, "Well, you just defend the private sector on your own," I don't think that's workable. It's our ability to bring these two parties and their different perspectives together in a common framework that enables us, I think, to get to where ultimately we need to be.

WALTER ISAACSON: And you said we have for 240 years of framework, it's a pretty simple one, which is unreasonable search. I've heard you talk about that. It used to be that nothing, anything, the trunk of your car, your safe deposit box, your diary, nothing was out of the reach of law if a court said it could be searched. Why did that change recently? And is that a problem?

ADMIRAL ROGERS: I think a lot of factors are coming together. I think we have to acknowledge that right now as a society we have broad distrust, in some ways, of the mechanisms and the structures of government and governance. Those structures within our nation that we have traditionally given responsibility -- law enforcement, intelligence -- oversight that we have traditionally given responsibility to execute some of these functions. I think we have to acknowledge we're living in a world now in which some of those mechanisms are not trusted. If you go back, much of the framework, the court, FISA court, congressional oversight to HSPCI and SSCI, the two congressional committees that conduct oversight, for example, for intelligence purposes, all created in the late 1970s, in the aftermath of the Pike and the Church Committees in which they came to a couple conclusions. We need to provide a legal framework for the intelligence organizations of the U.S. government to execute their operations so they're not acting indiscriminately.

Secondly, we need to provide a level of oversight so that the citizens of the nation have some level of awareness of what they are doing, why they are doing it. But at the same time we need to do it in a way that doesn't compromise what they're doing. Thus, was born the idea of, hey, Congress is the elected representatives of our citizens. We'll execute this oversight function in the name of the citizens, and thus was born the two oversight committees.

It's 40 years later now. And what I try to tell our team is we've got to step back, you guys, and ask ourselves, so that quirk structure that we've created, how is it viewed today by the citizens of our country. We have to acknowledge it's a slightly different construct. The government makes an argument

before the FISA court, and the judge shares the argument and the judge makes the decision, do they agree? Do they disagree? Have we met the threshold of evidentiary proof? Likewise, the oversight committees, in a time in which, again, I think we have to be honest, Congress, as in many other institutions, is not quite held in the same regard as it was potentially in the aftermath of Watergate, where Congress was viewed as, hey, look, you took a proactive role, you took on the Executive Branch, and you generated insights that help our nation understand some activity that was truly of concern to us.

You fast-forward 40 years, I would argue we're in a very different place now. It's just not the broad view that most -- not all, at least many citizens take.

So I think part of our challenge going forward is how do we create oversight mechanisms that enable intelligence, law enforcement, to do their important duties in a way that both engenders confidence for the citizens we serve but at the same time acknowledges in order to do this, we can't just publicly get into the details of everything we do. Because not only are citizens with a very lawful concern paying attention, but the very targets we're trying to access, they're paying attention as well. And they want to know, How are they coming after me? What are the sources they're using to generate insights, if I'm ISIL, if I'm a foreign state, they're very much interested in? So what are the intelligence? How are they doing what they do? That's not really what we want to give up.

WALTER ISAACSON: Do you think that private companies should be allowed to create devices and services that are designed specifically to thwart the reach of the courts?

ADMIRAL ROGERS: Let's ask an easy question.

WALTER ISAACSON: And, by the way, you've talked to Tim Cook about it. Tell me what you said to him.

ADMIRAL ROGERS: I'm not going to go into specifics, but, broadly, this is what I say. We have to acknowledge it as a nation we have two incredibly important imperatives here. We must ensure the security and the safety of our citizens while at the same time doing it in a way that does not undermine their rights or our very structures as a government. Because achieving security, in the name of becoming something we're not, is a bad place for us to be as a nation.

Likewise, I would argue, ensuring the protection -- ensuring the privacy and the rights of our citizens without also providing them security, I would argue that's not a great place for us to be. So, it's how do we find this middle ground. This is a tough challenge for us, because, again, it's happening in a broader context; it's happening in a time when the mechanisms of structure just are largely distrusted.

I'm struck by the fact, for example, phone companies, on a regular basis, are given significant numbers of search warrants to comply with a Federal court that says you must provide the Federal government, under specific circumstances, access to the communications of the phonecalls of the following individuals. And yet, when we use the same process for emails, for example, we're generating a very

different reaction as a society. I'm still trying to work my way through personally, what is the difference? What is it that generates a fundamentally different approach?

To go to your initial point to me where, as a nation, we had previously accepted the fundamental premise that nothing is beyond the reach of the government with appropriate protection and appropriate use of the court, a legal framework, the legislative branch. We've generally accepted that as a fundamental premise, and yet we seem to be in a different place now where, in some areas, we're not quite as comfortable. And I'm still trying to work my way through it. So in my conversations with my private-sector teammates, I go: We've got to have this conversation. We cannot vilify each other. It isn't one side is good and one side is bad. We're trying to make sure that these two incredibly foundational imperatives for us as a country are executed in a way that the one doesn't undermine the other. And that's not an easy challenge.

I think lastly -- I apologize for going on so long for you. But we have to acknowledge we're currently in a place where technology has outstripped our legal and our policy framework. And we've got to ask ourselves: How do we address that? Are we comfortable with that? That's not something that you want guys like me deciding. That's something I think more broadly we, as a society, have to have a conversation about, what are we comfortable with here, and not just vilify each other, one side's good and other side is bad. That's just so simplistic, and it isn't going to let us get to solutions; because in the end, we have to generate solutions, I think.

WALTER ISAACSON: As part of both the NSA and especially cyber commander protecting both the defense department but in general the critical infrastructure, what authority -- if, on the day running up to election day, there were large amounts of hacking and traffic and malware and denial of service attacks coming from a country like Russia, as we've already seen them come in on places, do you have the authority right now, or what type of authority would you need to A, defend against those attacks; and B, if necessary, retaliate against the attacks, if for example, some actor decided to wipe out the voter registration rolls of Miami, Cleveland and Philadelphia?

ADMIRAL ROGERS: So, right now as the commander of the United States Cyber Command, and as the director of the National Security Agency, do I have the authority to unilaterally access U.S. systems? No, I cannot do that.

And in the scenario that you highlight, where potentially we might be looking at a penetration, major damage, we have a structure and a process within the government where, in this case, either state, local, or private would approach the government looking for a system, we -- both Cyber Command and NSA -- would be part of a broader government effort to provide that. There's no simple, single rule that fits all. So, it's a case-by-case, specifics of a case-by-case. That's one of the challenges for some people I see in cyber where they will say to me: Well, I'm a little confused why we act this way in this situation and we act a very different way in another situation. I say: That's an appropriate approach to me because it's not one size fits all.

It's no different than -- excuse me -- in the application of kinetic force, for example, as a military guy. It isn't one size fits all. We tailor our rules of engagement, we tailor the decisions we make to the specifics of a particular incident or event, and we respond in a very discreet and appropriate way. Not, hey, it's the same thing no matter what happens.

WALTER ISAACSON: Well, let me just ask a question. You say people keep asking you about a problem, which is, you acted in a very specific way -- well, not you but the government -- with the Sony hack. You named who it was, you shamed them, you put sanctions on and for all we know, you may have done other things that were covert. With the Chinese, there were some indictments against PLA members.

With the Russians, you haven't done anything that we've known. Why not? Is it because you don't know that it's the Russians doing this to our various electoral systems in Illinois or DNC?

ADMIRAL ROGERS: So, first, that's a broader policy issue. I've got to acknowledge, hey, look, I'm a military guy. But -- so I'd make a couple points, Walter, based on what you just said. First, I think it's important we made a decision on the basis of the specifics in each of those scenarios. In one case, we opted to go with a very public, both acknowledgment of the activity, naming of the actor who did it, in this case the North Koreans, as well as specific actions we're going to take in response.

With our Chinese counterparts, we've opted to engage in a long-term ongoing dialogue about what our concerns are to try to identify the behaviors we find objectionable and to try to highlight through specific legal means, in this case, highlighting and indicting five specific individuals, here are concrete examples that we believe meet a legal threshold that would highlight the sorts of activity that we believe are unacceptable.

In the case of the Russia piece, I would just argue, look, this is an ongoing issue, so I'm not going to get into specifics. Let's wait and see how this plays out a little bit and don't just assume that because you haven't seen anything broadly, that it doesn't mean that there isn't activity ongoing. And we'll just let this play out a little bit.

WALTER ISAACSON: And if at some point there is activity ongoing, is there an advantage to being public with that?

ADMIRAL ROGERS: It depends on the scenario. If you look at Sony, for example, so that's November of 2014 -- it's hard to believe we're coming up on two years since the North Korean attack against Sony. At the time, my input -- and I'm just one person in the process. I had a couple of concerns. I said, number one, this is so public that we just can't put our head in the sand and pretend it's not happening.

Secondly, if I'm in the private sector and I see this kind of activity -- because it's directed at the private sector in this case, Sony, a private company -- hey government, if you're not going to do something here, then my option as the private sector is should I draw the conclusion that that means I need to do something and that I shouldn't look to the government in this case? That was an important part for me

of the Sony piece. I thought not only did we want to send a very clear message to the North Koreans, but I thought we also wanted to send a very clear signal to our own private sector about, hey, the government would be willing to stand up under specific conditions and highlight unacceptable behavior and try to bring the capabilities of the government to bear to stop that from happening again. I think that's a positive for us as a nation. I think the approach we've taken with China has been effective to date. I'm not going to argue it's perfect, but it's enabled us to continue moving forward in a dialogue and to agree to changes in behavior. We'll see how this plays out over time. But those are all positives.

WALTER ISAACSON: Can I just drill down right there? What changes in behavior have you seen on China?

ADMIRAL ROGERS: Well, remember, the specific agreement on the 25th of September, 2015. So, again, it's hard to believe we're slightly over a year from there. Can you tell --

WALTER ISAACSON: Time flies when you're having fun.

ADMIRAL ROGERS: -- I'm a happily married guy? I love dates.

What we agreed to there with them was, look, we acknowledge that nation states use cyber as a tool to generate insights as to what others in the world around us are doing. The difference of opinion that we had with the Chinese counterparts was, look, in the U.S. structure we do not take the mechanisms of government, intelligence structures, the military, we don't use those as a vehicle to access the private sector and other companies and other countries for the express purpose of then taking that data, providing it to the private sector in the United States to gain competitive economic damage. We don't do that. In our structure there's a large firewall between what the private sector does when it competes economically and what the role of the government is in that competitive process. We draw a strong firewall there.

Our concern with the Chinese was we don't see that same differentiation in your behavior. We see you penetrating U.S. private systems and then sharing that data with your companies to give them competitive advantage. Look, that is unacceptable to us. And so both of the leaders -- as I said a year ago, in the aftermath of the visit between the two presidents in Washington, came out and said: Hey, look, this is unacceptable behavior, and both nations agree we will not engage in that behavior.

WALTER ISAACSON: Are we having those conversations with the Russians?

ADMIRAL ROGERS: Slightly different structure there, I would argue. Again, everything is a case-by-case basis. The challenge set there is a little different. It's not quite the same.

WALTER ISAACSON: Do you consider our election infrastructure part of our critical infrastructure the way the electricity grid is?

ADMIRAL ROGERS: It's interesting. I think we need to step back and redefine a little bit just what does the idea of critical infrastructure mean in the 21st century? We traditionally have tended to look at it along very industrial lines. Does the segment produce an industrial output of significance to our nation: air travel, finance, petroleum distribution?

In the world that we're living in now, I think another thing we need to think about when we're trying to define what is critical infrastructure for me is the whole idea of data. When I look at the election structure, I go, look, that is the protection of data in the form of votes in the electoral college. What are the implications for us? Because, quite frankly, I don't think any of us really put a lot of time thinking, boy, would somebody ever contest, you know, the infrastructure associated with our election process? But clearly we are moving into a world in which, seemingly -- and you can pick any media outlet any day, every day we're watching major cyber penetrations, theft, extraction of data on a global basis. And we're entering a world where literally nothing seems to be beyond the reach or intent of someone out there to try to access it and often for a variety of purposes: economic advantage, intelligence, embarrassment.

WALTER ISAACSON: Do you see those things changing? In other words, it used to be for economic benefit and now, at least what we're seeing recently, it's just to sow doubt and mess up an election system.

ADMIRAL ROGERS: I mean, there's an aspect of it there. I also remind people, look, if you look at the totality of activity out there, the criminal segment is still the greatest majority. Probably -- depending on the source you want to use, probably 65% of the total cyber activity of concern that you see out in the Worldwide Web today is largely criminal, groups, individual actors using cyber, using the web as a vehicle to gain access to data which they then turn around for economic advantage. Hey, we sold credit card numbers. We sold social security numbers. We sell identities.

WALTER ISAACSON: That 65% is stable, or has it gone up or down?

ADMIRAL ROGERS: It's been pretty -- the last thing -- because I'd be the first to admit it, it's not the biggest focus for me. It seems to be pretty stable in terms of a percentage, but I will say that the capabilities of some of the criminal actors that you see today -- I mean, this is money. So it's not surprising: Where you find money, you find people willing to make investment and willing to generate capability, and the criminal segment sadly is no different. There's a lot of money out there, and so you see a lot of groups really upping their game in terms of what they're capable of doing.

WALTER ISAACSON: If we don't either name, shame, or retaliate or do something with, say, the Russians, if they're the ones messing with our election system, do you assume they'll do it to the German elections next?

ADMIRAL ROGERS: Well, the way I phrase it is don't look for this to be isolated behavior.

WALTER ISAACSON: In other words, yes?

ADMIRAL ROGERS: Yeah. Look for this -- I won't go to the specifics of a country, but my comment would be look for this sort of behavior to continue. And I think that goes to the broad question we're all trying to grapple with. So how do we change the dynamic to get to a place where behavior like this is unacceptable or is perceived to be of such a risk that you don't want to engage in it? And clearly, we're just not there today and that's not a good thing for us.

WALTER ISAACSON: And so we're not there today because we haven't been able to name or we haven't been able to retaliate or we don't have the rules of the road? What should we be doing?

ADMIRAL ROGERS: So my first comment is there's no silver bullet here. It's going to be a combination of how do we make it much more difficult for nations, actors, individuals to be able to successfully penetrate systems. You know, one of our challenges is we are dealing with literally trillions of sunk costs in the form of investments that are out there today, and our network structures and our data flow and our infrastructure, the way it's built, the way it's designed, much of it, most of it was built in a time in which redundancy, resiliency and defensibility were just not core design characteristics. Simplistically it was about, how do you achieve maximum efficiency and effectiveness at the lowest price point?

And so we have built structures over the decades that were never built for this kind of dynamic, this kind of environment where you have a wide range of actors attempting to penetrate them for a variety of purposes. To date, those purposes have largely been the extraction of information. But what happens when it's not just about extracting data and information anymore? What happens when it's about manipulating data so that you can't trust what you're looking at? Think about how that would shape our choices, our decisions as consumers, as businesses, as military individuals. If I couldn't believe the kind of picture that I'm looking at of an environment that enables me as a military commander to start to make risk-based decisions to try to gain advantage and forestall what an opponent is doing, if I lost that ability and instead I'm looking at a picture that's totally false and, in fact, is leading me to make choices that are not helping me, they're helping the opponent, in fact, they're undermining me, that's a bad place.

What happens when we get to the point where some non-state actors, let's take ISIL as an example, decide that the Worldwide Web offers not just the opportunity to spread the ideology, to recruit, to coordinate among geographically dispersed entities, to generate revenue -- what happens when they decide, this is a weapons system, this is a vulnerability, hey, we can exploit this? My concern is this is going to happen. It's the when to me, not the if. And most -- and I apologize. I'll just finish real quick. Most nation states, while they want to gain an advantage, they are unwilling to destroy the status quo as the price of gaining the advantage. I look at a non-state actor like ISIL and I think they have no desire to preserve the status quo. They have no desire to protect the mechanisms of stability that have engendered our ability to create these amazing global inter-connectivities and this amazing structure that we have. They have no interest in preserving that. That's not their vision.

WALTER ISAACSON: So if that's the case, is it that our -- are our offensive capabilities against ISIL not as much of a deterrent as in the old days when our intermediate-range nuclear missiles were a deterrent against an invasion across Europe? In other words, what type of cyber offense comes out of Fort Mead to an ISIL?

ADMIRAL ROGERS: So, I'm not going to get into the specifics. We have publicly acknowledged as a department that cyber command, as a DOD operational entity, is employing cyber in an offensive capability in Syria and Iraq against ISIL. I'm not going to get into the specifics of the how or the what. But one of my takeaways I hope people will draw from this is we have publicly acknowledged, now that we've been doing this for months, we've been able to do this in a very targeted, very focused way, in a very proportionate way.

So you haven't heard, you know, Oh, my God, look at what they're doing against civilian infrastructure, look at what they're doing against -- that's impacting NGOs in the space. We have tried to be very precise, very measured, very discreet. Because we are aware, hey, look, there's second and third implications here that we need to be mindful of. And so, you know, that's something that I feel very good about. We've been able to show that we can execute and use these sorts of offensive capabilities. We can have impact. We can do it in a way that doesn't cause fratricide with very legitimate second and third parties that are operating in the same space.

WALTER ISAACSON: For that to happen, you need to have cyber command, which is an operational division, and you do have it, very closely linked physically, both under your hat -- because you have two hats -- with the NSA, the intelligence gathering. There are proposals to separate, compartmentalize, as opposed to integrate more, to take them apart more. I know that's a big political discussion that will be ongoing. But what cautions would you give the next administration about answering that question, should we separate cyber command from NSA?

ADMIRAL ROGERS: First, clearly an ongoing discussion. We routinely, as an organization, assess our structures the way we're organized. That's nothing new. We do this all the time much more broadly across the department. Hey, that's perfectly appropriate. You always want to ask yourself: Are the assumptions that we made in the past still valid today? Is the structure and the processes we picked that we have created to generate cyber outcomes, do they still make sense? As we're working our way through this, you know, my points have been in the long run, I acknowledge, I think this is the right thing to do as cyber command gains more capability, as cyber command gains more capacity. I believe that in the long run, we want to keep these two organizations closely aligned. But we're probably going to want to get to a position where cyber command is able to act a little bit more on its own. And, quite frankly, part of it is just the human dynamic. These are two very -- I'm the first to acknowledge, these are two demanding sets of responsibilities. But on the other hand, I've also argued you don't want to do anything so precipitously that you end up incurring risk that you don't have to. I'm getting some broader policy decision. We'll work our way through the how, the if, the when. You know, there's some smart people looking at this. This is not something that's going to be done casually.

WALTER ISAACSON: The issue of end-to-end encryption, how bad is that for you, really?

ADMIRAL ROGERS: Now, it varies. If you are a law enforcement entity, a local sheriff, the FBI, encryption puts you in a very tough spot. You do not have the technical means, and you don't have the legal means to overcome it. So you are trying to figure out, I got a device, the potential has evidence related to exploitation of youth, crime, violence, guns, weapons, terrorism. And in many cases, these days, you increasingly find yourself unable to access it.

For the National Security Agency, the intelligence structure is a little different for us. We operate in foreign space, number one. So we have some legal options that are available to us that are domestic. Law enforcement teammates do not. Secondly, we've got a set of tools that we can look at more broadly. So my input to this has been, for us, this has had impact. That impact will grow over time. It's going to get worse, not better. That while many people, for example, will talk to me about the power of metadata. I'm like, Hey, look, I spent a lot of time on the bar in metadata. I don't disagree. But another thing I try to remind people is the goal -- let's talk about terrorism, where this really is starting to come to the fore, that's the one that's really driving this in some ways right now. Because you are watching groups that we know are attempting to conduct attacks in the United States, that have done attacks in western Europe, and they are using these tools to coordinate among each other and to move people, move money, move explosives.

WALTER ISAACSON: "These tools" means like an application, encryption? And you lose them and they go dark to you and you can't follow them?

ADMIRAL ROGERS: It depends on the scenario, specifically. But they clearly are aware of the technical limitations here, and they are trying to take advantage of that.

For us, the point I'm trying to make is, our goal is not to be in a position to respond in the aftermath of an attack. Is that part of our job? Yes. But the goal we're constantly striving for is to get ahead of the problem set and stop events from happening before they even occur. To do that, in my experience, you fundamentally have to get the content. Metadata won't tell you, so who are the specific actors here that I need to roll up? How many parts of the network are truly involved in this? What exactly is the target? How are they going to do this? Is it explosives, is it weapons, is it vehicles? Where is the target? You don't get all that from metadata, for example. So increasingly the challenge for law enforcement, for us is, how do you access content in a way that both protects the rights of lawful citizens but at the same time enables us to generate the insight that those citizens are counting on to help ensure their security and their safety?

WALTER ISAACSON: And if you could pick -- this is my last question -- one thing that Congress could pass that would get that balance right on that most important issue, let's keep it focused on possible use by terrorists of communications, what would you ask for?

ADMIRAL ROGERS: I say this to my congressional counterparts when I get asked: Help to try to create an environment in which we can have a meaningful dialogue about how we're going to deal with this.

Because I am a little concerned. My argument would be, you don't want us, intelligence or law enforcement, jamming a solution down your throat. I would argue, you don't want the private sector doing this unilaterally. How can we come together and bring the best of our nation? I say this out in the valley all the time: You are about the power of potential. You are the greatest innovative engine. You represent much, much broader than just the valley. You are the visible face of one of the most powerful innovative engines on this planet and in the history of this world.

As a society, traditionally, America is all about "can do." And I hear us right now spending a lot of time about "can't do." And the frustration for me is, can't we harness the power, the insight, the knowledge, the innovative approaches of the private sector, and the knowledge and skills of the government to come together and to key up options for our citizens to decide what are they comfortable with that would enable us to address this very important and fundamental issue? It goes to this mismatch about our legal framework and the state of technology.

WALTER ISAACSON: Admiral Mike Rogers, thank you very much for being with us.

ADMIRAL ROGERS: Thank you. Thank you. Thank you very much.

Radio-Canada - Nouvelles (site web)
Un employé de la NSA arrêté pour vol de données secrètes
Thursday, 06 October 2016
Byline: Journaliste maison

Non identifié - Un employé contractuel de la NSA soupçonné d'avoir volé des données de l'agence fédérale classées « top secret » a été arrêté, à la toute fin du mois d'août, par le FBI. C'est ce qu'a révélé le New York Times dans son édition du mercredi 5 octobre.
L'homme qui répond du non d'Harold Thomas Martin III est un salarié de Booz Allen Hamilton, une société sous-traitante travaillant pour la NSA. La même qui avait engagé Snowden, l'informaticien qui avait révélé le programme de surveillance et d'espionnage américain.

Selon le quotidien new-yorkais, la perquisition effectuée dans le domicile de M. Martin révèle une importante saisie de documents et d'informations numérisées stockées sur différents appareils électroniques. Le journal ajoute que la police avait retrouvé aussi des documents confidentiels dans la voiture de l'accusé.

Motivations inconnues

Interrogé par les agents du FBI, l'homme de 51 ans a d'abord nié les faits, avant de les reconnaitre, écrit le journal.

Dans la foulée des révélations du New York Times, les avocats de M. Martin ont publié un communiqué en affirmant qu'il n'y avait pas de « preuves évidentes » contre leur client. Il aime sa famille et son pays, il ne va pas trahir les États- Unis, ont-ils écrit.

Selon le journal américain, les motivations de M. Martin restent inconnues par les agents du FBI. Mais ces derniers le soupçonnent d'avoir voulu pirater les systèmes informatiques des pays rivaux des États-Unis (Russie, Chine, Iran et Corée du Nord) avec les codes confidentiels qu'il a volés.

Pour le FBI, il est très tôt de parler espionnage. Mais les agents fédéraux disent poursuivre l'enquête pour savoir si M. Martin n'est pas le responsable d'une fuite de code de la NSA classé « confidentiel » attribué au groupe dit Courtiers Fantômes. Les enquêteurs veulent savoir aussi s'il avait joué un rôle dans une série des fuites sur les écoutes téléphoniques américaines concernant des pays comme le Japon, l'Allemagne et publiées l'année dernière par Wikileaks.

Pas d'« épidémie » Snowden

Le FBI refuse de faire une comparaison avec l'affaire Snowden. Les enquêteurs pensent que M. Martin aurait « volé » les documents avant que l'affaire M. Snowden ne soit rendue publique, indique le quotidien new- yorkais.

Bruce Schneider, un spécialiste de sécurité informatique qui suit de près les fuites de la NSA, a indiqué au New York Times qu'il n'y avait « pas une épidémie » Snowden.

Toutefois, M. Schneider a fait remarquer que l'agence fédérale a recruté ces dernières années beaucoup de jeunes programmeurs et des spécialistes dans le piratage informatique. Les officiels ont peur que ces jeunes soient inspirés par Snowden, mais le suspect actuel ne semble pas répondre à ce profil, selon lui.

Dans un document du FBI, le département de la Justice évalue à plus de 1000 $ l'équipement volé par M. Martin qui, pour le moment, est poursuivi pour détention de matériels secrets et vol au détriment du gouvernement. Il risque respectivement un an et dix ans de prison pour ces faits.

Le Temps (Suisse)
La Suisse plus restrictive
Thursday, 06 October 2016
Byline: Sylvia Revello

Berne - Expert en droit des médias et des nouvelles technologies, Nicolas Capt analyse l'affaire Yahoo! du point de vue juridique suisse

Peut-on envisager un accord similaire à celui de Yahoo! entre les autorités et des fournisseurs suisses?

Au-delà du caractère illégal, cette situation me paraît peu probable. Les prérogatives étatiques sont très différentes en Suisse. Dans l'exemple américain, on est face à une surveillance à grande échelle, une sorte de fishing expedition qui ratisse large en espérant obtenir des résultats. Le cadre helvétique est bien plus restrictif, y compris avec la nouvelle loi sur le renseignement, qui pose de nombreux garde-fous. De la part des autorités pénales comme du Service de renseignement de la Confédération (SRC), l'observation des données privées reste limitée et surtout ciblée. La vraie différence réside dans une certaine opacité de la surveillance du SRC qui officie, par principe, hors de toute procédure pénale.

La NSA avait-elle vraiment besoin que Yahoo! lui fournisse ses données, connaissant sa puissance de frappe?

Il n'est pas absolument certain que la NSA soit capable de procéder seule à une surveillance aussi large. Politiquement parlant, je relève que le scandale est moindre en négociant un accord préalable avec la société plutôt qu'en opérant une attaque informatique contre une entreprise, qui plus est américaine. Cette forme de coopération assez servile n'existe pas, à ce jour, en Suisse. Le pays a d'ailleurs une vraie carte à jouer en termes de confidentialité des données - sorte d'héritage de feu le secret bancaire - et de respect de la vie privée. De nombreux data centers voient le jour dans ce sens et une association, VigiSwiss, défend la place suisse à l'international en tant que coffre-fort numérique.

Malgré leurs déclarations, Google et Microsoft pourraient-ils imiter Yahoo!?

Difficile de le dire, à ce stade, sans sombrer dans les conjectures. Le passé récent, et notamment le programme Prism, montre toutefois que beaucoup ont accepté de collaborer. Ils pourraient en revanche, comme Apple au début de l'année, opposer une résistance pour des raisons éthiques et/ou commerciales. Cette position de principe n'a toutefois pas empêché le gouvernement de parvenir à ses fins, en faisant déverrouiller l'iPhone appartenant à un terroriste par une société tierce.

The Pioneer
Kerala ISIS in cyber overdrive
Thursday, 06 October 2016

Kochi - The Kerala unit of the Islamic State of Iraq and Syria (ISIS), Ansar-ul-Khilafa is still active in cyberspace despite the arrest of six of its top leaders by the National Investigation Agency (NIA) from Kannur district on Sunday even as the Intelligence agencies believe that there could be several young men in northern Kerala, especially in Kasaragod, Kannur and Kozhikode districts, who may have connections with the global terror group or are its sympathisers.
According to Intelligence officials, a Facebook page which was being maintained allegedly by Manseed of Kannur, arrested from Kanakamala along with five others last Sunday, under the assumed name of

Sameer Ali, is still active and is being updated frequently. They said the page was updated even on Tuesday.

The NIA had found that Manseed alias Sameer was the chief coordinator of the 12-member control group of Ansar-ul-Khilafa Kerala.

Fresh posts declaring support to the ISIS and calling for jehad had appeared on the Facebook page in the past 48 hours, say officials. The new posts indicated that the page manager had knowledge of the six arrests. The messages aimed at jehadis said activities in the path of jehad did not depend on individuals and that jehadis might get killed or jailed but the jehad would not end because of such incidents.

The new posts, which also exhorted believers to wage war against those violating the laws of Allah, said it would be difficult for Keralites who had been keeping away from the path of jehad for several decades to join the movement. Updating is said to be happening on an hourly basis in the Telegram chat group of Ansar-ul-Khilafa Kerala. The NIA has learned that there are 32 participants in this chat group.

The NIA has found the Malayalam blog of the Kerala unit of the ISIS, which was started almost a year ago and had gone out of function last July after the agency infiltrated it. The agency has also found that articles written by Sameer Ali had been posted on the blog even the day before the arrest of the six alleged operatives from Kannur.

Participants in the group had been given strict instructions to keep details of the account concealed, sources said. The NIA has received information that those writing in the group's Malayalam blog, which had articles criticising the Muslim organisations in the State, are young Keralites living abroad.

Meanwhile, some non-resident Kerala industrialists could have provided financial assistance - knowingly or unknowingly - for the activities of Ansar-ul-Khilafa Kerala, sources said, adding that an Islamic outfit with extremist leanings based in northern Kerala could have provided help for the formation of the ISIS's State unit. Investigations are progressing in these matters, they said.

According to Central Intelligence agencies, the Kerala Police had failed in taking effective action even after the Facebook group of young Keralites had appeared in cyberspace in the name of Ansar-ul-Khilafa Kerala. This lapse on the part of the police could have contributed to the expansion of the group with ISIS sympathizers in the State.

It has now become clear that huge sums of money had flowed into Kerala from abroad for the formation and functioning of Ansar-ul-Khilafa Kerala. There are indications that some of the 22 people from Kasaragod and Palakkad districts who had disappeared mysteriously and are feared to have joined the ISIS in Afghanistan had been in direct or indirect contact with the leadership of Ansar-ul-Khilafa Kerala.

Yonhap News Agency

N. Korea shows increased activity at nuclear test site: 38 North

Friday, 07 October 2016

Byline: Staff reporter

Section: general

Washington - North Korea is showing increased activity at its nuclear test site in what could be part of preparations for a new test, a U.S. website monitoring the North said Thursday, amid concern the regime could undertake provocations to mark a key anniversary next week.
Commercial satellite imagery taken on Oct. 1 of the Punggye-ri underground test site in the country's northeast "indicates continuing activity at all three tunnel complexes that could be used to conduct a nuclear test," the website 38 North said.

Activity at the North Portal, where the communist nation conducted its fifth nuclear test last month, could be for a number of purposes "including collecting post-test data, sealing the portal or preparing for another test," the report said.

Satellite imagery shows a large vehicle, possibly a truck, near the portal's entrance, while a large canopy in its parking lot, which has been present for the past two months, remains in place, the report said. No signs of new excavation were seen, but there appear to be boxes or material around the side of the main building, it said.

Increased activity was spotted at the South Portal where excavation stopped in 2012, the report said.

Two small vehicles were seen on the road as well as what appears to be a group of people standing near one of the portal entrances, indicating ongoing work or maintenance, the report said.

"The purpose of this activity is also unclear although the portal is assumed to be capable of supporting a nuclear test once a decision is made to move forward," it said.

In addition, mining carts and furrows were evident on the spoil pile at the West Portal, but it is unlikely that tunnel excavation has resumed since the pile has not grown over the past two months, the report said.

South Korean officials have said that the North appears to be ready to carry out an additional nuclear test at any time. Speculation has grown that Pyongyang could conduct one to mark the anniversary of its ruling Workers' Party that falls on Monday next week.

Reuters

Satellite images show activity at North Korea nuclear test site - report

Friday, 07 October 2016

Byline: Staff reporter

Section: general

Seoul - An increase in activity at North Korea's nuclear test site could signal preparations for a new test or a collection of data from its last one, a U.S.-based monitoring group said on Friday, citing satellite images.
The 38 North group, run by Johns Hopkins University's School of Advanced International Studies, said there was activity at all three tunnel complexes at the Punggye-ri nuclear test site involving a large vehicle and personnel.

"One possible reason for this activity is to collect data on the Sept. 9 test although other purposes cannot be ruled out, such as sealing the portal or other preparations related to a new test," the group said, referring to the last nuclear test.

The North is believed to be ready for another nuclear test at any time and there has been speculation it could mark the Oct. 10 anniversary of the founding of its Workers' Party with another underground detonation.

North Korea conducted its first nuclear test in 2006 and has since then defied U.N. sanctions and rejected international talks to press ahead with the development of the weapons and missiles to carry them, which it says it needs for its defence.

In January, it conducted its fourth nuclear test and last month its fifth and biggest, on the anniversary of the nation's founding.

The United States and South Korea are pushing for tighter sanctions against North Korea by closing loopholes left in a U.N. Security Council resolution in March.

South Korea's Unification Ministry spokesman Jeong Joon-hee told a briefing there were no particular indication of a plan for a nuclear test timed to coincide with the Oct. 10 anniversary.

South Korea's Yonhap news agency cited an unidentified government official that there was activity at the North's rocket launch station near the west coast that could be preparations for a long-range missile launch.

Last month, the North said it had successfully conducted a ground test of a new rocket engine that would be used to launch satellites. South Korea said the engine could be used for a long-range missile.

North Korea last month fired three missiles that flew about 1,000 km (600 miles). In August, it tested a submarine-launched ballistic missile that international experts said showed considerable progress.

Japan said the possibility of further "provocative action" by North Korea could not be ruled out.

"The government is taking all possible measures in gathering information, exercising vigilance and taking surveillance activities to be able to respond to any situations," Japan's Chief Cabinet Secretary Yoshihide Suga told a news conference. (Reporting by Jack Kim and Ju-min Park; Editing by Robert Birsel)

Wall Street Journal

Accused Contractor Was on Hacking Team

Friday, 07 October 2016

Byline: Damian Paletta, Scott Calvert

Section: general

Washington - Harold "Hal" Martin, the former National Security Agency contractor charged this week with stealing government secrets, spent parts of the past decade on a government hacking team, sought funding for research into post-traumatic stress disorder, and tried to rally internet users to wage digital warfare against computer "commandos."
Investigators are still trying to determine why Mr. Martin, a former employee of consulting firm Booz Allen Hamilton who worked on projects at the NSA and the Pentagon, took classified documents containing computer-spying tools to his home in Glen Burnie, Md. But as the probe continues, more details of his background are coming into focus.

A former academic mentor of Mr. Martin described him as focused, and burdened by a sense that his insights weren't appreciated.

Roy Rada, a professor of information systems at the University of Maryland, Baltimore County until he retired in January, said he served as a mentor to Mr. Martin several years ago, and the two worked together for a few months. Mr. Rada, in an email to The Wall Street Journal and two other news organizations, said Mr. Martin, now 51 years old, was "highly motivated" and had served in the Navy in wars in the Middle East.

Mr. Rada said Mr. Martin had an "intense personal and professional interest in the post-traumatic stress disorder" and wanted to focus his graduate research in this area.

Mr. Martin had hoped he could secure enough funding to finance his graduate work on PTSD but wasn't able to, Mr. Rada recounted. Mr. Martin then decided to work with another mentor at UMBC, and Mr. Rada said he and his former mentee lost touch.

Mr. Rada described Mr. Martin as "thoughtful, sensitive, and dedicated."

"While he had a commanding physical presence, emotionally he suffered from the feeling that his relatively special situation was inadequately appreciated," he said, without expanding on what that situation might be.

Mr. Martin's LinkedIn page says he started his Ph.D. work at UMBC in 2007 but it remained incomplete. "Trying to finish that dissertation," he wrote. His graduate work had moved in another direction from PTSD. In 2014, he published a paper at a Seattle conference on cloud computing.

Cloud computing has been a focus for U.S. military and intelligence officials, who are interested both in protecting cloud-stored data from hackers and penetrating the cloud to steal information from others.

In 2009, someone using Mr. Martin's email address highlighted the vulnerability of data moving from clouds to "server farms" and then to computers. The person warned on Seclists.org, a site used by people to discuss computer security, of potential attackers including "'commandos' and 'dirty dozen' types mounting the electronic 'castle walls.'"

"You just have to ask yourself if you are ready form [sic] digital aiki-do," the person wrote, referring to martial arts. "Or do you intend to let digital banditry win the day and plunder your lands . . ."

According to his LinkedIn page, Mr. Martin was working as a government contractor at the NSA and Pentagon while trying to obtain his doctorate from UMBC.

In his government work, Mr. Martin was assigned to a unit that looked for holes in the U.S. intelligence apparatus using a process called "red-teaming," said Rep. C.A. "Dutch" Ruppersberger (D., Md.) in an interview.

Red teams are internal hacking groups that look for flaws in networks to help make them more secure. Team members can have access to some of the government's most sophisticated hacking tools. Mr. Ruppersberger, who received a classified briefing on Mr. Martin's case, said he didn't know exactly what Mr. Martin's work involved but called him "very knowledgeable."

"He was working in a sensitive area where they trusted his expertise," he said. Mr. Martin passed at least one polygraph test, Mr. Ruppersberger added.

The NSA didn't respond to requests for comment. Mr. Martin's lawyer, Jim Wyda, also didn't respond Thursday, but said Wednesday the case amounted only to allegations.

Mr. Martin's LinkedIn page doesn't mention his affiliation with Booz Allen or the NSA, saying only that he worked "for various cyber related initiatives across DoD [the Department of Defense] and the IC," or intelligence community.

On his LinkedIn page, Mr. Martin doesn't mention the interest in PTSD cited by Mr. Rada. It says he graduated from the University of Wisconsin in 1989. His service in the Navy, confirmed by the military, began in 1988, something he described as "not just a job, but an adventure as well."

Washington Post

Arrest of NSA contractor highlights growing concern over insider threats

Friday, 07 October 2016

Byline: Christian Davenport

Section: general

Washington - The arrest of a National Security Agency contractor charged with stealing highly classified material is the latest example of a trend that officials say can be every bit as dangerous as an outside hacker: the insider threat.
The federal government has been increasingly concerned about the ability of its own employees and contractors to use their positions to walk away with troves of sensitive information. And it has tried to

implement new safeguards to not only better secure important data but also monitor the people with access to it.

Fears over insider threats intensified after the breach by former Army Pfc. Chelsea Manning and Edward Snowden, an NSA contractor working for Booz Allen Hamilton. But with the revelation that Harold Thomas Martin III was arrested in August and charged with theft of government property and unauthorized removal and retention of classified materials, there will be even greater scrutiny of how the nation protects its secrets, officials said.

The allegations against Martin, 51, of Glen Burnie, Md., suggest "that our counterintelligence abilities are still inadequate," said Steven Aftergood, the director of the Project on Government Secrecy for the Federation of American Scientists, "and that the kinds of precautions that would be necessary to prevent removal of highly classified material are not in place. ... It simply should not be possible to remove information from a classified system without supervision by somebody else. And evidently that kind of supervision was lacking here."

Martin's federal public defenders said in a statement that the charges against him were "mere allegations." "There is no evidence that Hal Martin intended to betray his country," the attorneys said.

In response to the Manning WikiLeaks leak, President Obama in 2011 issued an executive order that established a National Insider Threat Task Force and required all federal agencies that handle classified material to institute programs to seek out saboteurs and spies.

Agencies began monitoring their computer networks with renewed scrutiny and tracking employee behavior for signs of problems. Even workers with the highest clearances face additional surveillance.

The Pentagon's Defense Security Service announced this year that contractors will be required to implement programs that are designed "to detect, deter and mitigate insider threats." Contractors will be required to designate a senior insider threat official to oversee the program and provide training on how best to implement it.

While many details of the Martin case are not yet known, it is clear that it is not good for Booz Allen to have a second employee charged with stealing secrets from one of its most important customers, officials said.

"When a government employee does something like this, it is a scandal of one sort or another," said Loren Thompson, a defense industry consultant who also serves at the Lexington Institute. "But when a contractor is involved, it's potentially a business-threatening situation."

In an SEC filing, Booz Allen said that "we immediately reached out to the authorities to offer our total cooperation in their investigation, and we fired the employee. We continue to cooperate fully with the government on its investigation into this serious matter."

It added that there have "been no material changes to our client engagements as a result of this matter."

After the Snowden scandal, Booz Allen vowed to strengthen its security procedures. And critics have blasted the nation's intelligence community for loose controls, especially over contractors. But contractors remain a vital component to the United States' national security and intelligence establishments, so much so that "the system would not function without them," Aftergood said.

Chris Taylor, a longtime defense industry executive who teaches a class on the business of national security at Georgetown University, said that the threats the country faces are very complex and moving so fast that it makes sense to tap outside expertise.

"Any bureaucracy has an optimum speed at which they can operate," he said. "And if they're wise enough to realize those constraints keep them behind the power curve, they look outside for capacity to help them get ahead."

Several top defense firms have developed technologies designed to root out insider threats for government agencies and corporations. Lockheed Martin provides a service called Wisdom, which it says acts as your "eyes and ears on the Web." On its website, the company says that "insider threat losses are escalating at an alarming rate, with trade secrets and [intellectual property] theft projected to double in 2017."

Booz Allen, which came under intense scrutiny after Snowden walked off with some of the NSA's most closely guarded secrets, also helps organizations root out rogue employees. Last year, it announced a partnership with Raytheon, which offers a service that can give organizations the ability to digitally record the activity on their employees' computer screens and play it back - even in slow motion.

"Organizations are paying more attention to protecting their enterprises against the growing cyberthreats, and as a result, they are putting more personnel, IT and consulting resources toward managing this risk," Brad Medairy, a Booz Allen senior vice president, said at the time. "While managing the outside risk is critical, equally as important is the threat from within."

The detection programs use artificial intelligence and machine learning to create profiles of employees based on their activity, vacuuming up reams of data: Every time an employee swipes their badge to get into the building, every time they log on to their computer, the phone calls they make, the amount of email sent and received, the files they access, the data they upload.

"All these things generate a breadcrumb trail of your activities," said Chris Kauffman, the chief executive of Personam, a Northern Virginia company that focuses on insider threats. "Then it's up to the machine learning algorithms to sift through the data to establish patterns."

It tracks "anomalies" such as off-hour entries into the building or when large files are downloaded. Kauffman said his company's system caught rogue attorneys who were surreptitiously making electronic copies of case files.

Even so, insider threats pose a delicate and difficult challenge and can be hard to detect, especially since large amounts of data can be downloaded quickly and stored on tiny devices.

"The problem with insider threats is that they're not trying to infiltrate the place," Thompson said. "They are already there, and they know most of the procedures guarding information. When you know those procedures, you can develop better ways of working around them."

Daily News and Analysis

ATS looks for terror clues on social media

Friday, 07 October 2016

Byline: Ritesh Shah

Section: general

Ahmedabad - If you are active on social media, don't be in a hurry to post likes or follow any content that has anything remotely to do with terrorism, atrocities, riots, extremist propaganda, and other such topics. For, along with physical spaces, the Gujarat Anti-Terrorism Squad has increased its surveillance in cyber space too. All major social networking sites, including Facebook, WhatsApp and Twitter, are under observation. Following the Uri attack and the surgical strikes by the Indian Army, the ATS has been keeping track of content being posted on the sites.
Whenever someone posts a like or follows content related to terrorism or extremist propaganda, the person comes on the radar of ATS. The person's movements are monitored. In Gujarat, maximum likes to sensitive, or potentially volatile, content are posted from Ahmedabad, Vadodara, Bharuch, Navsari and Valsad.

ATS officials are also keeping tab on visitors of terrorism convicts lodged in jails across the state. According to authorities, their movements could help the cops find out about sleeper cells. Suspects are already under observation on social media. To bust the sleeper cells, the state agencies are working in tandem with central agencies like IB, RAW and NIA among others. The Coast Guard too has been sharing information about activities at sea and coasts.

Informer network has been strengthened. Those who have been in touch with the terrorists earlier too are being monitored.

According to ATS sources, calls made between Gujarat and Pakistan are being monitored. KK Patel, DySP-ATS, said "We are taking all fresh inputs seriously. Every input is probed thoroughly. We are monitoring activities in jails too. We are not restricting ourselves to social media users in Gujarat. Suspicious posts from outside state and country too will be scanned." "Our network is spread in Bangladesh, Pakistan and other countries. But, we cannot do anything till we get evidence," Patel added.

ABC News

NSA Contractor Who Allegedly Stole Top Secret Info 'More Weirdo Than Whistleblower,' Officials Say

Thursday, 06 October 2016

Byline: Multiple reporters

Section: general

New York - The National Security Agency contractor who federal authorities say took top secret information from the NSA is being described as "more weirdo than whistleblower," senior officials told ABC News.
Harold Martin, 51, was arrested in late August in what neighbors described as a dramatic FBI raid, but it was not until Wednesday that his curious case was revealed in a criminal complaint. In court documents, the FBI says Martin took home physical documents and information stored on digital devices, some of which was sensitive compartmented information (SCI), the highest level of classification.

It was information that the FBI said, if made public, would "reasonably be expected to to cause exceptionally grave damage to the national security of the United States." In all, the Department of Justice said investigators seized "thousands of pages of documents and dozens of computer or other digital storage devices and media" that held "many terabytes of information."

Although Martin worked at Booz Allen Hamilton, the same contractor for whom Edward Snowden worked, and was apparently able to slip through the NSA's security with highly sensitive information, as Snowden did in 2013, officials said overnight that that appears to be where the similarities between the two end.

It is unclear why Martin, a Navy veteran, allegedly removed so much sensitive information from his workplace and allegedly stored it in his home, nearby woodsheds or his vehicle, but he has not been

charged with espionage -- indicating to some former officials that this case may not be as serious as Snowden's. The Department of Justice said Tuesday that if convicted, Martin could face up to 11 years in prison - - one year for unauthorized removal of classified material and 10 years for theft of government property. Snowden, however, could face a far harsher prison sentence, should he return to the U.S. from Moscow; the U.S. government has said the death penalty will not be sought.

"It's not a repeat of Snowden, but it is another insider," Chris Inglis, a former NSA deputy director, told ABC News Wednesday. "It could be quite harmful, but [so far] it's not as malicious or nefarious."

Jim Wyda, a public defender assigned to Martin, said there is "no evidence Hal Martin intended to betray his country."

"What we do know is that Hal Martin loves his family and his country. He served our nation honorably in the United States Navy, and he has devoted his entire career to serving and protecting America. We look forward to defending Hal Martin in court," Wyda said.

Regardless of Martin's intentions, the incident is another embarrassment for the NSA, coming three years after Snowden made off with a cache of data that exposed dozens of NSA surveillance programs. It is unclear whether Martin purportedly absconded with his data before or after post-Snowden security reforms were put in place.

"When you download this kind of top secret information off the NSA network into your own computer or into a thumb drive, alarms should go off. Apparently they didn't," said former White House cybersecurity adviser and current ABC News consultant Richard Clarke.

Martin's former employer, Booz Allen, released a statement Wednesday saying the company fired one of its employees, without identifying Martin, after learning of his arrest and that the firm continues to work with law enforcement.

The federal complaint complaint says Martin was interviewed by federal agents in late August and, when "confronted with specific documents, admitted he took documents and digital files from his work assignment to his residence and vehicle that he knew were classified." He allegedly said he knew what he had done was wrong.

Boston Herald

NSA Director Denies Mass Scanning of Yahoo Emails

Friday, 07 October 2016

Byline: Jordan Graham

Section: general

Boston - Top U.S. intelligence officials denied a blockbuster Reuters report claiming Yahoo built special software to scan emails to hundreds of millions of accounts, while a subsequent New York Times report claims the snooping was limited to suspected members of a terrorist organization.
"That would be illegal. We don't do that, and no court would ever grant us the authority to do that. We have to make a specific case. And what the court grants is specific authority for a specific period of time for a specific purpose," said Adm. Michael Rogers, director of the National Security Agency, speaking at the Cyber Security Summit at Massachusetts Institute of Technology Oct. 5.

"We have a legal framework in this nation that enables the government ... for specific reasons, under specific conditions, to make a case before a judge in which we're able to show a judge we have reason to believe that there is threat here to the United States associated with specific individuals and a judge grants, simplistically, authority for a specific purpose for a specific period of time to access data."

On Tuesday, Reuters reported Yahoo had built custom software for the U.S. government that scanned incoming emails to millions of accounts.

"I've read this real quickly and I thought, well, this is a little speculative," Rogers said.

In a statement, Yahoo called the story "misleading."

After Rogers spoke yesterday, The New York Times, citing sources, reported the order from the Justice Department required Yahoo to search for a "digital signature" used by a state-sponsored terrorist organization.

The Times said Yahoo modified its existing spam, virus and child pornography filter to look for messages with the digital signature.

According to the report, the search was unusual in that every email was scanned for the specific signature, rather than searching for a specific user's account. The Justice Department was able to convince a judge that signature was unique to the terrorist group. The search is no longer ongoing, the Times said.

Associated Press

After latest NSA breach, does agency do enough to protect classified data?

Friday, 07 October 2016

Byline: Staff report

Section: general

Washington - The arrest of a National Security Agency contractor accused of stealing classified information represents the second known case of a government contractor being publicly accused of removing secret data from the intelligence agency since 2013.
The latest arrest came despite efforts to reform security after the Edward Snowden disclosures, especially in regard to insider threats.

Harold Thomas Martin III, 51, of Glen Burnie, Maryland, was arrested by the FBI in August, after federal prosecutors say he illegally removed highly classified information and stored the material in his home and car. A defense attorney said Martin did not intend to betray his country.

The arrest was not made public until Wednesday, when the Justice Department unsealed a criminal complaint that accused Martin of having been in possession of top-secret information that could cause "exceptionally grave danger" to national security if disclosed.

The fact that Snowden and now Martin -- both working for Booz Allen Hamilton as contractors for NSA -- were able to leave the NSA with highly classified documents, especially given the supposed security upgrades put into place, raises the question of whether the intelligence agency's efforts to tighten internal security afterward were effective or adequate. The NSA declined to comment.

"One key thing we don't have visibility into now is how he was caught, because that would provide some insight into whether the reforms that were put in post-Snowden were effective or not, or their relative efficacy," said Rajesh De, who was the NSA's general counsel when the Snowden story broke and remained there until last year. Snowden's 2013 theft of documents that were leaked to journalists revealed the NSA's bulk collection of millions of Americans' phone records.

Rep. Adam Schiff of California, the senior Democrat on the House Permanent Select Committee on Intelligence, said in a statement that "it is painfully clear that the intelligence community still has much to do to institutionalize reforms designed to protect (U.S. government secrets) from insider threats."

While details remain sparse, Martin's arrest also illustrates the difficulty of guarding against an insider threat given that employees that, by virtue of their clearance level and jobs, must be entrusted with the nation's secrets.

It's unlikely, given the thousands of people in the intelligence community, "you're going to be able to stop every incident of somebody taking documents if they're determined to do so. But the real question is how quickly can you detect it, how quickly can you mitigate the harm of any such incident," De said.

Adm. Mike Rogers, who heads the NSA, has repeatedly spoken since 2013 about efforts the agency has taken to ensure that such a thing doesn't happen again. He has said the agency tried to strike a balance so as to not overly upset workers, who are law-abiding citizens, with aggressive internal security mechanisms.

On Wednesday evening at a Harvard University event, Rogers declined to offer details on the ongoing investigation but officially confirmed that the contractor was employed at the NSA, which monitors and collects sensitive information and data, mostly from overseas.

Among the classified documents found with Martin, the FBI said, were six that contain sensitive intelligence -- meaning they were produced through sensitive government sources or methods that are critical to national security -- and date back to 2014. All the documents were clearly marked as classified information, according to a FBI affidavit accompanying the complaint.

The complaint does not specify which documents Martin is alleged to have taken. He was arrested around the same time U.S. officials acknowledged an investigation into a cyber leak of purported hacking tools used by the NSA. That toolkit consists of malicious software intended to tamper with firewalls, the electronic defenses protecting computer networks. Those documents were leaked by a group calling itself the "Shadow Brokers." The complaint does not reference that group or allege a link to Martin.

White House spokesman Josh Earnest said President Barack Obama takes the situation "quite seriously. And it is a good reminder for all of us with security clearances about how important it is for us to protect sensitive national security information."

The New York Times first reported the arrest of a NSA contractor who worked for Booz Allen Hamilton. Booz Allen said in a statement that after learning of the arrest of one of its employees, it contacted law enforcement authorities to offer its cooperation and fired the worker.

At Martin's home, investigators found stolen property valued at "well in excess of $1,000," the complaint said. He voluntarily agreed to an interview.

"Martin at first denied, and later when confronted with specific documents, admitted he took documents and digital files from his work assignment to his residence and vehicle that he knew were classified," the affidavit says. "Martin stated that he knew what he had done was wrong and that he should not have done it because he knew it was unauthorized."

He has been in custody since his arrest in August.

"There is no evidence that Hal Martin intended to betray his country," his public defenders, James Wyda and Deborah Boardman, said in a statement. "What we do know is that Hal Martin loves his family and his country. He served honorably as a lieutenant in the United States Navy, and he has devoted his entire career to serving his country. We look forward to defending Hal Martin in court."

The complaint charges Martin with unauthorized removal and retention of classified materials and theft of government property.

In 2013, journalists relying on classified documents stolen by Snowden revealed the NSA's bulk collection phone records and spurred a national debate on privacy and national security.

Rogers has said that since those revelations, he's repeatedly reminded the workforce of their agreement to never divulge the sensitive information they've been given access to. In prior comments, Rogers has said security isn't just about technical and insider threat preparation, but also about ensuring professional behavior.

"At times, I have some people telling me, 'Hey, what this should show you is you can't trust contractors,' " said Rogers, in a speech at Stanford University in 2014, noting that some of the biggest compromises of information came from direct U.S. employees. "This idea that you can't trust contractors, I just don't think I'm concerned about the long-term implications of that."

FCW. com

White House official: Cyberthreats continue to multiply

Friday, 07 October 2016

Byline: Sean D. Carberry

Section: general

Washington - A senior White House official said cyberthreats are figuring more prominently in President Barack Obama's daily briefing on intelligence and national security concerns.
"What I have found in the three-and-a-half years I have been in this position is that cyberthreats have consumed a greater and greater portion of the piece of the briefing that I do," said Lisa Monaco, assistant to the president for homeland security and counterterrorism.

Speaking at the Washington Post Cybersecurity Summit, Monaco said that almost on a daily basis now, she has to brief the president on some variety of cyberthreat.

"I've been struck by the breadth of the threats that we're facing, certainly against the U.S. government, against the private sector," she said.

Monaco added that cyberthreats are coming from an increasing range of actors --countries such as Russia, China, Iran and North Korea; criminal entities; and individual hackers.

"The other thing that is featured prominently in [the president's] briefing and in cyberthreats in general has been the range of tactics that we're seeing," she said. "Added to issues like denial-of-service attacks has been the increasing willingness of aggressive actors to use destructive attacks in the cyber realm."

In addition, the threat of data manipulation is growing. Monaco said the integrity of data is a near-, mid- and long-term concern.

In that regard, she acknowledged the recent probing of state election systems but echoed the argument of FBI Director James Comey and others that U.S. election systems are resilient and often not connected to any network, thereby protecting them from being hackers.

Intelligence officials and industry experts have attributed those probes and the hacks of Democratic National Committee servers to actors backed by the Russian government. Members of Congress have accused the Obama administration of failing to take public and assertive action against Russia, which they said is emboldened by the lack of retaliation and a clear policy of cyber deterrence.

"I disagree with the critics that we don't have a strategy or a deterrence policy," Monaco said.

She argued that Obama has worked to create an international set of norms for cyber behavior -- for example, by establishing that countries will not launch cyberattacks on one another's critical infrastructure and will not conduct cyber espionage for economic purposes.

"When countries violate those norms, there's an isolation of that country, there's an agreement that you can impose sanctions," Monaco said. "Maybe there is a consideration that there's an act of aggression if those norms are violated, so there's a framework there."

She added that the administration continues to build a response framework based on the broad question of what is in America's national security interest.

"We will respond in a time and place and manner of our choosing, and when we do so, we will consider a full range of tools -- economic, diplomatic, criminal law enforcement, military -- and some of those responses may be public and some of them may not be," she said.

The same guiding philosophy is used to respond to terrorism or any military or intelligence actions against U.S. interests, she added.

Furthermore, any public declarations or actions must not reveal the sources and methods the U.S. used to gather intelligence and attribute an attack to a particular actor, Monaco said.

She cited the U.S. decision to confront China over its cyber espionage as an example of how publicly attributing malicious cyber activity can have a deterrent effect.

"We've seen a diminishment in that behavior [by China]," Monaco said. "However, I think this is something we have to be continually vigilant on and be very clear, as we have been with the Chinese, that we expect adherence to this commitment," she added in reference to the agreement reached between China and the U.S. to fight economic cyber espionage.

In addition, the U.S. continues to face the threat of the "malicious insider," she said, and she cited the Justice Department's arrest of a Booz Allen Hamilton contractor who is alleged to have stolen National Security Agency software used to hack foreign adversaries.

"What this case and others have pointed out is we can't completely guarantee that we can eliminate the threat of a determined insider who is determined to steal information," Monaco said.

Jakarta Post

Kaspersky Lab hosts annual Cybersecurity Weekend in Bali

Friday, 07 October 2016

Byline: Desy Nurhayati

Section: general

Bali - Global cybersecurity company Kaspersky Lab is set to hold the Cybersecurity Weekend for Asia Pacific countries in Jimbaran, Bali, on Friday.
During the annual event, the company's experts and renowned leaders in cybersecurity will provide updates on the latest cybercrime trends, particularly in the financial industry. They will reveal secrets and tips for businesses to protect themselves and survive in a world of cybersecurity threats.

"Our objective for the event is to share our expertise in cybersecurity and to show the audience different perspectives of cybersecurity, focusing on the financial industry," Kaspersky Lab Asia Pacific's head of corporate communications, Jesmond Chang, said on Thursday.

Information technology for financial transactions is advancing at a tremendous pace in Asia Pacific. As a result, many organizations and users tend to forget to implement cybersecurity.

"We hope that by creating more awareness, the public will have a better understanding of cybersecurity and together we can move towards making the cyberspace a safer place," Chang said.

The Australian

'Top-Down' Grid A Gift For Savvy Cyber Attacks

Friday, 07 October 2016

Byline: Roger Bradbury

Section: Commentary

Commentary: The shutdown of South Australia last week is a near- perfect example of the impact of a cyberattack. A one-day shutdown led to hundreds of millions of dollars in losses to the economy, disruptions to citizens' lives and an unravelling of political, social and economic certainties.
Sure, South Australia has peculiarities that made it particularly susceptible to such an event. But the shutdown nevertheless shows in high relief the vulnerability of today's interconnected systems of critical infrastructure.

What we saw last week was not just a loss of the electricity network but also the shutdown of the other infrastructure networks: telecommunications, water, sewerage, transport, financial services, the internet and so on.

Advanced Western societies have spent the past 30 years refining and interconnecting their critical infrastructure, improving their efficiency but also increasing their vulnerability. We've reached the point where the interconnections are more or less complete, so every critical infra-structure -- energy, water, fin-ance, transport or cyber -- is dep-endent, to a high degree, on every other.

This interdependency means disruptions in one infrastructure quickly spread to all other interconnected systems. And because these infrastructures -- with the exceptions of cyber and transport -- are

organised in a top-down hierarchy, it means if the disruptions can spread up to the top of the tree, they can then spread down to the rest of the network.

This is what happened in South Australia. Excessively hierarchical networks in key infrastructures enabled -- one may say encouraged -- the collapse of each of those networks.

(Note: Roger Bradbury is a professor in the Australian National University's National Security College.)

Gulf News

'Undertaking' the mission of recalibrating cyber security

Friday, 07 October 2016

Byline: Faisal Al Bannai

Section: general

Dubai - Over the last 20 years of technological innovation, it has become increasingly apparent that successful start-ups have a much more disruptive impact on the status quo, developing radical new business models or actually creating ones that previously did not exist.
What lies at the heart of this deeply disruptive ability is twofold. The first being the fact that the very nature of modern technology today allows an instantaneous engagement with a huge number of entities and people across continents. The second is because successful start-ups are entrepreneurial; entrepreneurship being derived from the French word that means "to undertake".

Thus successful start-ups have a sense of "undertaking" in their mission; meaning they have a purpose for being and are looking to find a solution to a set of problems, or even better, create altogether new use cases that render earlier problems irrelevant.

Cyber security is in need of an entrepreneurial approach, which is to say, a requirement for new ideas, new ways of doing things, and most fundamentally, a new attitude to what protection and resiliency really mean in a digital world.

The best start- ups and entrepreneurs do not exist for existence's sake. They are constantly in motion, driven by the "undertaking" to make things quicker, easier, better, more resilient. They ground themselves in the techniques and industry norms of the day but then go on to leap towards new problem-solving ideas, which challenge the status quo and in some cases obliterate it.

The exponential growth in digital networking means that we have entered uncharted territory with respect to the way digital infrastructure is utilised and information transmitted. With the sheer volume of digital information being exchanged and the importance of such data in allowing us to live our daily lives as normal, adding immunity to this environment requires an entrepreneurial flair, an "undertaking" to protect digital infrastructure end-to-end.

Last month, the UK's security agency GCHQ announced the launch of a cyber security accelerator as part of a programme to create two "world-leading" innovation centres. The accelerator will see selected start-ups receive a grant and be able to work in the building.

Creation of the accelerator is the first part of a renewed attempt by the UK government to invest in cyber security. In November 2015, then-Chancellor George Osborne said £1.9 billion ($2.4 billion) would be made available for investing in cyber defences.

The accelerator will be the first of two innovation centres where cyber start-ups can base themselves in their crucial early months, and which can become platforms for giving those start- ups the best possible support.

As well as using the funding for developing start-ups and the UK's cyber scene, the money would also be used for launching active defence programmes against national threats.

While not exclusively focused on cyber security, in Dubai a bold accelerator programme has also been launched with the aim to utilise technology to solve national-level challenges.

The Dubai Future Accelerators is the world's largest government-supported accelerator, launched by Shaikh Hamdan Bin Mohammad Bin Rashid Al Maktoum, Crown Prince of Dubai and Chairman of the Dubai Future Foundation. The programme is in line with the directives of His Highness Shaikh Mohammad Bin Rashid Al Maktoum, Vice-President and Prime Minister of the UAE and Ruler of Dubai, and identifies ground breaking companies from around the world, offering them the opportunity to find and test new solutions to real-life challenges.

We welcome the rise of increased disruption in cyber security and believe it is a necessary development in bolstering defences for every nation, enterprise, and individual.

Le Mag (Maroc)

Presse: le 'Maroc' remplacé par 'Califat' sur une carte d'un avion d'Air France

Thursday, 06 October 2016

Byline: Adam Sfali

Section: general

Paris - Dans un avion d'Air France quelqu'un a joué avec les cartes de trajectoires de vol, vus par les passagers sur les écrans de l'avion.
Selon le site du journal britannique The Telegraph, citant des sources des services secrets français, dans le cadre d'une série de tentatives de sabotages qu'auraient subit la compagnie Air France, des membres du personnel du transporter aérien français, présumés radicalisés auraient bidouiller les cartes de trajectoires de vol sur un avion en s'attaquant à deux pays, le Maroc et Israël.

Ainsi, sur une carte affichée sur les écrans de l'avion, les passagers pouvaient lire un nom bizarre collé sur la carte du Maroc : " Califat" probablement en référence au prétendu califat autoproclamé par les terroristes de daech en Irak. Sur une autre carte, le nom d'Israël a été effacé et remplacé par Gaza.

Selon les mêmes sources, Air France serait victime d'une série de tentatives d'attentats dont les coupables ne seraient d'autres que des membres de son personnel naviguant et au sol.

L'une des plus dangereuses actions aurait été une tentative de provoquer un accident aérien en déconnectant le cockpit d'un avion des commandes de ses moteurs. Les services secrets français disent enquêter sur ces dangereuses tentatives, mais apparemment sans grands succès.

Ottawa Citizen
Eyes in sky hit operational turbulence
Tuesday, 11 October 2016
Byline: David Pugliese

Ottawa - Canada's much-vaunted surveillance planes operating over Iraq were so limited in the information they could collect and share with allies, Canadian military personnel planning CF-18 attacks had to rely on the U.S. for data, according to documents obtained by the Ottawa Citizen. The briefing, produced last year on lessons learned from operations in Iraq in 2014, also pointed out efforts to set up ball hockey facilities and a Tim Hortons for personnel at a base in Kuwait should take a back seat to getting key components of the mission in place.
Canada initially contributed special forces, Aurora surveillance aircraft, a refuelling plane and CF-18 fighter jets to the international coalition battling Islamic extremists.

The Liberal government withdrew the jets, but expanded the number of special forces and kept the refuelling planes and Auroras on scene.

Canadian officers have claimed from the beginning of the mission the upgraded CP-140 Auroras are among the most advanced surveillance aircraft in the world. But the "lessons learned" document, obtained through the Access to Information law, tells a different story.

"The CP140 deployed without the organic capability to share their data with coalition partners," it notes.

In addition, the software needed to process some CP-140 surveillance data was not available and the aircrews needed "greater experience operating over land."

The Aurora is primarily a maritime surveillance plane, but the upgrades allow it to collect data on ground targets.

The problems didn't stop with the Auroras. There were concerns about the overall lack of ability to share information Canada collected from various sources with its allies. In addition, the Canadian Forces had problems accessing coalition intelligence data without having to go through a U.S. military intermediary.

Gathering information about targets the CF-18s were to attack proved difficult. Problems with the planes' targeting pods "severely" limited some information gathering, although the details were censored.

"Poor information" was provided to those deciding on targets. There is a need to increase the capability to "contribute to target discovery," other comments in the briefing point out.

Military staff asked about the lessons learned said while ball hockey and a Tim Hortons trailer were "a nice boost," these "projects must wait well into the sustainment phase after the mission's essential components are all in place."

Other issues included: Significant delays in del ivering communications equipment and having enough trained personnel.

Military communications personnel sent back to Canada within seven days of arriving in Kuwait, and before the systems were up and running.

Some military personnel, who travelled overseas on civilian flights, had to use their own credit cards to pay up front, then had trouble getting reimbursed. In some cases, they had to spend up to $1,000 just for baggage.

Civilian contractors supporting the refuelling aircraft detachment were not properly prepared for work in Kuwait or the type of accommodation they were given.

There should be a 24/7 duty desk to deal with problems encountered by those on overseas missions. "A list of people who can actually help with problems would be nice," said one person. "Help accounts suck. They are rarely monitored. Real people with real contact lists only."

Commanders back in Canada weren't spared criticism either. Some of those serving in Kuwait questioned the abilities of the Ottawa-based Canadian Joint Operations Command, which co-ordinates military missions at home and around the world.

"Despite the best of intentions and a desire to do so, CJOC is incapable of conducting true 24/7 operations, at least as it concerns targeting," said one critic.

Canadian Forces spokesman Capt. Vincent Bouchard said in an email many of the challenges outlined in the document are common when setting up a multinational operation abroad. "The capabilities the Block III CP140s brought to theatre were new, both to the RCAF and our allies," he said. "As it was expected, it took time to learn how to make the most of these new capabilities in the context of a multinational operation."

Bouchard said the points raised in the documents were dealt with and the Aurora detachment continues to provide valuable surveillance information for the coalition.

He repeated the Canadian military's statement the Auroras are "world-class intelligence surveillance and reconnaissance aircraft." Ottawa Citizen dpugliese@postmedia.com Twitter.com/davidpugliese

Ottawa Citizen

Government ramps up Facebook advertising
Tuesday, 11 October 2016
Byline: Jason Fekete

Ottawa - Rapidly changing how it communicates with Canadians, the federal government is on pace to spend more on Facebook ads in the Liberals' first year in office than it did between 2006 and 2014 combined.
The Liberal government spent at least $3.8 million on Facebook ads between November 2015 and June 2016 targeting Canadians and foreigners of various age groups and demographics, and is on pace to spend well over $6 million during Prime Minister Justin Trudeau's first year in office, according to documents tabled in the House of Commons.

The data from dozens of departments, agencies and Crown Corporations was tabled in response to a question from Conservative MP Martin Shields.

By comparison, the federal government spent $5.8 million on Facebook ads between April 2006 and early June 2014, according to a federal government response to a similar question two years ago.

As well, the spending on Facebook ads during the Liberal tenure doesn't include that from CBC/Radio-Canada, which was one of the biggest spenders detailed in the last response. The government declined to release the information this time around, saying it's "competitive information." Government of Canada annual advertising reports show the rapidly changing trend that sees federal departments and agencies looking to contact Canadians more through the Internet.

In the 2011-12 fiscal year, just over 10 per cent of federal government media placements purchased through its agency of record were on the Internet (including search and display ads, and paid social media ads). That number more than doubled to over 25 per cent of media placements by 2014-15. (Data for the 2015-16 fiscal year won't be released until January).

Some of the biggest government spenders on Facebook ads were agencies and Crown corporations that often don't garner much attention, but turned to social media to promote various events, exhibits and government programs, as well as market Canada internationally.

The details on the spending also show how specific a targeted audience the government is going after.

Destination Canada, formerly the Canadian Tourism Commission, spent more than $1.8 million between November and July on Facebook ads, most of it going after "potential travellers to Canada" and to "raise awareness" by promoting videos and links to Internet pages.

Immigration, Refugees and Citizenship Canada coughed up $467,300 for Facebook ads, including $67,300 to "raise awareness among Canadians to get involved and support efforts in welcoming Syrian refugees."

The primary target audiences and demographics were "Canadians that may wish to donate, assist or sponsor refugees" as well as "Canadian youth." The secondary target audiences were "community stakeholders and partners," Canadian media, provincial/territorial and municipal governments, and major corporations.

The other $400,000 spent by the department targeted foreign travellers, students and temporary foreign workers age 18-65 coming to Canada, to inform them of the need to obtain an electronic travel authorization.

The Royal Canadian Mint spent more than $147,000 on Facebook ads to promote specialty coins it produced, including a "Batman vs. Superman $20 Silver coin" to English and French Canadian comic fans, a "gingerbread coin," Star Wars coins, and one promoting the 40th anniversary of the Toronto Blue Jays, among many others.

Via Rail spent more than $437,000 promoting its rail services, but didn't provide specifics on the various campaigns.

Statistics Canada spent about $228,000 on Facebook ads to promote the 2016 Census. Statistics Canada's ad campaigns were broken down into various target audiences and demographics, including the mass population, aboriginal population, "ethnic groups," the male population and the "unattached and mobile population."

Export Development Canada spent nearly $130,000 on Facebook ads targeted at small and medium Canadian companies that "export or have interest in exporting," highlighting various trade agreements, managing the risks of international trade, and several other initiatives.

Various federal museums spent tens of thousands of dollars combined targeting audiences in Canada and abroad for various exhibits.

The Canada Science and Technology Museum spent $15,000 promoting Star Trek: The Starfleet Academy Experience to adults in the Ottawa/Gatineau area, while the Canadian Museum of History spent thousands promoting exhibitions on such things as Vikings and Thomas the Train.

CBC.CA
CSIS, Bill C-51 and Canada's growing metadata collection mess
Tuesday, 11 October 2016
Byline: Steven Zhou
Section: Opinion

Opinion: Much has been made over whether the Canadian Security Intelligence Service, Canada's spy agency, should be armed with broader powers to "disrupt" what it perceives as terrorist plots. A report tabled this month by the Security Intelligence Review Committee, which watches over CSIS's work, notes that while the spy agency hasn't abused its new powers of disruption, its bulk data collection program needs to be scaled back.

It's easy to think of CSIS and other spy agencies as shadowy organizations that carry out James Bond-like "missions" involving cool gadgets and high-tech weaponry, but the Snowden leaks, among other revelations, have shown the public that metadata collection (online communications, phone logs and other electronic exchanges that can be intercepted in enormous amounts) now constitutes the state's primary instrument of control.

Privacy Commissioner Daniel Therrien recently called upon legislators (the Liberals in particular) to amend certain aspects of Canada's national security laws in order to address the issue of metadata collection.

In particular, Therrien referred to the Communications Security Establishment, which seems to get a lot less public scrutiny than CSIS. The CSE is responsible for collecting massive volumes of foreign communications through "signals-intelligence," (or "sigint"), but also tends to drag up large amounts of Canadian metadata as well, which it isn't supposed to be doing.

This is also a point that Jean-Pierre Plouffe, the commissioner who provides oversight for the work the CSE does, has consistently made. Plouffe tabled his annual report earlier in the year and revealed that the CSE illegally and inadvertently shared a large amount of metadata with Canada's "Five Eyes" intelligence allies: the U.K., U.S., New Zealand and Australia.

The shared metadata could have included the private communications information of Canadians. He noted that there's no way to tell exactly how long the CSE has been doing this, and that the agency has also been buying faulty software that should have worked to protect people's privacy.

Given the amount of work and data collection that CSIS and the CSE both do, it's hard to see how each agency's mandate should be expanded without a corresponding expansion of the powers of watchdogs who monitor their work.

Under Stephen Harper, the Security Intelligence Review Committee wasn't even fully staffed, and for all their promises to reform Canada's national security apparatus, Justin Trudeau's Liberals still haven't released any details about how they want to do that.

Meanwhile, Therrien's report also reveals that many government agencies didn't go through with the proper protocol to assess whether they have the necessary infrastructure in place to protect people's privacy, as each department is given more leeway to share this data with each other.

This is one of the main features of Bill C-51, which is the same omnibus bill that gave CSIS their new powers to "disrupt."

Therrien reported that as each government agency is given permission to share data with other agencies, the responsible thing would have been to assess how these newly acquired capabilities would impact Canadians' privacy. Rather than carry out this assessment and look out for the Canadian people, many agencies that acquired this power under C-51 simply chose not to do them.

Therrien stressed that the information-sharing regime mandated by C- 51 is "unprecedented" in its scope and that law-abiding Canadian citizens who aren't under suspicion shouldn't be caught up in it at all. Yet this country's sprawling metadata regime and national security agencies don't seem to have any powerful tools to ensure any meaningful level of privacy protection.

One can, for the moment, leave aside the issue of whether or not the collection of metadata is itself a smart and constitutional thing to do, but even if the answer is yes, there still needs to be a discussion over how to keep the scope of collection within the appropriate parameters. CSIS has since halted (for the time being) its bulk metadata collection programs, but the CSE has not.

And as threats like the Islamic State continue to exist and inspire like-minded terrorists across the world, the Canadian public seems to have put the issue of privacy on the backburner.

Bill C-51 anti-terror arrests without a crime concern legal experts

This complacency cannot continue if there's to be a meaningful check on the state's power to intrude upon the lives of its citizens.

Steven Zhou is a Toronto writer who has experience in human rights advocacy. He has worked for Human Rights Watch, OXFAM Canada and other NGOs.

The Hindu
Mumbai govt. law college website hacked
Tuesday, 11 October 2016
Byline: Gautam S Mengle

Mumbai - The website of the Government Law College in Mumbai could be the latest victim of the 'cyber war' supposedly being waged by Pakistani hackers on Indian websites in response to the surgical strikes in Pakistan by the Indian Army earlier this month.
Multiple sources inside the GLC confirmed to The Hindu that the Churchgate based institute's website was found to be hacked on Monday evening. The hackers left a message on the home page which claimed the hack to be the handwork of a group calling itself 'PakCyberPirates'. "To all Indians out there....surgical strike...." the message said.

Sources said that the hack was discovered by around 6:00 pm by a student of the GLC, who brought it to the notice of the some professors, after which the police were informed.

The 'cyber war' first began on October 3, when the website of the National Green Tribula based in Delhi was hacked by unknown persons who left pro-Pakistan slogans on the home page. A day later, the website of a Kerala based institute was also hacked and a similar message left by the perpetrators.

Text messages to Inspector General of Police (Cyber) Brijesh Singh, Maharashtra Police and Deputy Commissioner of Police (Cyber), Sachin Patil did not receive any response.

Times of India
Hack your targets with machetes, Islamic State tells lone wolves
Tuesday, 11 October 2016
Byline: Bharti Jain

New Delhi - Islamic State (IS) modules and 'lone wolves' in India have lately been instructed by their handlers to focus on hacking their targets, particularly foreign citizens, to death with big chopping knives or machetes.
"We have gathered that IS modules and lone wolves here are being told by their handlers not to risk gathering explosives, assembling IEDs or illegally buying automatic weapons for attacks. Instead, all they need to do is buy big chopping knives or machetes, which would neither raise suspicion nor involve a huge cost," a senior intelligence official told TOI.

The first case of IS-inspired youths plotting beheadings came to light in July when a module led by terrorist Masiuddin alias Abu Musa was busted by West Bengal CID and machetes recovered. Now, members of the Kerala-Tamil Nadu module arrested last week have revealed that they too planned to hack foreigners to death in the two southern states.

The motive behind the proposed hacking attacks in India, according to top sources in intelligence agencies, is to create maximum impact in terms of terrorising people, given the gore and horror associated with them, and grab eyeballs, including that of international audience.

Agencies believe IS-inspired youth may also be looking to record these hackings and share the photos and videos with their handlers, so that they can be uploaded on IS's online forums to promote the outfit in India.

This trend was seen in Bangladesh, with the Dhaka attackers capturing the hacking of foreigners during the July 1 hostage situation in Holey Artisan cafe with their smartphones. These photos were later uploaded by IS.

"It has been noticed that IS modules are now largely operating as small, localised groups in different states -- particularly Maharashtra, Kerala, Tamil Nadu, Telangana and Karnataka. After the NIA busted a pan-India module in January leading to two dozen arrests across northern, southern and western states, IS handlers have been encouraging Indian contacts to work in smaller groups with minimal inter-connectivity. This is to escape surveillance and minimise arrests in case a module is detected," an intelligence officer said.

In the case of the Kerala-Tamil Nadu module busted recently, those arrested are believed to have gathered for a meeting at Kanakamala hilltop in Kannur to discuss plans for acquiring machetes when an NIA team, based on a specific intelligence alert, closed in on them and arrested five people. "Though they were discussing targeting Jews the plan, as per our assessment, was to hack foreigners to death in tourist hotspots in Kerala and Tamil Nadu," an intelligence officer said.

"In the case of the West Bengal module, the accused were arrested after they bought the machetes and before they could hack the members of a family that night. But we decided against waiting for the Kerala-TN youth to acquire the knives/machetes before arresting them," the officer added.

However, the threat of hacking attacks still looms, with many radicalised Indian youths in touch with IS handlers and motivators online. "We are keeping them under surveillance and would ask the agencies concerned to arrest them as and when the threat of their planning or executing an attack becomes imminent," the officer said.

Straits Times
Asean members should cooperate to fight full spectrum of cyber threats
Tuesday, 11 October 2016
Byline: Lim Yan Liang

Singapore - The Singapore Government wants to intensify Asean-wide cooperation to build a stronger cyberspace commons in a region where governments are vulnerable to a spectrum of cyber attacks, Minister for Communications and Information Yaacob Ibrahim said on Tuesday (Oct 11).
Speaking at the first Asean ministerial conference on cyber security at the Shangri-la Hotel, Dr Yaacob, who is also Minister-in-charge of cyber security, identified three areas where the group of 10 countries should focus its efforts in order to fight the "full spectrum of cyber threats - cybercrime, espionage, and other malicious activities".

The ministerial conference took place one day after the Government launched its National Cybersecurity Strategy, a wide-ranging document that maps Singapore's efforts to secure its online space.

The first is cyber capacity building so that Asean member states can deepen its capacity to fight malicious cyber activity.

This is crucial as a joint Singtel-FireEye study found that South-east Asian governments are more likely to be targeted for attack than other organisations.

Visitors trying out virtual reality goggles at a booth at the inaugural Singapore International Cyber Week at Suntec Convention and Exhibition Centre yesterday.

"Attack targets could range from financial to data theft, reputation as damage, and also disruption to our critical information infrastructure," he said.

To this end, Dr Yaacob launched a new $10 million Asean Cyber Capacity Programme, which Singapore will channel towards honing the technical skills and incident response capabilities of fellow Asean countries.

"The money will pay for resources, expertise and training so that we will be equipped to drive and take ownership of the cyber security agenda in our respective countries," he said.

Second, Dr Yaacob urged Asean members to tap into global efforts to build a trusted cyberspace, such as through international law enforcement efforts like the Interpol Global Complex for Innovation (IGCI) that is based in Singapore. "Countries have to actively support the IGCI for its continued success and effectiveness," he said.

"We can support the IGCI by seconding more Asean law enforcement officers to the IGCI. By partnering Interpol, we can conduct more joint operations against cyber criminals and enhance the collective safety and security of Asean."

Singapore will also contribute $900,000 to the CyberGreen global initiative that provides tools for a country to measure its level of cyber health, announced Dr Yaacob.

With this sponsorship, all Asean member countries will be able to access the CyberGreen platform through Singapore for free and be able to better identify different levels of threats and ways to counter them.

Third, Asean has to start a dialogue on cyber norms, and work towards developing a set of regional cyber norms.

"Cyber capacity building, cyberspace awareness, and cyber norms: these are three suggestions to Asean for enhancing cyber security cooperation," said Dr Yaacob. "Singapore is committed to these ideas, and we are backing our words with resources and investment."

New York Times
American Cellphones Ringing in Tehran

Sunday, 09 October 2016
Byline: Thomas Erdbrink

Tehran - Rushing for a plane to Tehran because of a family emergency, the Iranian-American businessman stuffed his mobile phone into his carry-on, forgetting to turn it off.
It was useless in Iran anyway, he knew. American mobile phones never worked in the country, and even after the recent nuclear deal, many economic sanctions remain in place, frustrating foreign businesses interested in cracking the Iranian market.

So it was something of a shock when, having fallen asleep after arriving at his sick grandmother's house in Tehran, the businessman, Faryar Ghazanfari, an intellectual-property lawyer, heard a buzzing coming from the bag.

At first, he thought it was an alarm. Then he picked up. "I couldn't believe what was happening," he said. "It was San Francisco. A colleague wanted an update on a patent case."

Until recently, an American phone in Iran would not receive any signal. But that has quietly changed. This past week, a spokesman for AT&T acknowledged that the company was providing voice and data service in Iran to its customers with American phones through a partnership with a local firm, RighTel. An employee at the Iranian company, fully owned by a state entity, confirmed the partnership.

While the announcement that Airbus and Boeing will provide dozens of jetliners to Iranian carriers garnered worldwide headlines last month, the deal that AT&T clinched in March, making it the only American provider to offer phone service in Iran, flew under the radar.

The agreement is one of the few signs that the promises President Hassan Rouhani made long ago of welcoming Western businesses and ending Iran's isolation are at last beginning to be realized.

"This is a step in the right direction," Masoud Daneshmand, an official at the Iran Chamber of Commerce, said of AT&T's partnership with RighTel. "The fact that phones are working in Iran and the United States is a sign of good will on both sides."

With its oil wealth and nearly 80 million consumers, Iran has long held out the promise of a lucrative, if elusive, market for Western companies. In the immediate aftermath of the nuclear deal in January and the lifting of many economic sanctions, there were heightened expectations in both countries that the day had finally arrived.

But enough sanctions remained that Western banks refused to finance commerce with Iran without specific licenses from the United States Treasury. That seemed to choke off most business opportunities outside the oil and gas sector and the airlines. But for whatever reasons, AT&T decided to move ahead, apparently determined to shun publicity about its moves.

It remains unclear how AT&T and RighTel will settle accounts. A representative for AT&T said the company would not disclose information on financial arrangements made with the Treasury or with its Iranian partner. One possible clue: RighTel is owned by the Social Security Organization of Iran, a state entity that has large stakes in several domestic banks.

The Treasury would also not speak about the deal, saying in a statement that it "generally does not comment on specific licenses or engagement with private parties."

Nevertheless, having working American mobile phones in Iran sends a powerful message that times are changing, albeit very slowly.

"Now we are, of course, hoping that the United States lifts all trade restrictions on Iran," Mr. Daneshmand said. "In return, we will lift visa restrictions for Americans."

In the past, Iranian interest in AT&T was of a different nature. In 2011, Iranian hackers targeted the carrier along with several other companies, dozens of banks and even a small dam in a suburb of New York, the Justice Department wrote in a complaint this year. Seven Iranian computer specialists who regularly worked for the Islamic Revolutionary Guards Corps were accused of carrying out the attacks.

AT&T still faces the many hurdles that all companies have in doing business in Iran. In addition to its endemic corruption and bureaucratic inefficiency, Iran works on a calendar different from the West's, with different months and a Thursday- Friday weekend. The communication infrastructure is poor but improving, and many websites are blocked by the government.

And there is still the possibility of opposition from conservative clerics and Iran's supreme leader, Ayatollah Ali Khamenei, who could end the arrangement in a flash if he felt it was inappropriate.

For Iranian hard-liners, direct service to the United States means yet another connection to the "Great Satan," the place they wish death upon in every Friday Prayer. For many of them, simply the idea of an ever-friendlier and familiar America is a threat to the founding ideology of the Islamic republic.

For many, perhaps, but by no means all. "If we get service in return, it is not that bad," said Mohammad Javad Helali, a Shiite Muslim cleric connected to the hard-line faction. "We just hope that the services will be free from infiltration by American intelligence services."

The opening up of phone service is undoubtedly a welcome surprise to Iranians and the approximately two million Iranians living in the United States, many of whom travel frequently to their home country.

Azad Jafarian, an Iranian-American filmmaker, said his mother had just flown in from Los Angeles through a connection in the Persian Gulf state of Qatar, and he smiled when he saw her turning off the flight mode on her cellphone, bringing it back to normal operating status.

What happened next startled him. "I was driving her home, I saw her swiping her phone, and seconds later the phone started ringing," Mr. Jafarian recalled. In a light panic, he told her to turn it off. "I was like, 'This can't be real.'"

Canberra Times
IT security Watchdog warns of tougher scrutiny Super funds targets for cyber attacks
Sunday, 09 October 2016
Byline: Clancy Yeates

Canberra - Australia's $2.1 trillion pool of retirement savings is being targeted disproportionately in serious cyber attacks on the financial sector, official figures suggest. Banks, insurance companies, and wealth managers all face an increasingly elaborate array of cyber attacks, but a recent survey by the financial regulator shows the superannuation industry was attacked most frequently within the sector. While financial institutions have not yet suffered a "material" loss from these incidents, the Australian Prudential Regulation Authority plans to take a tougher line in making sure the sector can fend off cyber attacks. APRA last week released the results of survey looking into cyber security incidents at 37 financial institutions between last October and this March, and how they were managed. More than half of the businesses had been hit with an attack serious enough to warrant involvement from executive managers in the 12months before the survey. The superannuation industry was the most likely to have been hit
by such an attack, with 75 per cent of funds experiencing a cyber security "incident" that was serious enough to report to executive managers. In comparison, 44 per cent of banks and 46 per cent of insurers suffered incidents that were elevated to such a level. APRA said it was possible that super was more attractive to perpetrators because of the high account balances, though it also said that super funds may have a different threshold for reporting cyber breaches up the management tree than banks. Even so, law enforcement official have previously said Australia's hefty pool of super is being targeted by cyber criminals engaging in identity theft. Across the entire financial sector, a fifth of respondents had experienced several "potentially high impact" incidents. These included "advanced persistent threats" - where attackers break into a network and steal information, often

for political or commercial motives - and "denial of service" attacks - which are designed to bring a website down. Fourteen per cent of institutions had been targeted in attacks where hackers use malicious software to infiltrate a network and make data unreadable, known as a "ransomware" attack. One in eight institutions had suffered attacks that could damage their reputations - such as having their websites defaced or social media accounts hacked. In response, APRA flagged tougher scrutiny in this area and said boards and top managers must be well prepared for handling cyber attacks. "APRA intends to lift the supervisory and regulatory expectations for regulated entities to not only secure themselves against cyber attacks, but to implement improved mechanisms to quickly identify and remediate successful attacks when they occur," it said. While Australian banks have not suffered "material" losses from cyber attacks, in 2014 about 76 million household bank accounts were compromised in a cyber attack on US giant JP Morgan. Local banks regularly highlight their attempts to combat cyber crime, with

Commonwealth Bank chief executive Ian Narev last week saying the bank spent an "inordinate amount of time and money" looking after customers' online data. Mr Narev told the government's banking inquiry these security concerns needed to be taken into account in the push from some committee members for a fresh debate about bank account portability, which would allow customers to change banks more easily. "We need to make sure that in terms of access to data, security of data, how the data are used those principles are absolutely sacrosanct," Mr Narev said.

The Daily Beast
Russia's Senior-Most officials' Ordered DNC Hack
Saturday, 08 October 2016
Byline: Shane Harris and Nancy Youssel

Washington - The Obama administration has concluded that "Russia's senior-most officials" ordered hackers to break into the computer networks of American political organizations in order "to interfere with the U.S. election process," intelligence and security agencies said in a joint statement Friday. The statement was the administration's first public attribution of the hacks against the Democratic National Committee and a second political institution to the Russian government. Privately, officials had said for the past few months that all signs pointed to an operation being directed by Moscow intended to meddle with the November election.

That evidence mounted as law enforcement and intelligence agencies sifted through technical details about the hack and eventually reached a consensus that Russia was to blame, a senior administration official told The Daily Beast.

The process continued "as the intelligence community gathered more information and got higher and higher degrees of confidence" attributing the hacks to Russia, the official said. The agencies, along with the Department of Homeland Security, came to a consensus "recently" the official added, without specifying a precise date, but he added that intelligence and law enforcement "worked as quickly as possible to release as much information as possible" without compromising sensitive sources and methods.

"The intelligence community has high confidence in its attribution into the intrusions in the [Democratic National Committee] and the [Democratic Congressional Campaign Committee] based on forensic evidence cited by a private cyber firm and the intelligence community's own review and understanding of the cyber activities by the Russian government," a second U.S. official told The Daily Beast.

The joint statement also attributed activities by three separate online organizations to the Russian campaign.

"The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed

efforts," the statement said. DCLeaks has posted stolen emails of current and former U.S. officials. And Guccifer 2.0, which claims to be an independent hacker, had been believed to be the source of stolen DNC emails to WikiLeaks, which published them last summer.

Officials also said they had detected Russian attempts to target state and local-level elections systems.

"We also worked as quickly as possible to release as much information as possible in order to provide state and local officials sufficient time to fortify their infrastructure," the official said. The Department of Homeland Security and the FBI have put state elections officials on notice that hackers have been trying to access voter registration files and could cause havoc on Election Day. So far, 25 states have asked the department to help scan their computer networks for security weaknesses.

Notably, the statement didn't blame the Russian government for targeting state elections systems, but it did say the activity had been traced to servers owned by a "Russian company."

But the Obama administration did squarely blame the DNC hacks on the Kremlin--and not just lower-level officials. The authorizations for the hacks came from the "most senior levels of the Russian government," a U.S. official told the Beast.

The administration's decision to name Russia raised two immediate questions: Why now? And what next?

The first official said the timing had nothing to do with Sunday's presidential debate or the election campaign in general. Privately, some Republicans groused that the decision appeared motivated to bolster suspicions that the Russians are hacking Democratic organizations in order to boost the campaign of Donald Trump.

The official also said the timing of the statement had nothing to do with the administration's decision to break off negotiations with Russia over and end to the civil war in Syria. Earlier Friday, Secretary of State John Kerry accused the Russian government of "war crimes" for attacks on civilian institutions, including hospitals, raising an already tense U.S.-Russia relationship to a new level.

So what will the U.S. do now that it has blamed Russia for the hacks?

"Denouncing these Russian attacks is a good first step but what if anything will Obama do to make Putin pay a price for his subversion?" Max Boot, a senior fellow at the Council on Foreign Relations, told The Daily Beast. If Putin gets away with it, as he's gotten away with so much else, that will be an invitation to him to continue doing what he's doing."

The second official said it was up to "the Department of Justice to determine what happens next." The first official said the U.S. response would generally follow the model set when President Obama publicly blamed North Korea for a hack against Sony Pictures.

In that case, the administration took what it deemed a "proportionate" response, and sanctioned North Korean individuals and conducted limited cyber attacks on North Korean networks.

But the Russian hacks aren't entirely analogous to those against Sony.

"This case is unique because there is the electoral angle," the official said, adding that the hacks represented an assault on American democracy and the political process. "When it comes to a potential response to this the president has made clear we will take action to protect our interests at a time and place of our choosing."

"Consistent with the practice we have adopted in the past, the public should not assume that whey will necessarily know what actions have been taken or what actions we will take," the official said, adding that the administration was "not taking anything off the table."

The top Democrat on the House Intelligence Committee, who had already said that intelligence led him to conclude Russia was behind the hacks, praised the administration's statement as a helpful "first step" that now had to be backed up with action."

"In terms of next steps, I would love to see the administration working with our European allies that have also been the subject of Russian hacking attempts to interfere with their institutions," Rep. Adam Schiff told The Daily Beast. "There have to be a series of graduated responses that lets Russia know this is not cost free."

"Now that we've said Russia is responsible, it increases the demands for action," Jason Healey, a former White House cybersecurity official now working at Columbia University's School for International and Public Affairs. "This should include improving election security and brush- back pitches against Putin using our own cyber capabilities, but perhaps first Obama should call a Article 4 consultation with our NATO allies. France has its own election coming up, as does Germany, which has also been brave in calling out Russian activity."

While officials suggested they only recently concluded that Russia was behind the hacks, a Sept. 22 statement by California Sen. Dianne Feinstein and Rep. Adam Schiff suggested that some members of Congress had been briefed about the U.S's conclusions weeks ago.

"Based on briefings we have received, we have concluded that the Russian intelligence agencies are making a serious and concerted effort to influence the U.S. election," the statement read. "We believe that orders for the Russian intelligence agencies to conduct such actions could come only from very senior levels of the Russian government.

The announcement of the findings immediately raised eyebrows, given this week's collapsing relations between Russia and the U.S. this week over Syria.

On Friday, Secretary of State John Kerry accused Russia of a "targeted strategy to terrorize civilians and to kill anybody and everybody who is in the way of their military objectives."

Earlier in the week, the State Department announced it had suspended ceasefire talks after Russia launched an aggressive airstrike campaign over eastern Aleppo, hitting hospitals, food and water supplies. The strikes are part of Syrian regime Bashar al Assad and Russia's attempt to siege and starve opposition out of the city. Those strikes, and the harm they have done to civilians, including children, has been widely condemned by the international community.

But for all the outrage, the Obama administration has no plans to intervene militarily in Aleppo to stop the attacks or on behalf of its rebels under Russian and regime attack. The administration has said its goal in Syria is to destroy the self-proclaimed Islamic State in Iraq and Syria. Intervening in the five-year civil war could have unintended consequences, the administration has said, namely a possible proxy war with Russia.

How this will impact the American election is anyone's guess. Trump's rivals have repeatedly targeted his ties to--and affinity for-- Russian policymakers. Trump has downplayed accusations that Vladimir Putin has had journalist and dissidents killed, responding that America, too, has done its fair share of killing. Trump has denied that Russia was responsible for downing Malaysia Airlines Flight 17 in the skies of eastern Ukraine, even though U.S. officials accused Russian- backed separatists of destroying the commercial jet, and killing all 298 passengers on board, with a Russian-imported Buk anti-aircraft missile, a claim now corroborated by a two year-long investigation. Trump has also denied that Putin invaded Ukraine, or ever would under his administration, even though its annexation of Crimea is a matter of public record and now admitted to by Putin.

Those surrounding the nominee have also had their political and financial ties to Russia scrutinized. Trump's former campaign manager Paul Manafort is seen as close to the Kremlin, and even more so to its former client in Kiev, Ukrainian President Viktor Yanukovych, who fled the country in 2014 after the Euromaidan Revolution. Ukrainian investigators have since uncovered ledgers belonging to Yanukovych's Party of Regions suggesting that cash payments were disbursed to Manafort, who consulted for the now-banned party, and that Manafort, as part of his policy advice, encouraged the former leader to whip up anti-American and pro-separatist sentiments in Crimea as early as 2006, during NATO exercises held on the peninsula. While Manafort formally resigned from the Trump campaign after these and other compromising disclosures, he is thought to still a relevant figure behind-the-scenes in advising the real estate tycoon on his White House ambitions. Moreover, another Trump advisor, Carter Page, has traveled to Moscow and been rumored to be a point-man between Putin and the Trump campaign--even if few senior figures in Russia claim to have ever even heard of him.

Wall Street Journal
U.S. Alleges Russia Hacked Emails to Sabotage Election
Saturday, 08 October 2016
Byline: Damian Paletta

Washington - The U.S. intelligence community took the extraordinary step Friday of directly accusing the Russian government of trying to interfere in the coming U.S. elections by purposefully leaking emails hacked from the Democratic National Committee and other entities.
The intelligence agencies, in a joint statement, alleged the hacks were directed by the most senior officials in the Russian government.

"We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities," the statement said.

The agencies said some state election systems have been recently scanned and probed and that this action originated from servers operated by a Russian company. But the statement stopped short of definitively blaming the Russian government for that activity.

The allegation, coming less than four months after the DNC first disclosed it was hacked, puts the U.S. and Russia on an even more adversarial path following the breakdown of negotiations over hostilities in Syria and other diplomatic spats.

U.S. officials have blamed foreign countries for cyberattacks in the past, notably attributing a hack of Sony Pictures to North Korea in 2014. But it is highly unusual, if not unprecedented, for Washington to directly accuse a powerful country of attempting to sabotage U.S. elections.

"The U.S. Intelligence Community is confident that the Russian Government directed the recent compromises of emails from U.S. persons and institutions, including from U.S. political organizations," said the joint statement from agencies including the Central Intelligence Agency and the National Security Agency.

It added that leaks by three entities -- a hacker self-described as Guccifer 2.0, the website DCleaks.com and the organization WikiLeaks -- "are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures are intended to interfere with the U.S. election process."

The Kremlin late Friday said the accusations were "nonsense," according to Interfax news agency. "Tens of thousands of hackers attack the site of [Russian President Vladimir] Putin every day. Many attacks are traced back to U.S. territory. We don't blame the White House or . . . [the CIA] every time," Kremlin spokesman Dmitry Peskov was cited as saying.

An administration official said the U.S. government could activate numerous measures in response to the alleged Russian operation, including diplomatic and economic steps as well as criminal charges.

Accusing a foreign government of attempting to interfere in the U.S. election leaves several difficult choices for the White House. Many computer experts and even U.S. lawmakers have said there should be more of a deterrent to prevent nation states from launching computer attacks.

The White House may choose to level sanctions against Russia or Russian businesses believed to be connected to the operation, or it may launch computer attacks of its own if President Barack Obama believes such retaliation is merited.

The agencies did offer a note of reassurance, saying "it would be extremely difficult for someone, including a nation-state actor, to alter actual ballot counts or election results by cyberattack or intrusion," citing the decentralized nature of the U.S. election system and protections that election officials have installed.

The intelligence community and the Federal Bureau of Investigation have spent months probing the operation and regularly briefed congressional leaders, telling them weeks ago that they believed Moscow was behind the operation. The FBI probe is continuing and could result in legal action.

Members of both parties called for consequences. Sen. Ben Sasse (R., Neb.), a member of the Homeland Security Committee, said Friday's statement should prompt strong action against Moscow.

Rep. Adam Schiff (D., Calif.), the top Democrat on the House Intelligence Committee, said that the U.S. is considering more responses but they would be carefully weighed.

"One thing that has gotten the Russians' attention is sanctions," Mr. Schiff said, referring to steps taken by Western countries in response to Russia's invasion of Ukraine.

New York Times
U.S. Says Russia Directed Hacks to Influence Elections
Saturday, 08 October 2016
Byline: David E. Sanger & Charlie Savage

Washington - The Obama administration on Friday formally accused the Russian government of stealing and disclosing emails from the Democratic National Committee and a range of other institutions and prominent individuals, immediately raising the issue of whether President Obama would seek sanctions or other retaliation.
In a statement from the director of national intelligence, James Clapper Jr., and the Department of Homeland Security, the government said the leaked emails that have appeared on a variety of websites "are intended to interfere with the U.S. election process." The emails were posted on the well-known WikiLeaks site and two newer sites, DCLeaks.com and Guccifer 2.0, identified as being associated with Russian intelligence.

"We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities," the statement said. It did not name President Vladimir V. Putin of Russia, but that appeared to be the intention.

The statement from Mr. Clapper and the Department of Homeland Security, which is primarily responsible for defending the country against sophisticated cyberattacks, said the intelligence agencies were less certain who was responsible for "scanning and probing" online election rolls in states around the country. It said that those "in most cases originated from servers operated by a Russian company," but stopped short of alleging the Russian government was responsible for those probes.

The announcement came only hours after Secretary of State John Kerry called for the Russian and Syrian governments to face a formal war-crimes investigation over attacks on civilians in Aleppo and other parts of Syria. Taken together, the developments mark a sharp escalation of Washington's many confrontations with Moscow this year.

For weeks, aides to Mr. Obama have been debating whether to openly attribute the cyberattacks to Russia, and as recently as Wednesday the director of the National Security Agency, Adm. Michael Rogers, refused to publicly accuse Moscow.

But with little more than a month to go before the presidential election, one senior administration official said that Mr. Obama was "under pressure to act now," in part because a declaration closer to Election Day would appear to be political.

Two days ahead of the second presidential debate, the announcement also puts the Republican nominee, Donald J. Trump, more on the defensive over his assertion last month that Mr. Putin is a better leader than Mr. Obama. In the first presidential debate, former Secretary of State Hillary Clinton, Mr. Trump's Democratic rival, blamed Russia for the cyberattacks on the Democratic National Committee, but Mr. Trump said there was no evidence that Russia was responsible; he suggested it could have been the Chinese or " somebody sitting on their bed that weighs 400 pounds."

Soon after the administration accused the Russians of hacking into the Democratic National Committee, WikiLeaks published hacked emails by John Podesta, the Clinton campaign chairman. In a Twitter message Friday evening, Mr. Podesta said that "I'm not happy about being hacked by the Russians in their attempt to throw the election to Donald Trump."

WikiLeaks has released troves of hacked Democratic emails, but has not revealed the source of the documents.

A major question is how Mr. Obama might respond without setting off an escalating cyberspace conflict with Russia between now and Nov. 8. One possibility is that the announcement itself -- an effort to "name and shame" -- will deter further action. But Mr. Obama's aides have assembled a range of

possible responses, from using economic sanctions to covert action against Russian targets, potentially including the computers used in the hack.

The official accusation against Russia comes after anonymous American intelligence officials told The New York Times in July that they had "high confidence" that the Russian government was behind the hack of the D.N.C., which led to the resignation of Representative Debbie Wasserman Schultz, the Florida Democrat, amid evidence that the committee was favoring Mrs. Clinton over her competitor for the party nomination, Senator Bernie Sanders of Vermont.

The months of subsequent silence frustrated some in Congress, and several weeks ago the top Democrats on the House and Senate intelligence committees, Adam Schiff and Dianne Feinstein, both of California, said Russia and its leaders were responsible, citing classified briefings.

Mr. Schiff, who had urged the Obama administration to name Russia and better prepare American voters for the possibility of interference between now and the election, on Friday praised the decision "to call out Russia on its malevolent interference in our political affairs."

"I hope this will establish a deterrent to further meddling," he said. "I don't think the Russians have decided yet how much they plan to continue their interference, so I think this attribution is very timely. We're also encouraging the administration to work with our European partners, who have been the subject of even worse meddling, to coordinate a response to this."

Mr. Schiff said he was afraid Russian hackers might attempt to delete or manipulate voter rolls, causing long lines at the polls and delays in counting votes because people would be forced to cast provisional ballots. (Voting machines themselves are not linked to the internet, so it is effectively impossible to hack them in a systematic way and change the outcome, specialists say.)

But as "profound" as that concern is, Mr. Schiff said, he and others see as "the most grave risk" something else: Russia could take emails it has already stolen, manipulate them to create a false impression that a candidate has done something outrageous or illegal, and cause them to be published online shortly before the election. That, he said, "could have an election-altering effect."

Federal officials are trying to help states plug holes in their internet defenses for election management systems. One thing they won't do before the election is pronounce such systems "critical infrastructure," as the secretary of Homeland Security, Jeh Johnson, proposed in August.

Mr. Johnson's notion provoked a backlash from conservatives. Republicans like Brian P. Kemp, the secretary of state in Georgia, and Jon A. Husted, his counterpart in Ohio, accused the Obama administration of overreach, saying it was trying to carry out a federal takeover.

Administration officials said that the idea of declaring elections systems critical infrastructure is dead for now, lest it discourage states from working with the federal government.

"Our focus right now, in the remaining days before Nov. 8, is to encourage states to come forward and request our assistance," Mr. Johnson said in a recent interview.

The department has offered states two kinds of help, both for free: a remote cyber "hygiene" scan of their servers by department officials who look for known vulnerabilities and can recommend patches, and a more intensive on-site analysis by a team of computer security specialists.

The department's emphasis on voluntary measures has met with mixed success: So far, 28 states have accepted that offer, the department said, but it declined to name them.

Officials with election agencies in the large swing states of Ohio, North Carolina, and Pennsylvania said they were participating. (Pennsylvania is particularly important because its electronic voting machines lack a paper audit trail for recounts.) Florida, another large swing state, is not participating in this particular program, but officials in the office of its secretary of state said they had already been working with federal partners before Mr. Johnson initiated the effort.

Still, while the number of participants has been slowly creeping up, the window is closing. A Homeland Security official said it takes about a week to complete the necessary paperwork to permit the department to begin the work, and that the more intensive on-site effort takes about two weeks. That suggests that soon after the middle of October, it will be too late to provide any help to late takers.

The fact that 22 states are not, as yet, participating does not necessarily mean all of them are vulnerable in ways that participants are not. Kay Stimson, a spokeswoman for the National Association of Secretaries of State, noted that some states had already been taking cybersecurity measures that are likely equivalent to what the department is offering.

Motherboard Blog
Yahoo May Have Exposed Rogers Customer Emails to US Spies
Saturday, 08 October 2016
Byline: Jordan Pearson

Toronto - On Friday, Motherboard reported that beleaguered US company Yahoo allowed someone--possibly a US intelligence agency such as the NSA or FBI--to install a backdoor on its servers, likely for scanning purposes, that afforded unfettered access to Yahoo's systems, including users' personal emails. "This backdoor was installed in a way that endangered all of Yahoo users," a source familiar with the incident told Motherboard.

This should concern Canadians, because Rogers, one of the largest telecom companies in the country, totally outsources its email systems to Yahoo. Emails sent from Rogers accounts are sent to Yahoo's US

servers for storage and processing, and Yahoo scans Rogers emails for spam, malware, and child pornography.

This isn't the first time that Rogers' ties to Yahoo have compromised Canadians: The Toronto Star previously reported that Rogers customer data was included in the massive hack in September.

Moreover, several experts consulted by Motherboard said that by dint of Rogers emails transiting and being stored on Yahoo's US servers, they would likely have been subject to any sort of system-wide email dragnet installed by US intelligence.

Neither the NSA, nor its Canadian counterpart, the Communications Security Establishment (CSE), are legally allowed to spy on the content of domestic Canadians' digital communications, with the exception that the CSE monitors emails sent to the government.

Neither Yahoo nor Rogers would comment directly on these allegations.

"I'd imagine that, yes, the program would have applied to Rogers customer emails, unless Yahoo elected to specifically exclude them"

When asked if customer emails are routed through the US, Rogers spokesperson Andrew Garas stated that "when you register for a Yahoo account, your registration information and other data will be transmitted to the United States and/or other countries for processing and storage by Yahoo." This, the spokesperson continued, includes email.

To see what kind of data Yahoo could pull from a message, I asked a Rogers-subscribing friend to send me a test email. The routing information contained in the email confirmed that the email was sent through a Yahoo-owned server in New York.

The routing information was analyzed by American Civil Liberties Union staff technologist Daniel Gillmor and Citizen Lab researcher Bill Marczak, who both agreed that a system-wide email scanning system in the US could have captured the content of the Rogers email, despite it being sent and received within Canada.

"Any program that scans all the mail that Yahoo has access to would have scanned this email," Gillmor wrote me in a message.

"If Yahoo chose to segment their scanning by limiting it only to mails that have '@yahoo.com' email addresses [and omitted those sent from @rogers.com], of course, then they would have chosen to exclude this email from the scan," Gillmor continued. "It's not clear to me whether any such constraint was in place, though."

"I'd imagine that, yes, the program would have applied to Rogers customer emails, unless Yahoo elected to specifically exclude them," wrote Marczak in an email.

Yahoo declined to comment on whether the alleged system filtered out emails from Rogers customers.

Tobi Cohen, a spokesperson for the Office of the Privacy Commissioner, confirmed that Rogers consulted the office in the wake of the Yahoo hack. But as far as the possibility that Rogers customer emails had been siphoned into a surveillance dragnet goes, "Given we don't have detailed information about the matter, we are not in a position to comment," Cohen wrote.

When asked if Rogers was aware of the allegations against Yahoo or if the company is concerned that a backdoor could have affected its customers, spokesperson Garas referred me to Yahoo's statement and wrote that "as such, we believe this matter is closed."

Rogers would not comment when asked if it had any plans to change email providers in response to the Yahoo story.

New York Times
Surveillance in the Post-Obama Era
Sunday, 09 October 2016

Editorial: During his 2008 campaign, President Obama vowed to assert greater oversight of the massive surveillance apparatus built in the wake of the Sept. 11 attacks, arguing that the United States needed to strike a better balance between privacy and security and that all intelligence programs should be lawful.
"I will provide our intelligence and law enforcement agencies with the tools they need to track and take out the terrorists without undermining our Constitution and our freedom," Mr. Obama said in 2007.

Once in office, however, the Obama White House failed to meaningfully scale back surveillance practices established by Mr. Obama's predecessor, including the unlawful bulk collection of Americans' domestic phone call records.

It was only after a National Security Agency whistle- blower, Edward Snowden, exposed how much data American intelligence agencies were collecting and hoarding that the administration began to disclose the capabilities, legal underpinnings and safeguards of government surveillance programs.

The Snowden revelations prompted important reforms. Still, the debate over the proper balance between privacy and security remains far from settled. Disappointingly, the two candidates vying to replace Mr. Obama have failed to outline clear and comprehensive visions for one of the most consequential sets of choices the next president will face.

One big issue is what to do when a key provision of the law that gives the N.S.A. the authority to collect the electronic communications of foreigners -- which inevitably sucks in their correspondence with Americans -- expires at the end of 2017. Before reauthorizing that part of the law, Section 702 of the Foreign Intelligence Surveillance Act, the next president and Congress should craft a more narrow authority that ensures that the data of Americans cannot be searched without a warrant.

How best to respond to encryption technology, which is evolving rapidly, will be another major challenge. Earlier this year, the White House supported the Justice Department's heavy- handed order to compel Apple to disable a security feature that would have allowed the government access to a locked iPhone that belonged to a mass shooter. That request, withdrawn before the legal fight was settled, would have forced the company to develop a capability that it argued would have undermined the privacy of its customers. The next president should refrain from forcing technology companies to build encryption systems that can be breached, which would make everyone's private information more vulnerable to hackers.

The next president should be more forthcoming in disclosing the legal rationale and effectiveness of the government's surveillance programs. "Just trust us," its default response to reasonable requests for more information, simply isn't enough. The latest instance involved reports earlier this week that Yahoo was compelled last year to screen all messages for a specific type of correspondence the government was interested in spotting, as part of surveillance of a state-sponsored terrorist organization. Left unsaid was whether it worked and whether other email providers have been issued similar secret orders.

The Republican nominee, Donald Trump, has not substantively addressed any of these issues. But he has proposed draconian, unconstitutional measures to keep the nation safe, including carrying out surveillance of mosques and creating a database of Muslims. This is offensive and outrageous. "We're going to have to do certain things that were frankly unthinkable a year ago," he said last November.

Hillary Clinton has been more measured in discussing surveillance and encryption. Her campaign has suggested creating a national commission to explore legal and practical questions surrounding encryption. Mrs. Clinton has also said she would like to foster a more constructive relationship with Silicon Valley leaders, who have often been reluctant to collaborate with intelligence agencies. But she has been troublingly vague on specifics.

The next president needs to take the initiative early on to outline a responsible philosophy and approach toward surveillance and privacy issues. Even if that happens, Congress still needs to be more assertive than in the past in setting clear parameters to ensure that intelligence gathering programs are legally sound and effective. It would be a shame if it took a new whistle-blower to force what should be a continuing, vigorous debate.

Follow The New York Times Opinion section on Facebook and Twitter (@NYTopinion), and sign up for the Opinion Today newsletter.

CBC.CA
Drop in police requests for electronic surveillance of suspected criminals baffles experts
Sunday, 09 October 2016
Byline: Alison Crawford

Ottawa - Experts say they're baffled by the big drop in the number of applications from police to conduct electronic surveillance on citizens.
In 2015, peace officers asked for authorization to intercept and record private communications 66 times, down from 114 a year earlier.

Police can ask a judge for permission to intercept someone's personal communications when they suspect serious criminal activity. Such authorizations generally last around 60 days.

The data comes from the Department of Public Safety's annual report on the use of electronic surveillance in Canada.

The report describes how, when applying for authorization, police most often said they suspected drug trafficking, terrorism, conspiracy and possession of stolen property. It also says charges were laid against 56 people identified during an interception.

Brenda McPhail welcomes the information, but the director of privacy, technology and surveillance for the Canadian Civil Liberties Association, can't explain the drop. McPhail says there's a limit to how helpful numbers are without any analysis.

"We could wonder whether or not the categories they are required to report in are so narrow that they are not catching the new kinds of interception technologies and techniques that are being used," she said.

Christopher Parson agrees. He's with the telecom transparency project at the Munk School of Global Affairs' Citizen Lab.

"Wiretaps are meant to be a tool of last resort so what that may suggest is authorities are finding other ways of gaining evidence that is less intrusive on Canadians' privacy, more generally," Parsons told CBC News.

Parliamentary security committee coming

That has the potential to be a good thing, according to Parsons.

"Unfortunately we don't have data on any of the other tools law enforcement uses. One of the anomalies in the Canadian situation, actually, is outside of these reports, we really have no clear indication of how often police are using their powers," said Parsons.

The government is currently holding consultations on Canada's national security framework. A spokesman for the Department of Public Safety says the public should share their views about police and security agency investigative capabilities in a digital world.

"More broadly, the government is advancing legislation to establish a committee of parliamentarians with special access to classified information to increase the accountability of all security agencies and departments," added spokesman Scott Bardsley.

USA Today
Could the U.S. election be hacked? ; At national level, no, but experts say it wouldn't take much to sow discord
Tuesday, 11 October 2016
Byline: Elizabeth Weise

Washington - The impact of Russian hacking on the upcoming presidential election was a topic in Sunday night's debate, raising the question: Is the U.S. election hackable? Experts say at the national level, no. But there could be individual incidents that undermine faith in the system.
There's almost no danger the U.S. presidential election could be affected by hackers. It's simply too decentralized and for the most part too offline to be threatened, according to the head of the FBI and several security experts.

"National elections are conducted at the local level by local officials on equipment that they obtained locally," so there's no single point of vulnerability to tampering here, said Pamela Smith, president of Verified Voting, a non-partisan, non-profit organization that advocates for elections accuracy.

In testimony before the House Judiciary Committee last month, FBI Director James Comey said that while concern has been rightly focused on the integrity of state voter registration systems, the actual voting process remains "very hard to hack into because it is so clunky and dispersed. It is Mary and Fred putting a machine under the basketball hoop at the gym. These things are not connected to the Internet."

Nevertheless, Comey said federal authorities have been counseling state officials to secure their systems, especially voter registration databases, as hackers have continued to "scan" the systems for vulnerabilities.

In Sunday's debate, Democratic presidential candidate Hillary Clinton noted U.S. intelligence officials have blamed Russia for hacking Democratic officials accounts.

"We have never in the history of our country been in a situation where an adversary, a foreign power, is working so hard to influence the outcome of the election," she said, and alluded to her Republican opponent Donald Trump's praise of Russian president Vladimir Putin.

Trump replied that he knew "nothing about the inner workings of Russia" and didn't address electoral issues. However, on the campaign trail he has said multiple times he fears the election will be stolen. In August in Columbus, Ohio, he said, "I'm afraid the election's going to be rigged. I have to be honest."

In some jurisdictions, local rules allow the transfer of election results using Wi-Fi rather than putting the information on a thumb drive that's physically taken to the central tally site. Others simply use outdated machines.

Depending on the voting machine, all it might take would be one disgruntled election official plugging in a thumb drive containing malware to falsify vote tallies, said Mike Baker, founder of Mosaic451, a computer security company that focuses on infrastructure protection, including for some state and federal election networks.

So far, 33 states and 11 county or local election agencies have approached the Department of Homeland Security for cybersecurity risk and vulnerability assessments, Secretary Jeh Johnson said in a statement Monday.

But time is a factor, and he encouraged election agencies to ask for help now.

"There are only 29 days until Election Day, and it can take up to two weeks from the time we receive authorization to run the scans and identify vulnerabilities. It can then take at least an additional week for state and local election officials to mitigate any vulnerabilities on systems that we may find," he said.

The good news is that in the upcoming election, close to 80% of voters nationwide are in areas that will use either paper ballots or voting machines with paper backups, both of which are considered much more secure than online-only systems, Smith said.

While election officials worry about such possibilities, they're loath to discuss them publicly. Voters losing confidence in the system and not turning out to vote is a greater threat to the integrity of the election system than hackers, they believe.

"It's a tough position for us to be in. We don't want to scare voters away," said Kim Alexander of the California Voter foundation, a non- profit, non-partisan organization that promoted the responsible use of technology in elections.

The fear is that proof of even one example of vote manipulation could be amplified through social media to threaten the electorate's trust in the entire system.

That trust is a bedrock of American democracy and if it's lost, "that puts us in a whole different category of countries that don't have free and fair elections," said Melinda Jackson, chair of the political science department at San Jose State University.

Fars News Agency
Why an Unhackable Mobile Phone Is a 'Complete Marketing Myth'
Tuesday, 11 October 2016

Tehran - The mobile security market is taking flight due to high- profile hackings, but is there such a thing as an unhackable phone? Especially one that costs as much as $14,000?
Consider this: The smartphone in your pocket is 10 times more powerful than the fastest multi- million dollar supercomputers of just 20 years ago. There are tens of millions of lines of software in that phone of yours. There are hundreds of apps written by more than one million developers, some of whom are hackers, and some of whom are just incompetent at security. And then there are chips in your phone that run sophisticated software, from companies located in countries all around the world, all of which have security bugs.

The complexity is mind-boggling -- and so are all the security vulnerabilities that exist and will be found in the future. In short, anyone who claims to sell an "unhackable phone" is either ignorant or lying.

With cybercriminals increasingly targeting mobile devices (such as with malicious apps and phishing schemes), threatening both the consumer and enterprises, the market is rushing to provide solutions to mobile security threats. Gartner calls this Mobile Threat Defense.

Everyone -- no matter which phone they own -- needs to be vigilant before downloading apps. For example, hackers recently created versions of Pokémon Go that contained malicious spyware that was released to eager fans before its official release. Even the first version of the legitimate Pokémon Go app was spying on many of your activities, and the developer and app stores didn't catch it.

Despite the marketing hype, it is impossible to detect all malicious app behavior through a one-time scan of an app before it's published on an app store. Bad apps often exploit operating system vulnerabilities that have not been discovered or fixed by the mobile device vendor. Apps can have "sleeper cell" behavior, where they don't exhibit malicious behavior when being analyzed for app store approval -- they wait until being deployed in the real world. Cybercriminals can also easily sideload apps onto both Android and iOS platforms from illegitimate app stores.

In addition to bad apps, we are seeing an increase in the number of criminals, hackers and hostile governments willing to pay for zero-day mobile exploits. These silent and secretive threats can take over your mobile phone simply by sending you a text message or email with a link to a malicious website. Unfortunately, new security threats and hacks are typically found after successful attacks have been

reported by victims, researched and a fix is created by programmers. A hack may affect thousands or even hundreds of thousands of people before it is detected and fixed.

It's also important to consider that most phones claiming to be "secure" or "unhackable" come from companies that base their phone on the Android operating system. Android is a state-of-the-art mobile device operating system, but more than 100 new security bugs are regularly discovered and need to be fixed every year. This trend shows no signs of slowing, and as mobile devices get ever smarter with more software and capabilities, there will be more bugs that hackers can exploit.

Taking a deeper look into the security of mobile devices shows that in August 2016 alone, there were 42 security vulnerabilities detected in the Android operating system or the Nexus device hardware. In July 2016, 54 such vulnerabilities were found. This monthly trend has been consistent for years. There is no sign that it will stop. You can be assured that every mobile device has 10-50 security vulnerabilities that will be discovered in the next month. And the month after that. And so on.

Of interest is that about half of the discovered vulnerabilities were not in the phone's operating system itself, but instead were found in the operating systems and software that run the chips inside the device. These tiny bits of software, called firmware, contain dozens of security bugs, which are discovered every month. These firmware security vulnerabilities impact the software that operates cell phone modems, cameras, Wi-Fi, sound, displays, USB, Bluetooth, power drivers and more on each device. These components are from a variety of manufacturers around the world. It is simply impossible to ensure that these myriad components are secure.

Furthermore, it is critical to point out that 65 percent of Android devices in use around the world still run old versions of the operating system, with hundreds of known bugs.

The iOS operating system is also not immune to security bugs. Security fixes have been, and will be, continuously applied to the iOS operating system for Apple iPhones and iPads once they are reported. For example, in July 2016 alone, fixes for 29 types of security vulnerabilities were released by Apple. These fixes addressed 46 separate issues.

In August 2016, only one month later, news broke that hackers and governments were infiltrating iPhones with advanced spyware to steal data and spy on all app communications, even encrypted apps. Attackers simply sent users a text message with a malicious link. The attacks appear to be created by a commercial company in Israel, called NOS, that makes spyware for mobile devices.

And what about those Wi-Fi networks we rely on when in airports and at hotels? Make no mistake, they often spy on our communications. The so-called "captive portal," where you have to enter your hotel room number, or just click on a terms of service agreement, are often traps to capture your email, passwords and web browsing activities. Be vigilant about which networks you connect to while traveling. If you receive a warning when connecting to a new Wi-Fi network, do not click "Continue." Try another network.

All of these issues make it impossible for a single device to be completely secure. Organizations need mobile threat defense security tools that will protect the enterprise as employees connect their devices to malicious networks and download questionable data-stealing apps around the world. Consumers need to be vigilant before downloading apps (read and confirm permissions are in place), be wary of text messages from unknown sources and only join known and trusted Wi-Fi networks. And hang up on the hype of an "unhackable phone."

The National (UAE)
Smart city Dubai must beat hackers in security race
Tuesday, 11 October 2016
Byline: Caline Malek

Dubai - Smart cities such as Dubai will have to continuously upgrade their technology to evade hackers, according to the first US secretary of homeland security.
Tom Ridge, former governor of Pennsylvania, told a cyber security conference that the internet will be linked to the success of smart cities.

"We live in an extraordinary age and one of great and accelerated change," he said. "In two decades, the internet has transformed humanity. It now drives the way we communicate, educate, how we receive information and we are hyper-connected. It has revolutionised the manner in which we educate our children, conduct our business and manage government affairs."

In 2012, it was estimated there would be 12 billion internet connected devices by 2020. In 2013, that figure was increased to 75 billion, a number Mr Ridge described as "staggering".

As a global hub, the UAE is a prime target for cyber attacks. "Any enterprise that is as successful, vibrant and connected like Dubai [is a target]," Mr Ridge said. "It's a centre for financial transactions and trade historically. That's what makes the Government's decision to make it a smart city timely and relevant and increases the pressure on [it] to do it right because it becomes an iconic player in the region and the world. The higher the profile, the more sophisticated the attacks." He said leaders had to accept the "risk reward" arrangement which involves understanding the perils that come with transforming a city into a smart city.

"Dealing with issues of cyber security calls for constant improvement because it's such a dynamic environment," said Mr Ridge. "Assessments have to be regular because the threat and the sophistication of the attack changes all the time so as advanced as the cyber-security protocols may be in the UAE, the real challenge is not to accept it today because you could be secure today and insecure tomorrow."

Telecoms firm du is a target of between 70 to 100 cyber-attacks each day. None have succeeded as of yet. "The number of cyber security incidents in 2009 was a bit over five million," said Osman Sultan, du's

chief executive. "In 2015, it counted over 60 million. This is a growth of more than 1,000 per cent in six years. We are in the midst of an incredible transformation, one that became so rapidly disruptive and global, more than any transformation in the history of mankind and that is changing everything we do in our lives. "The digital and online transformation is the determining factor of the age we live in."

He said cyber security should not be an afterthought for an organisation's IT department. "It should be at the heart of the thought itself," he said. "There are rewards in this hyper- connected world we live in. Risks are there because of this connectivity and we have to hope that one day, the risks will not become greater than the rewards. But that is an act of faith that all of us are making that we can harness the incredible rewards that come from a smarter and more connected world."

Experts said employees were considered the weakest link in the cyber security chain. "One of the biggest risks in cyber security is the employee and we keep seeing this," said Ibrahim Al Mallouhi, du's vice president of security operations. "We are doing awareness programmes now for our internal staff about cyber security threats and models because it evolves so fast."

Mr Ridge said resilience in governments was key. "We must be ready to quickly identify, contain and resolve a breach to limit disruption and recover quickly. A cyber-attack can bring everything to a screeching halt. Cities that are resilient will change what it means to be truly a smart city and those that adapt to change not only survive, but flourish."

London Times
Police use snooping devices on phones
Tuesday, 11 October 2016
Byline: Fiona Hamilton

London - A string of police forces have secretly purchased surveillance technology that enables large amounts of phone data to be collected from passers-by, it has emerged.
At least seven forces in England and Wales are now thought to be using IMSI Catchers that can collect and identify call and message data from mobile phones within a given area. They mimic mobile-phone towers and act as a "dummy", sending out signals that trick devices into automatically trying to connect to them.

Police find the Catchers useful to track suspects and uncover their phone activity, but they can capture information from other mobiles within a radius of up to five miles. It is believed that there is no automatic deletion of the gathered material from police systems, meaning that forces could be harvesting information about tens of thousands of members of the public.

The Times reported in 2014 that the Metropolitan police had purchased the technology. It emerged yesterday that at least six more forces are thought to be using IMSI Catchers.

Research by the Bristol Cable website, a media co-operative, showed that forces in the West Midlands, West Mercia, Warwickshire, Staffordshire, Avon and Somerset, and South Yorkshire are likely to have purchased IMSI.

Forces refuse to confirm such purchases, citing security concerns. However, official procurement documents referred to CCDC, or covert communications data capture, and there are police contracts with Cellxion, which manufactures IMSI.

Scotland Yard paid more than £1 million to Cellxion for "CCDC" last year and Avon and Somerset police paid the company £169,575 for "CCDC equipment", as well as other "communications and computing equipment", according to purchase data examined by the Cable. Unredacted minutes from a meeting in May between West Mercia and Warwickshire police said: "West Midlands and Staffordshire police have recently purchased and operated 4G-compatible CCDC equipment."

Warwickshire and West Mercia went on to purchase new CCDC technology. South Yorkshire budget papers showed that the force spent £144,000 in 2015-16 on "IMSI Covert Communications", which it confirmed was CCDC.

The use of the devices can be authorised by a chief constable without having to seek permission from a judge or minister. Privacy International has previously pointed out that the lack of transparency from British police is in contrast with overseas forces, which disclose their use of the technology.

London Daily Telegraph
Apple Watches banned from Cabinet after ministers warned devices could be vulnerable to hacking
Sunday, 09 October 2016
Byline: Peter Dominiczak

London - Ministers have been barred from wearing Apple Watches during Cabinet meetings amid concerns that they could be hacked by Russian spies, The Telegraph has learned.
Under David Cameron, several cabinet ministers wore the smart watches, including Michael Gove, the former Justice Secretary.

However, under Theresa May ministers have been barred from wearing them amid concerns that they could be used by hackers as listening devices.

Mobile phones have already been barred from the Cabinet because of similar concerns.

One source said: "The Russians are trying to hack everything."

Mr Gove disrupted one Cabinet meeting when he was Chief Whip by inadvertently playing a Beyonce song.

Sarah Vine, his wife, disclosed that he was "surreptitiously checking his emails", but pressed the wrong button when a message came through.

Ms Vine said: "So the cabinet was treated to the first few bars of a song from Beyonce."

It comes amid mounting fears about the scale of Russian hacking in the West.

Concerns have been raised after hackers obtained confidential emails from the Democratic National Congress during the US election.

Russian hackers have also obtained the medical files of some of the world's most famous athletes.

Xinhua News Agency
S'pore set to deepen cyber capacities across ASEAN member states
Tuesday, 11 October 2016

Singapore - Singapore's Minister for Communications and Information Yaacob Ibrahim on Tuesday announced that the country is pleased to launch a 10-million-Singapore dollar (7.25 million U.S. dollars) ASEAN Cyber Capacity Program (ACCP) to help fund various efforts to deepen cyber capacities across ASEAN member states.
Minister Yaacob Ibrahim made the announcement in his opening remarks at the inaugural ASEAN Ministerial Conference on Cybersecurity, which was held during the Singapore International Cyber Week 2016.

Yaacob, the minister-in-charge of cybersecurity, said the money will pay for resources, expertise and training, so that ASEAN countries will be equipped to drive and take ownership of their respective cybersecurity agenda.

The minister said the program, which will be launched in April 2017, will provide the resource to broaden the scope of capacity building activities and better hone technical skills and incident response.

"It will also support discussion and consultancy work in areas such as the formation of national cybersecurity agencies, formulating cybersecurity strategies, and even legislation," added Yaacob.

Motherboard (Vice Magazine)
FBI Hacked Computers in Australia as Part of Global Child Porn Sting
Monday, 10 October 2016
Byline: Joseph Cox

New York - In early 2015, the FBI hacked thousands of computers across the world, based on a single, arguably illegal, warrant.
Now, Motherboard has learned that as part of the same operation, the FBI also hacked computers in Australia, highlighting how law enforcement agencies are increasingly using malware to remotely search computers outside of their jurisdiction.

The case, codenamed Operation Pacifier, revolves around the FBI's investigation into one of the largest ever dark web child pornography sites, called Playpen. When the FBI seized the site in 2015, instead of shutting it down, the agency briefly ran Playpen from a government server in order to deploy a network investigative technique (NIT)--the agency's term for a piece of malware--in an attempt to identify its visitors.

The agency's malware used a Tor Browser exploit, and then grabbed a suspected Playpen user's IP address, MAC address, and other technical information. As well as obtaining over 1,000 US IP addresses, and distributing much of this information throughout the FBI and to other US-based law enforcement agencies, the FBI also gave details on suspects overseas to foreign agencies.

The Australian Federal Police (AFP) was one of those agencies. During the processing of a Freedom of Information request filed by Motherboard, the AFP said it held a wealth of data on Operation Pacifier, including a large PROMIS case file. PROMIS is the case management tool AFP officers use to catalogue investigations and store intelligence.

During preliminary searches, the AFP found 600MB of file data and "One PROMIS case alone containing over 2000 case note entries," a letter from the AFP to Motherboard reads. The agency confirmed that this file relates to the international referrals the AFP received in relation to Operation Pacifier. A single PROMIS case note entry does not necessarily equate to an IP address provided by the FBI; PROMIS is frequently updated throughout AFP investigations.

Australia is just the latest country to be revealed as part of Operation Pacifier. A Europol presentation uncovered by Motherboard said that the law enforcement agency had generated over 3,200 related cases, including 39 cases in Denmark. A second presentation showed that police in Colombia had worked on Operation Pacifier as well.

Earlier this year, an Austrian politician wrote in a letter to MPs that 50 IPs from the country had been obtained during the operation. The FBI also hacked computers in Greece and Chile, and there are indications of more related arrests in Turkey and the UK.

During a recent court hearing, Daniel Alfin, an FBI Special Agent who is working on the Playpen investigation, said that some of the suspected Playpen users based overseas have not yet been arrested or apprehended, "because of the amount of time it takes to get work done in some foreign countries."

But, in what shows the increasing use of malware to target suspects overseas, Australian authorities hacked into computers based in the US. Through US court documents, Motherboard found that a small unit of a regional police force led a separate operation to hack suspected visitors of another dark web child pornography site, including over 30 alleged US-based users.

The AFP previously told Motherboard it was not aware of the operation.

The Intercept
Report Finds Loose Laws on Data and Surveillance In Latin America
Monday, 10 October 2016
Byline: Cora Currier

Washington - The laws in many Latin American countries haven't kept pace with the increasing power of surveillance technology, creating the potential for serious abuses, according to a new report from a privacy watchdog.
Despite recent revelations of widespread use of spyware capable of infiltrating phones and computers by many governments in the region-- including in some instances, against political opposition and journalists-- not a single Latin American country surveyed in the report has specific laws on the use of such invasive technology. Many countries, including Brazil, Colombia, Chile and Mexico, require companies to log detailed data on their customers and give law enforcement access to the information on demand. Colombia has a ban on encryption, and El Salvador requires communications providers to decrypt traffic at the government's demand.

The report, written by researchers for the San Francisco-based Electronic Frontier Foundation, looked at surveillance laws in 12 countries in Central and South America. It opens with a stark reminder of what is at stake: A history of the collaboration among military dictatorships in Argentina, Chile, Paraguay, Bolivia, Uruguay and Brazil in the 1970s and 80s known as "Operation Condor." Files discovered later documented torture, disappearances, imprisonment and executions, enabled through a regime of informants and surveillance.

Many intelligence agencies in the region were formed under these military dictatorships, and even after transitioning to democratic rule, most Latin American countries maintained strong executive branch powers "without well-placed controls or public oversight mechanisms." Given the power vested in many presidents in the region, the report says, "intelligence agencies in Latin America have been powerful tools in presidential politics, specially used to spy on dissident groups, opposition politicians or independent journalists."

Colombia's national security agency under former president Álvaro Uribe was found to have illegally wiretapped calls and hacked the emails of his political opponents. The revelation of the scandal in 2011 led to the dissolution of the agency and various reforms - though the authors of the EFF report still think the country's broad intelligence law leaves room for abuse.

"We're especially concerned with laws requiring data retention on the whole population for future use by law enforcement," said Katitza Rodriguez, one of the authors of the report. "Colombia has a retention period of 5 years, and there are no clear rules of who can access the data and how it will be deleted after the fact."

While Mexico's Supreme Court recently put some safeguards on the country's data retention law, limiting who could access the information, Paraguay was the only country EFF found that had rejected data retention policies entirely.

In the United States, the FBI has clashed with companies over what sort of information they are required to turn over and what they are legally required to do, most famously trying to force Apple to break into the iPhone of the San Bernardino shooter. Latin American governments have also pushed providers to do their bidding with aggressive interpretations of what the law requires.

Earlier this year, a state judge in Brazil shut down the messaging service Whatsapp for 72 hours, after demanding that the company turn over the content of messages for a criminal investigation. Whatsapp stated that it could not turn over what it didn't have, since the app, with end-to-end encryption, doesn't have a record of what users send. (The judge's order was overturned by another court.)

EFF found that Colombia has a law on the books that actually bans the use of encryption.

"If it were actually enforced, many things would be illegal," Rodriguez said. "They aren't enforcing it now, but as the use of encryption becomes more widespread that old law is becoming more relevant."

The report is also concerned with the increased surveillance firepower readily available to governments. When company records for the Italian spyware manufacturer Hacking Team were hacked and released online last year, it came out that Brazil, Colombia, Chile, Ecuador, Honduras, Mexico, and Panama had bought surveillance software from the company, and many other nearby countries had been in talks with them.

Mexico was Hacking Team's top client, and not just federal agencies bought the spyware but also many state governments and the national oil company PEMEX, which do not have the authority to conduct surveillance. Mexican journalists uncovered that the governor of the state of Puebla had used the malware to spy on political opponents.

Cases like Puebla get at the heart of one of the report's main takeaways: While it found some positive trends in terms of legal protections and transparency reports, the issue is how the law is interpreted and enforced.

"Without public oversight- not just judicial oversight -- the laws on the books just won't work," said Rodriguez.

Vice Magazine
Spy fraud
Sunday, 09 October 2016
Byline: Jason Leopold

New York - When contractors and employees who work for America's most powerful intelligence agencies get bored at work, they sometimes kill time by viewing pornography on their classified government computers, browsing online dating services, engaging in "sex chats" with minors, and playing games on Facebook.
And they charge U.S. taxpayers millions of dollars for it.

Between 2013 and 2015, the Intelligence Community's Inspector General, the watchdog entity overseeing 16 federal intelligence agencies, investigated dozens of instances of employee misconduct and crimes based on referrals it received from intelligence agencies. Many of them centered on widespread contracting fraud involving individuals who worked on highly classified intelligence programs for the NSA, the CIA, and the Office of Director of National Intelligence (ODNI) on behalf of well-known contractors such as IBM, Booz Allen Hamilton, Boeing, and General Dynamics.

That's according to hundreds of pages of top-secret internal watchdog reports that were declassified and released to VICE News in response to a Freedom of Information Act lawsuit.

Because much of the inspector general's work is shrouded in secrecy, very few of its investigative reports are ever publicly released. This is the first broad- based, behind-the-scenes look at how the office, headed by Charles McCullough, has handled misconduct. McCullough is the watchdog who reviewed Hillary Clinton's State Department emails and referred the case to the FBI after finding that a few dozen messages stored on her private email server contained highly classified information.

Presumably, lawmakers on the House and Senate intelligence committees, which conduct oversight of the intelligence community, have seen the inspector general's reports. But several key lawmakers, including the ranking Democrat on the Senate Intelligence Committee, Dianne Feinstein, declined to comment on the substance of the investigations or how such misconduct negatively impacts intelligence work.

Experts said this type of misconduct is problematic on multiple levels and can pose a threat to national security. Scott Amey, the general counsel of good government group the Project on Government Oversight, which tracks waste and fraud by government contractors, reviewed the reports for VICE News.

"The contractors are primarily to blame, but these records show that intel agencies don't have a handle on the situation, and no one seems to enforce contract requirements," Amey said. He likened the waste

uncovered in the reports to an infamous instance of defense contractor excess uncovered during the Reagan administration. "We have stated that time-card fraud is the next $436 hammer, and these records prove that."

"The mischarging is in the millions, which shows the lack of contract administration and oversight by everyone involved," Amey added.

In one case, a contractor for the massive Science Applications International Corporation admitted that "95% of his time spent on the Internet was for personal use" at the ODNI, and that he spent nearly all day emailing and instant-messaging his friends. He also worked for the National Counterintelligence Center, which is responsible for collecting, monitoring, and analyzing information on potential terrorist threats.

Over the course of six years, the person billed the government $974,470 for 10,573 hours of work, even though much of it, he said during an administrative hearing, was spent accessing "online dating and social accounts to view images of scantily clad or naked women." After a two-year investigation, the person was found to have violated internal intelligence community policies, which included the misuse of government equipment. His access to classified information was revoked and he was fired.

Several contractors for Science Applications came under investigation for fraud and misconduct. For nearly a year, the inspector general investigated one who was assigned to ODNI for engaging in "graphic sexual chat" on a near daily basis from 2010 through 2013 using the agency's internal network. The contractor "often engaged in as many as 20 exchanges per day seeking sex partners. The majority of [his] sex chat included attempts to establish after work sexual encounters, descriptions of desired sex acts and graphic descriptions of his genitalia," according to the report.

After the inspector general learned that the contractor may have also used the agency's network to "establish a sexual relationship with a possible minor residing in northern Virginia," the watchdog referred the case to the FBI and a local task force on internet crimes against children. As the FBI began to probe the matter, ODNI officials detected that the contractor attempted to establish a sex chat with another possible minor in Colorado.

The contractor's access to government computer systems was suspended and he was swiftly escorted out of ODNI facilities. The FBI and law enforcement in Virginia took over the investigation, but neither would comment on whether the case was ever prosecuted.

In another case, a contractor working for the National Reconnaissance Office, which oversees spy satellites, allegedly abused his infant son between 2008 and 2009. The allegations surfaced in the contractor's 2009 polygraph examination. But the spy satellite agency's internal protocols apparently prohibited employees from reporting the incident to local law enforcement. The inspector general spent four years probing the case and recommended "a thorough review of the responsibility for reporting Federal and state crimes amongst the relevant NRO offices."

In another report, the inspector general said it opened up an investigation into a General Dynamics subcontractor -- he worked for technology company ManTech -- and found that while assigned to work for ODNI from 2005 to 2012, he didn't work. At all.

During a hearing, the contractor told the inspector general that he "took advantage of the lack of supervision and lack of work on the contract. He said that since 2005 he recorded [thousands of] hours which he did not work." This cost taxpayers $410,300.

The nature of the contracts and the type of the intelligence work performed is classified and was redacted from all but one of the reports VICE News obtained. (In that case, a program manager was found to have done nothing wrong when he played a role in selecting Honeywell as a contractor after his wife inherited about $45,000 in Honeywell stock.) But intelligence sources said the watchdog's investigations could involve contractors who work on any number of programs that involve analyzing NSA signals intelligence, CIA covert operations, and sensitive military programs and operations.

The outsourcing of intelligence work exploded after 9/11, and now five major corporations control most of it. Budget cutbacks were partly responsible for the explosion, and experienced people who worked for the government were lured to the private sector by higher pay. But outsourcing is risky because government agencies don't have an adequate workforce to oversee the contractors, meaning there's plenty of opportunity for waste, fraud, and abuse.

"It's a lot easier to track people and their work when fewer government and contractor program and personnel layers exist," said Amey, the good government group lawyer. "The move to outsource work seems to come with an acceptance of risk and tolerance for waste and fraud."

And, perhaps, negligence. The reports show that contractors and employees with access to top-secret information used public Wi-Fi to perform their work, at times on their personal computers, and in so doing risked exposing classified intelligence information.

Of all the investigations the watchdog launched over the past three years, only one involved a media leak. In 2012, McClatchy reporter Marisa Taylor obtained a letter sent to Congress by the inspector general of the National Reconnaissance Office. The letter regarded claims that an official there retaliated against four whistleblowers who raised red flags about contracting crimes.

Ultimately, the Intelligence Community Inspector General was unable to determine who was responsible for leaking the letter to Taylor (it appeared to have been a member of Congress). But as the subsequent report said, the letter did not contain "restricted handling guidance and was unclassified, [and] the release of the letter was not a criminal act as typically required in official leak investigations."

Steven Aftergood, the executive director of the Project on Government Secrecy at the Federation of American Scientists, told VICE News the kind of widespread abuse by government contractors revealed by the reports "defrauds the taxpayer."

"More subtly, it spreads corruption among the workforce and reduces expectations of competence and high performance," Aftergood said. "Contractors have always played an important role in intelligence, but in recent years they have assumed greater prominence in intelligence collection, analysis, and production. So messing around on the job could occasionally have serious consequences."

The bright side, Aftergood said, is that the watchdog is "actively investigating" the misconduct and aggressively trying to weed it out.

Newsweek
In Russian Hacks of Democrats, a Ghost of the Soviet Past
Monday, 10 October 2016
Byline: Jeff Stein

Column - Felix Dzerzhinsky must be chortling in his Red Square tomb. Nearly a century ago the first head of the Soviet secret police perfected the art of "disinformation," the clever crafting of false information to sow confusion among the Kremlin's enemies. His heirs have brazenly remounted the technique in an all-out attack on the American political system. It's not been subtle.
'We stand for organized terror," Dzerzhinsky famously wrote. "This should be frankly admitted. Terror is an absolute necessity during times of revolution." When the Soviet Union collapsed in 1991, Muscovites fed up with decades of repression tore down Dzerzhinsky's monstrous statue in Lubyanka Square, site of the KGB's infamous interrogation tombs, but he's making a comeback in the hearts of the Kremlin. In 2005, a smaller bust of the secret police chief, who died in 1927, was restored in the courtyard of the Moscow police headquarters. Last year, city election officials greenlighted a referendum to restore "Iron Felix," as the 40-foot high hulk was known.

Vladimir Putin seems to be a fan-and not shy about it. The Kremlin left its fingerprint on the hack of the Democratic Party's data vaults, investigators say. The person or team of hackers known as Guccifer 2.0 left behind a signature in Cyrillic, "Felix Dzerzhinsky."

"If these are indeed the Russians," Nina Khruscheva, the great-granddaughter of Soviet Premier Nikita Khrushchev tells Newsweek, "it only suggests that they either want to be caught and laugh at those who think they caught them."

It's possible someone else posing as a Russian wants Putin to be blamed for the hack attacks, says Khruscheva-always a possibility in the murky Internet underworld. But that's not likely, according to the Obama administration, which last week pointed a finger directly at the Kremlin.

"We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities," said the statement from the director of national intelligence, James R. Clapper Jr., and the Department of Homeland Security.

One of their targets, John Podesta, Hillary Clinton's campaign chairman, had no doubt where the latest attacks on the Democrats originated. "I'm not happy about being hacked by the Russians in their quest to throw the election to Donald Trump," an obviously enraged Podesta tweeted. But, "[I] don't have time to figure out which docs are real and which are faked."

And that's exactly the point of disinformation--a term invented by the Soviets.

"The purpose of developing black propaganda is not to throw a whole slew of fake documents into the stream, but to insert or delete words or phrases into the record which are damaging but [can only] later be disapproved," says Malcolm Nance, a career U.S. intelligence officer and author of The Plot to Hack America, published just days ago. The genius of the technique is that the correction takes days, or weeks, to catch up to the fiction. By then, gullible masses have digested the fabrications as truth.

The best disinformation closely hews to widespread suspicions about its target. Wikileaks's exposure of Hillary Clinton's private speeches to Wall Street bankers, apparently in concert with Russian hackers, seems tailored to further alienate the party's left wing, which is to say on-the-fence followers of Bernie Sanders.

But some of the purported excerpts from her speeches are obvious fabrications, says Nance.

One quote has her saying, "Muslim Immigration and Multicultural Madness have left a trail of misery and mayhem across Germany-with far worse to come because of demographics." She supposedly goes on to say that "Muslims make up only 9% of Berlin's population but account for 70% of young repeat criminals..."

Her purported phrasing about immigration "is on its face ridiculous," Nance says, since it would seem to align her with the xenophobic rants of Trump and his fellow travelers. And "never in a million years," he maintains, "would the top diplomat of the United States use any phraseology or Nazi-like statistics like this."

The same goes for Clinton's supposed embrace of "open borders" in the Western Hemisphere, he says. That almost certainly fabricated quote tracks with paranoia generated by the Trump campaign.

"We don't know what evidence the U.S. government has" that the Kremlin is quarterbacking such attacks on the Clinton campaign, notes Henry Farrell, a George Washington University associate professor of political science and international affairs who has written on the politics of the Internet. But as the Obama administration pointedly said last week, "Such activity is not new to Moscow -- the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence

public opinion there," Farrell wrote in the Washington Post. Such a statement, Farrell said, "can possibly be read as tiptoeing one step toward agreement with the Northern Europeans" that Russia is waging a not-so-covert war on them, putting Washington one step closer to a cyber war itself.

Washington needs to stay cool, counsels Khruscheva, a professor at the New School who graduated from Moscow State University in 1987, during the death rattles of the Soviet Union. (She earned a PhD in Comparative Literature from Princeton University in 1998.) "Putin was a covert KGB operative, so shadow games must be his thing," she said by email, "but endowing the Russians with the power to bring down American democracy is silly." We will withstand his provocations, but in the meantime, "he is laughing at all of it," she says, the exposure of "lying cunning politicians and vulgar business showmen."

The problem, of course, is that the cunning Putin may overstep, poking a wobbly, unsure Uncle Sam one too many times, setting in motion a new Cold War that won't be so easily controlled.

Journal de Québec
Anonymat imposé pour une réunion sur la radicalisation
Tuesday, 11 October 2016
Byline: Taïeb Moalla

Québec - Québec refuse de dévoiler les noms des participants
Invoquant des enjeux de sécurité, le gouvernement du Québec refuse de dévoiler les noms des participants à une conférence de L'UNESCO sur la radicalisation des jeunes. Cet événement se déroulera au Centre des congrès de Québec du 30 octobre au 1er novembre.

«À l'heure actuelle, compte tenu de la sensibilité des sujets abordés dans le cadre de la conférence et pour des questions de sécurité, nous ne pouvons pas dévoiler la liste des participants», a répondu Pascal Ouellet, responsable des relations avec les médias au sein du ministère des Relations internationales et de la Francophonie (MRIF).

UNESCO

Le «programme provisoire» de la conférence est bel et bien en ligne sur le site internet du MRIF. Divers ateliers et séances sont prévus. Il s'agit notamment «d'internet et radicalismes violents», de «témoignages de jeunes et de familles directement touchés par la radicalisation violente» ou encore de «la lutte et de la prévention contre la radicalisation».

Par contre, aucun nom d'expert ou d'intervenant ne figure sur le programme. «L'identité des conférenciers sera dévoilée dans les jours précédant l'événement», a ajouté M. Ouellet.

250 À 300 EXPERTS

En mai dernier, L'UNESCO et Québec ont fait savoir que 250 à 300 experts dialogueront sous le thème: «Internet et la radicalisation des jeunes: prévenir, agir et vivre ensemble». Le coût d'organisation de la rencontre est d'environ 800 000 $, dont 500 000 $ assumés par le gouvernement du Québec.

Interrogé il y a quelques mois sur le profil des participants, Indrajit Banerjee, directeur de division à L'UNESCO, a répondu que «ce sera un mélange. Il y aura des représentants des gouvernements, mais aussi des gens qui ont une expérience concrète en matière de radicalisation et de cybersécurité».

Au moment d'annoncer l'événement, Québec a insisté sur l'importance d'éviter toute stigmatisation, même si l'actualité récente a été fortement marquée par le terrorisme islamiste.

«Le terme "radicalisation" englobe tout. On ne veut pas non plus identifier ou montrer du doigt des gens ou des groupes en particulier», a signalé la ministre des Relations internationales, Christine St-pierre.

FranceTv Info (site web)
Pour se protéger contre l'espionnage russe, le gouvernement britannique bannit l'Apple Watch
Tuesday, 11 October 2016

Londres - Pour se protéger contre l'espionnage russe, le gouvernement britannique bannit l'Apple Watch des ministères
En Grande Bretagne, la montre connectées d'Apple est désormais interdites lors des réunions ministérielles. Les services de sécurité pensent que la Russie pourrait y placer un mouchard.

La montre connectée d'Apple n'est pas la bienvenue au sein du gouvernement britannique. Le gadget est désormais banni des ministères. Motif ? Un risque d'espionnage. Des hackers pourraient se servir de ces montres pour écouter les conversations de leurs propriétaires.

Des montres qui peuvent devenir des mouchards

C'est le quotidien Telegraph qui révèle que les ministres britanniques ont été priés de ne pas porter d'Apple Watch lors des réunions officielles du Cabinet par crainte d'espionnage russe. Ces montres comportent un petit micro, qui sert à activer la commande vocale, à dicter des messages ou à répondre à des appels. On peut penser que c'est ce qui inquiète les autorités car, du coup, ces montres peuvent, en théorie, être transformées en mouchard afin d'écouter des conversations. Certes, pour cela, encore faut-il qu'un logiciel espion ait été introduit dans la montre. Les services de sécurité britanniques pensent que les Russes en sont capables, visiblement.

Les smartphones et les tablettes sont déjà interdits de séjour lors des réunions du cabinet britannique depuis 2013 et doivent rester à l'écart, enfermés dans des boîtes qui ne laissent passer ni les bruits ni les ondes.

The National (UAE)
NYU Abu Dhabi engineers seek to make cities more secure
Tuesday, 11 October 2016
Byline: Caline Malek

Abu Dhabi - The UAE is hardening its critical infrastructure against hacking with plans to test the security of electronic chips used to operate everything from a city's power grid to phones, satellites, aviation, and medical and military applications.
Earlier this year, cybersecurity experts and materials engineers warned that defects could be introduced in manufacturing these components, compromising their efficiency and safety.

The UAE owns the semi-conductor manufacturing company Global Foundries, which has a fabrication facility in New York which benefited from a multi- billion dollar investment last year. However, making these outside the UAE means there could be a security risk in the supply chain.

Now New York University Abu Dhabi is moving forward with a plan to test these components. "Someone may alter the design or insert something malicious into the final chip," said Ozgur Sinanoglu, associate professor of electrical and computer engineering at NYUAD. "We need to make sure no trojans are inserted inside the chip, and my research addresses these kind of problems."

NYUAD has created a test bed in its laboratory at the Saadiyat Island campus, allowing students to hack devices and create defences, said Michail Maniatakos, assistant professor of electrical and computer engineering.

"The devices control some kind of industrial process, whether a nuclear factory or a whole city's power, and we'd like to see the effect of hacking into the process and what can happen to a city," he said.

The team mapped the UAE and New York power grids for simulation. They also plan to map the UAE's transport networks, including cameras, toll gates and traffic lights. Mapping can take between a week and six months.

"The attackers are always a step ahead. For every defence you implement, they'll come up with a new attack," said Prof Maniatakos.

"So to win the game, you have to attack it first before someone else does it for you. This needs a proper security mindset that is heavily needed here."

The university is working with the US government to better protect its army, and Global Foundries, owned by Mubadala, to make chips with built-in defence systems. "We're about to finish the first secure version and the chip will hopefully be fabricated in the next month for the first time in the UAE," Mr Sinanoglu said.

"It's a lot of research but we have the opportunity for the first time to create something real. The threats are out there and this affects everybody equally."

Experts said the project is vital for cyber security in the UAE. "It proves again that Abu Dhabi is leading the region in advanced research and development projects across all sectors to now include defence, space and security innovations," said Matthew Cochran, chairman of the Defence Marketing Services Council in Abu Dhabi.

Cyber security for the so-called "internet of things" - the increased connectedness of physical devices through the internet - could still be improved, he said. "We must protect ourselves from those that would do our society harm via hacked and inserted kill switches that could make our everyday equipment useless," said Mr Cochran.

Straits Times
Singapore launches $10m fund to help Asean fight cyber threats
Thursday, 13 October 2016
Byline: Lim Yan Liang

Singapore - Singapore is taking concrete steps to step up cooperation across Asean for a more secure cyberspace, Communications and Information Minister Yaacob Ibrahim said Tuesday as he launched a $10 million fund to help fellow Asean nations build up their cyber response capabilities.
Ibrahim, who is minister-in-charge of cyber security, told the first Asean Ministerial Conference on Cyber Security at the Shangri-La Hotel the grouping could focus its efforts in three areas to fight the "full spectrum of cyber threats: Cybercrime, espionage, and other malicious activities".

The meeting came a day after Singapore launched its National Cyber Security Strategy, in which building regional and global partnerships to fight cyber threats is a key pillar.

The first area Asean members can cooperate in is helping strengthen one another's technical capabilities to better respond to incidents.

South-east Asia is a prime target for cyber attacks, and a Singtel-FireEye study found organisations in the region face a 45 per cent higher risk of a targeted cyber attack than the global average. One in four such attacks is aimed at governments.

"Attack targets could range from financial to data theft, reputational damage, and also disruption to our critical information infrastructure," Yaacob said.

The new $10 million Asean Cyber Capacity Programme is aimed at building up a credible response to such threats, he added. It will help train technical officers to deal with attacks, and train policymakers and prosecutors to shape members' cyber-security strategies and laws.

Second, Asean members can tap into global efforts to build a trusted cyberspace, like the Interpol Global Complex for Innovation (IGCI) that is based here, Yaacob said.

"We can support the IGCI by seconding more Asean law-enforcement officers to the IGCI. By partnering Interpol, we can conduct more joint operations against cyber criminals and enhance the collective safety and security of Asean."

Singapore will also contribute $900,000 to the CyberGreen global initiative that provides tools for a country to measure its level of cyber health, announced Yaacob.

With this funding, all Asean members can access the CyberGreen platform through Singapore for free and better identify different levels of threats and ways to counter them.

The third area is for Asean states to start a dialogue on cyber norms -- a conversation that began globally a decade ago -- to develop a regional understanding of such norms and take part in the global effort, he said.

"Cyber capacity- building, cyberspace awareness, and cyber norms: these are three suggestions to Asean for enhancing cyber-security cooperation," said Yaacob. "Singapore is committed to these ideas, and we are backing our words with resources and investment."

Sydney Morning Herald
PM's 'favourite thing': WhatsApp chat raises security fears
Thursday, 13 October 2016
Byline: James Massola

Sydney - Prime Minister Malcolm Turnbull and his most senior cabinet ministers are using a third-party messaging application to conduct confidential discussions, prompting cyber security experts to warn the innovation could actually pose a security risk.
The use of WhatsApp is not limited to senior ministers; private chat "groups" exist for government chiefs of staff, ministerial media advisers, the frontline economic team, and a defence-focused "broadcast group" used by Defence Industry Minister Christopher Pyne to communicate with MPs and staff.

Fairfax Media has spoken with four cyber security experts who have each flagged potential security issues with the widespread use of WhatsApp by the Turnbull government - particularly at a cabinet level - in place of secure, government email servers from platforms approved by the Australian Signals Directorate (ASD), Australia's cyber intelligence agency.

Craig Searle, the founder of security consultancy firm Hivint, pointed out WhatsApp was not an approved platform on the ASD list of Evaluated Products or Certified Cloud Services, whereas Apple's iOS operating system and Blackberry's operating system were.

"Should government be using secure messaging apps? Yes, they are a great idea. But for government staff in particular, they have to be cognisant of data classification requirements, they should behave securely and use products on the Australia government's certified list," Mr Searle said. "If a government employee were to transfer classified data across a non-approved app or network, that could be a potential security breach."

WhatsApp has a user base of about 1 billion people and can be used to send one-to-one and group messages, or video and make phone calls. It is owned by Facebook, with which it recently began to share more user data.

Multiple government staff confirmed to Fairfax Media the platform was widely used within the government, including by a group of cabinet ministers.

"I can't imagine ASD is very happy about it," one staffer said.

A government spokesman said the WhatsApp groups were designed to improve internal government communication and co-ordination. The spokesman did not deny a cabinet-level group existed but said secure information such as classified, sensitive and "not for release" material was handled in the appropriate way.

"The government uses many channels of communications, including WhatsApp," he said. "All classified communications happen appropriately on secure channels. There is a protocol around the security of mobile devices."

But Australian Strategic Policy Institute cyber security expert Tobias Feakin said despite WhatsApp trumpeting end-to-end encryption - which secures a message once it is sent from one phone, via a server, to another phone - risks remained.

"The risk of WhatsApp is at either end of the cycle, on the sending device or receiving device. People can misplace a device and then it can potentially be accessed. Then there is phishing - someone clicking a link or opening an attachment [in the app] which downloads software," Dr Feakin said. "The headache for government is that this is a platform that rests outside government's purview and that therefore poses some security risks."

Queensland University of Technology security expert Emeritus Professor Bill Caelli said cabinet communications should happen on a secure device or not at all.

"If it's not on ASD's list ... the answer is 100 per cent 'no'."

University of Canberra director of internet safety Nigel Phair said "of course" cabinet ministers should not use WhatsApp.

One senior staffer said WhatsApp was the Prime Minister's "favourite thing, so everyone jumped on it" when Mr Turnbull became Liberal Party leader in September 2015.

Adelaide Advertiser
The bungling spies like us
Thursday, 13 October 2016
Byline: Peter Jean

Spy agency ASIO tapped the wrong phone by mistake, illegally hacked a computer and had to pay for professional carpet cleaning in a home its agents raided.

And its sister intelligence agency the Australian Secret Intelligence Service passed information about Australians to a "foreign liaison" without applying privacy rules. A series of stuff-ups by Australia's intelligence organisations have been made public in Inspector- General of Intelligence and Security's Margaret Stone's annual report. Most were reported to Ms Stone's office by the agencies themselves after they realised they had made mistakes.

The report reveals ASIO tapped the wrong phone because it had an "incorrect number" and a telco mistakenly sent the agency wrongly intercepted SMS messages. An "administrative "oversight" also led to a computer being accessed without a warrant from the Attorney- General. And a woman whose home was raided by ASIO agents executing a search warrant complained to the Inspector-General that the property had been left in a "disordered state" at the end of the search.

She added the list of seized property given to her by ASIO was so faint it was illegible.Ms Stone, a former Federal Court judge, has wide-ranging powers to review the activities of intelligence agencies.

Global Times
China must be wary of extremist cyber incitement
Thursday, 13 October 2016
Byline: Zhang Yi

Beijing - According to local media reports, a female student at a vocational school in Anhui Province stood trial on Tuesday for possessing items promoting terrorism and extremism. In 2013, she became friends with someone known as "Abdullah" on QQ, an online chat platform in China. She apparently planned to become a jihadist under Abdullah's incitement.
Terrorists and extremist groups have been using social networks to lure young people into jihad. According to a Washington Post report in 2014, online chat rooms advised girls on how to "discretely disobey their parents and sneak away."

Young men are victims as well. Aaron Riseberg, an American expert and tracker of online jihadists, once noted that online, young men often ended up creating a "self-inflicted post traumatic stress disorder" leading to violence.

Mohammed Emwazi, a British Arab and an alumnus of Britain's University of Westminster dubbed Jihadi John in the British press, was the executioner in a number of gruesome Islamic State videos showing the beheadings of hostages.

The increasing number of Americans and Europeans seeking to join terror groups suggests that IS' online efforts may be paying off, which requires vigilance and countermeasures from China, a victim of terror attacks in recent years.

Chinese religious extremists and separatists acting overseas have also made use of the Internet to indoctrinate people. The East Turkestan Information Center, a group affiliated with the East Turkestan Independence Movement (ETIM), propagandizes violence and terrorism on the Internet to foment ethnic resentment.

The ETIM, which has been labeled as a violent separatist group and a terrorist organization by many countries, has produced hundreds of videos on terrorism.

Instigation of terrorism and teaching of violent techniques via these videos on the Internet has become a new method for ETIM to evoke terror attacks in China. In 2014, police in the Xinjiang Uyghur Autonomous Region detained 232 people who circulated videos disseminating terrorism online.

The rise of the new media era coincides with the unchecked growth of terror groups that hold the "black flags of jihad." On the one hand, the popularity of new media platforms means information spread fast, but on the other, it provides more room for extreme religious views and terror thoughts.

China should join hands with the international community to keep a watchful eye on harmful information on the Internet and educate netizens about its detrimental effect on themselves and the country.

New York Times
Donald Trump Finds Improbable Ally in WikiLeaks
Thursday, 13 October 2016
Byline: Multiple reporters

New York - In the final weeks of a dizzying presidential campaign, Donald J. Trump is suddenly embracing an unlikely ally: The document- spilling group WikiLeaks, which Republicans denounced when it published classified State Department cables and Pentagon secrets about the wars in Iraq and Afghanistan.
Mr. Trump, his advisers, and many of his supporters are increasingly seizing on a trove of embarrassing emails from Hillary Clinton's campaign that WikiLeaks has been publishing -- and that American intelligence agencies said on Friday came largely from Russian intelligence agencies, with the authorization of "Russia's senior-most officials."

The Trump campaign's willingness to use WikiLeaks is an extraordinary turnabout after years of bipartisan criticism of the organization and its leader, Julian Assange, for past disclosures of American national security intelligence and other confidential information.

The accusation that Russian agents are now playing an almost-daily role in helping fuel Mr. Trump's latest political attacks on Mrs. Clinton raises far greater concerns, though, about foreign interference in a presidential election.

With the White House weighing its next move -- from possible sanctions to covert, retaliatory cyberaction -- President Vladimir V. Putin of Russia insisted on Wednesday that his nation was being falsely accused. "The hysteria is merely caused by the fact that somebody needs to divert the attention of the American people from the essence of what was exposed by the hackers," Mr. Putin said.

He did acknowledge that the disclosures were the work of an illegal hack -- which is further than Mr. Trump went in Sunday's debate. In one exchange with Mrs. Clinton, the Republican candidate said: "Maybe there is no hacking. But they always blame Russia," he said, as part of an effort to "tarnish me."

Mr. Trump has seized on more than 6,000 emails published so far this week, apparently from the personal Gmail account of Mrs. Clinton's campaign chairman, John D. Podesta. Based on a few emails plucked from the account, Mr. Trump and his team have accused Clinton aides of improperly receiving inside information from the Obama administration.

That stems from correspondence that shows that the campaign received an update from the Department of Justice about the timing of the release of Mrs. Clinton's State Department emails. On Wednesday, Trump advisers flagged others messages that they argued were critical of New Hampshire voters and of Catholics.

As Mr. Trump struggles to rebound from revelations that he bragged in 2005 about his power to sexually assault women, Republican allies say he has come to believe that WikiLeaks could yield a critical mass of negative and destructive information -- if not a smoking gun -- that drives up Mrs. Clinton's already high unfavorable ratings with voters and perhaps even derails her candidacy.

Following Mr. Trump's wishes, his advisers have aggressively pushed the Clinton camp emails in news media briefings and cable news appearances, bringing up the hacked messages to battle back from the questions about Mr. Trump's comments about women. But as much as Mr. Trump sees WikiLeaks coming to his rescue, strategists in his own party take a dim view of its ultimate impact.

The Clinton campaign is trying its own political jujitsu with the hacks, arguing that they are more evidence that Mr. Trump is in the pocket of Mr. Putin, whom the Republican candidate has declined to denounce for his annexation of Crimea, his intimidation of former Soviet states that are now part of NATO, or for its abandonment last week of a nuclear arrangement with the United States. Mr. Podesta has gone even further, saying in a statement on Wednesday evening that there was "the possibility that Trump's allies had advance knowledge of the release of these illegally obtained emails."

Intelligence officials say that so far they have not concluded there was any such collusion, but the investigation into who got into Mr. Podesta's emails, and how they got into WikiLeaks' hands, has just begun.

Those emails began to appear on Friday afternoon, just hours after the director of National Intelligence and the Department of Homeland Security issued a statement attributing previous hacks to the Russian government. Officials on Wednesday said it may take weeks to establish whether Mr. Podesta's emails were also hacked by the Russians -- though they said the attack on his Gmail account fits the pattern of previous Russian- sponsored email thefts.

Republicans have previously condemned WikiLeaks and similarly blasted the leaks by Edward J. Snowden, a National Security Agency contractor, and said they were evidence of carelessness by the Obama administration.

When Mr. Snowden's disclosures about the scope of the N.S.A. spying were brought to light, it touched off a feverish debate over government invading people's privacy, and many Republicans denounced Mr. Snowden as a traitor. The emails from Mr. Podesta were also the result of an illegal hack -- but of a private email account or campaign emails, not a government agency.

Among the Trump supporters who have most vocally praised WikiLeaks is Sean Hannity, the Fox News host who excoriated the site's editor, Julian Assange, years ago.

Representative Peter T. King, the Republican from Long Island, who supports Mr. Trump, said he would not go as far as Mr. Hannity had in "rehabilitating Assange." Then, conflating the WikiLeaks disclosures with the Snowden disclosures, he added that: "I thought what Snowden did was disgraceful, treasonous. But the reality is the information is out there, and if Hillary doesn't deny it then to me it certainly has to be used."

Rudolph W. Giuliani, the former New York City mayor and another Trump supporter, said that Democrats showed no compunction about using unauthorized material when it came to Mr. Trump's 1995 tax returns, or a leaked NBC audio recording of Mr. Trump boasting about groping. Mr. Trump's campaign manager, Kellyanne Conway, insisted on Wednesday that the information that WikiLeaks and other outlets had made public from hacking collectives is "relevant."

"But for this information, a number of revelations would remain secret -- how Hillary Clinton really feels, how paranoid she really was about an Elizabeth Warren challenge, her ability to articulate a message that's cohesive and credible," Ms. Conway said in an interview. She dismissed questions about spreading information that is stolen and in some cases unsubstantiated. "They say stuff all the time that's not verified," Ms. Conway said of Democrats. "This is the wild wild West of instantaneous information that people neither trust nor verify, they just repeat."

Ms. Conway and the former House speaker, Newt Gingrich, held a conference call with reporters to highlight an email from Mrs. Clinton's campaign manager, Jennifer Palmieri, which they insisted showed "bias" toward Catholics. Ms. Palmieri told reporters she did not recognize that email.

While some Republican strategists questioned the maneuver by Mr. Trump, the Clinton campaign seemed uncertain about how to navigate the disclosures, particularly after calling attention to the unauthorized disclosures of pages of Mr. Trump's tax returns in The New York Times and an 11-year-old tape featuring the candidate bragging about forcing himself on women. For the most part, the Clinton team repeatedly criticized news organizations for using hacked materials. But privately, Democrats expressed deep concern about how much more widespread the breaches could be.

Counting on an "October surprise" bombshell has never been a winning gambit for a struggling presidential nominee, and Republican pollsters say that the WikiLeaks email will do little to help Mr. Trump attract more undecided voters, especially women, or reassure wavering Trump supporters.

More than anything, pollsters say, the emails will merely reinforce the views of relatively narrow numbers of people who are intensely suspicious of government. "Trump has a hard-core base," said Neil Newhouse, a Republican pollster. "They ought to spend less time figuring out how to reinforce those people and more time trying to add to his vote column."

Mr. Trump, at a rally on Wednesday afternoon in Ocala, Fla., called the hacked campaign emails "unbelievable" and urged voters to read the messages "released by WikiLeaks." He said the emails "make more clear than ever, just how much is at stake in November and how unattractive and dishonest our country has become."

"It tells you the inner heart," he said. "You got to read it."

For many of Mr. Trump's supporters, the sudden appearance of confidential Clinton campaign emails is a stroke of fortune that, they think, could improve Mr. Trump's chances of winning on Nov. 8. "I think if he makes it a big deal, if he keeps on pressuring on it, it really will help," said Diego Rielo, 24, of Gainesville, Fla.

Dane Graves, 47, of Dunnellon, Fla., said the email disclosures were a strategic benefit for Mr. Trump because they "reaffirmed" comments that he has made as a candidate about the two-faced nature of politicians and alleged malfeasance in government.

"He's not basing his campaign on WikiLeaks -- it's only backing up what he's been saying the whole time," Mr. Graves said. "It's really backing up what the people have been feeling all of this time about the corruption of government, embedded, just the trickle-down corruption."

Some veteran Republican strategists say the WikiLeaks disclosures may be heartening to Mr. Trump and his supporters, but the emails are highly unlikely to influence undecided voters in battleground states like Ohio and North Carolina..

"There's real nihilism in the Trump campaign right now, just determined to do anything and say anything to make this the most disgusting final weeks in a presidential campaign ever," said Steve Schmidt, who

was a senior adviser to John McCain's campaign in 2008. "Distrust of Clinton is pretty well baked into parts of the electorate right now. But 55 to 60 percent of the country is open to a Clinton presidency and wants to see the next president get to work with Congress to help the country."

Washington Post
Social media spur adoration - and assassins, study says
Thursday, 13 October 2016
Byline: Michael Rosenwald

Washington - Social media have altered the motives and targets of those who set out to kill public figures, spreading the threat beyond politicians to music stars, athletes and other pop-culture icons, according to a new study by a senior FBI official and a prominent forensic psychologist.
The study, which was published online Wednesday in the journal Behavioral Sciences and the Law, aims to update a landmark Secret Service report that examined attacks on public figures between 1949 and 1995, ending with the "Unabomber," Ted Kaczysnki.

That report, which looked at 83 attackers, found that 68 percent of targets were government or judicial figures, while 19 percent were celebrities. The new study is narrower - 58 attackers from 1995 to 2015 - but it found that 38 percent targeted government or judicial figures, while 34 percent focused on movie, sports and media celebrities.

The authors attribute that shift to Facebook, Twitter, Instagram and other social media, which fuel a culture of celebrity and create an illusion of intimacy with stars.

For some attackers, especially the one-third who are delusional, this digital relationship feels like a personal connection, with a seemingly two-way conversation that amplifies infatuation.

At the same time, the public figures traditionally stalked by assassins - politicians and other government officials - have lost some of their appeal, the study found. They aren't seen as powerful symbols whose deaths will provide eternal fame. Rather, attackers who go after them blame them for their troubled lives and are seeking retribution - a motive that puts pop-culture figures at risk as well.

"These attacks are now angry and personal," said J. Reid Meloy, the lead author of the paper and a professor of forensic psychiatry at the University of California at San Diego. "They don't want fame. They want revenge for some perceived wrong."

Meloy and co-author Molly Amman, program manager in the FBI behavioral-analysis unit that studies targeted attacks, coined a term for this new type of targets: "publicly intimate figures." And social media doesn't just offer attackers this faux connection. It can also tip them off to where a target might soon be.

In the paper, the authors describe dozens of victims who are public figures: Paris Hilton, attacked outside a courthouse by a stalker; Tom Brokaw, targeted with anthrax, allegedly by a disgruntled researcher wanting money; and Roanoke television reporter Alison Parker, killed on live TV by an angry former co-worker.

Given the timeline of the study, the authors could not include this summer's fatal shooting of Christina Grimmie, a former singer on "The Voice." But that attack, Meloy said, is an important example of his study's findings. Grimmie was shot by a man obsessed with her social-media posts. He lost weight and became a vegan to try to win her heart.

Reaction to the study in threat-assessment and criminology circles was mixed.

"To those of us involved in threat assessment, this is data that confirms what we have been observing," said Mario Scalora, who directs the Targeted Violence Research Team at the University of Nebraska.

Marisa R. Randazzo, former chief research psychologist at the Secret Service and now a managing partner at Sigma Threat Management, said, "The reason why this is such an important study is that it provides a comprehensive view of the wide range of people who have become targets because of their public-figure status."

But other experts raised questions about the methodology, arguing that the data wasn't an apples-to-apples comparison with the earlier study and that the tally of attacks could be incomplete because they were identified by Google searches. Also, those arrested weren't interviewed, limiting insight into motive.

The authors acknowledged these potential shortcomings in the paper. (The authors of the previous study did not respond to requests for comment.)

The authors argue that fame has become less of a motive in attacks on public figures because social media provides the opportunity for anyone to become a star. Instead, attackers target public figures out of anger for some slight, real or perceived.

The study did find numerous aspects of attacks on public figures that have remained constant. The attackers are almost always male. They are often mentally disturbed. They don't make direct threats before taking action.

A spokeswoman for the Secret Service said the agency has reviewed attack trends, releasing a report last year. That report looked only at attacks on federal buildings or employees. The primary motive: "Retaliation for a perceived personal slight or wrong." Fourth on the list: "Seeking fame or attention."

NBC News

Russia May Be Hacking Us More, But China Is Hacking Us Much Less
Wednesday, 12 October 2016
Byline: Ken Dilanian

New York - In a rare bit of good cyber security news, Chinese hacking thefts of American corporate secrets have plummeted in the 13 months since China signed an agreement with the Obama administration to curb economic espionage, U.S. officials and outside experts say.
Analysts say the success may hold lessons for how the U.S. should deal with Russia, which at the same time has stepped up a different sort of hacking campaign that officials says is aimed at undermining confidence in the American election.

The change in China's behavior "has been the biggest success we've had in this arena in 30 years," said Dmitri Alperovitch, co-founder of Crowdstrike, a cyber security firm that tracks computer network intrusions.

"And it wasn't anything we did in cyber space -- it was the threat of sanctions and the impact on their economy."

Alperovitch said his firm has observed a 90 percent drop in commercial hacking against U.S. firms attributable to Chinese government actors. U.S, intelligence agencies also have reported a sharp falloff, according to officials briefed on the matter.

To be sure, Alperovitch and others say, Chinese intelligence agencies are still hacking to steal national U.S. security secrets, including attacking defense firms. But those attacks are considered commonplace, because they are exactly what the National Security Agency does to China and other U.S. adversaries.

At issue in the agreement President Obama signed with President Xi Jinping in September 2015 was hacking to steal corporate intellectual property to benefit Chinese firms. The U.S. says it doesn't do that, but China did it with impunity for years, in what a former NSA director called the biggest transfer of wealth in modern history.

After years of pressure, Obama elevated the issue and threatened sanctions on China. The U.S. also indicted five members of the People's Liberation Army in 2014, accusing them of commercial hacking.

In the agreement, China essentially promised to stop doing it.

The dropoff actually began a year before the agreement was signed, according to a study released in June by the iSight intelligence unit of FireEye, a cyber security company.

"Since mid-2014, we have observed an overall decrease in successful network compromises by China-based groups against organizations in the U.S. and 25 other countries," the report said. "These shifts

have coincided with ongoing political and military reforms in China, widespread exposure of Chinese cyber activity, and unprecedented action by the U.S. government."

In addition, a cyber hotline to facilitate speedy communication between China and the U.S. over hacking incidents is in the testing phase, U.S. officials told NBC News.

Instead of targeting U.S. firms, Alperovitch said, China has turned its hackers inward, probing Chinese companies as part of an anti-corruption campaign -- and also against Russia.

"We're seeing a massive increase in domestic intrusions (by the Chinese government) against companies in China where they are using this for an anti-corruption campaign," he said. "And we're actually seeing a massive increase in attacks on Russia. They've stolen everything that Russia has in the defense space."

Last week, the Obama administration formally accused Russia of a campaign of hacking designed to interfere in the U.S. election campaign, including an effort to steal and leak embarrassing emails by Democrats. So far, the U.S. has taken no observable action in response.

White House Press Secretary Josh Earnest said Tuesday that the U.S. is mulling a "proportional" response to Russia, but he declined to be more specific.

"The president has talked before about the significant capabilities that the U.S. government has to both defend our systems in the United States but also carry out offensive operations in other countries," he said on Air Force One en route to a Hillary Clinton campaign event in North Carolina. "So there are a range of responses that are available to the president and he will consider a response that is proportional."

Fox News
FBI, DOJ roiled by Comey, Lynch decision to let Clinton slide by on emails, says insider
Wednesday, 12 October 2016
Byline: Malia Zimmerman, Adam Housley

Washington - The decision to let Hillary Clinton off the hook for mishandling classified information has roiled the FBI and Department of Justice, with one person closely involved in the year-long probe telling FoxNews.com that career agents and attorneys on the case unanimously believed the Democratic presidential nominee should have been charged.
The source, who spoke to FoxNews.com on the condition of anonymity, said FBI Director James Comey's dramatic July 5 announcement that he would not recommend to the Attorney General's office that the former secretary of state be charged left members of the investigative team dismayed and disgusted. More than 100 FBI agents and analysts worked around the clock with six attorneys from the DOJ's National Security Division, Counter Espionage Section, to investigate the case.

"No trial level attorney agreed, no agent working the case agreed, with the decision not to prosecute -- it was a top-down decision," said the source, whose identity and role in the case has been verified by FoxNews.com.

A high-ranking FBI official told Fox News that while it might not have been a unanimous decision, "It was unanimous that we all wanted her [Clinton's] security clearance yanked."

"It is safe to say the vast majority felt she should be prosecuted," the senior FBI official told Fox News. "We were floored while listening to the FBI briefing because Comey laid it all out, and then said 'but we are doing nothing,' which made no sense to us."

Andrew Napolitano, former judge and senior judicial analyst for Fox News Channel, said many law enforcement agents involved with the Clinton email investigation have similar beliefs.

"It is well known that the FBI agents on the ground, the human beings who did the investigative work, had built an extremely strong case against Hillary Clinton and were furious when the case did not move forward," said Napolitano. "They believe the decision not to prosecute came from The White House."

The claim also is backed up by a report in the New York Post this week, which quotes a number of veteran FBI agents saying FBI Director James Comey "has permanently damaged the bureau's reputation for uncompromising investigations with his cowardly whitewash of former Secretary of State Hillary Clinton's mishandling of classified information using an unauthorized private email server."

"The FBI has politicized itself, and its reputation will suffer for a long time. I hold Director Comey responsible," Dennis V. Hughes, the first chief of the FBI's computer investigations unit, told the Post. Retired FBI agent Michael M. Biasello added to the report, saying, "Comey has singlehandedly ruined the reputation of the organization."

Especially angering the team, which painstakingly pieced together deleted emails and interviewed witnesses to prove that sensitive information was left unprotected, was the fact that Comey based his decision on a conclusion that a recommendation to charge would not be followed by DOJ prosecutors, even though the bureau's role was merely to advise, Fox News was told.

"Basically, James Comey hijacked the DOJ's role by saying 'no reasonable prosecutor would bring this case,'" the Fox News source said. "The FBI does not decide who to prosecute and when, that is the sole province of a prosecutor -- that never happens.

"I know zero prosecutors in the DOJ's National Security Division who would not have taken the case to a grand jury," the source added. "One was never even convened."

Napolitano agreed, saying the FBI investigation was hampered from the beginning, because there was no grand jury, and no search warrants or subpoenas issued.

"The FBI could not seize anything related to the investigation, only request things. As an example, in order to get the laptop, they had to agree to grant immunity," Napolitano said.

In early 2015, it was revealed that Clinton had used a private email server in her Chappaqua, N.Y., home to conduct government business while serving from 2009-2013. The emails on the private server included thousands of messages that would later be marked classified by the State Department retroactively. Federal law makes it a crime for a government employee to possess classified information in an unsecure manner, and the relevant statute does not require a finding of intent.

Although Comey found that Clinton was "extremely careless in their handling of very sensitive, highly classified information," he said "no charges are appropriate in this case."

Well before Comey's announcement, which came days after Bill Clinton met in secret with Comey's boss, Attorney General Loretta Lynch, there were signs the investigation would go nowhere, the source told FoxNews.com. One was the fact that the FBI forced its agents and analysts involved in the case to sign non-disclosure agreements.

"This is unheard of, because of the stifling nature it has on the investigative process," the source said.

Another oddity was the five so-called immunity agreements granted to Clinton's State Department aides and IT experts.

Cheryl Mills, Clinton's former chief of staff, along with two other State Department staffers, John Bentel and Heather Samuelson, were afforded immunity agreements, as was Bryan Pagliano, Clinton's former IT aide, and Paul Combetta, an employee at Platte River networks, the firm hired to manage her server after she left the State Department.

As Fox News has reported, Combetta utilized the computer program "Bleachbit" to destroy Clinton's records, despite an order from Congress to preserve them, and Samuelson also destroyed Clinton's emails. Pagliano established the system that illegally transferred classified and top secret information to Clinton's private server. Mills disclosed classified information to the Clinton's family foundation in the process, breaking federal laws.

None should have been granted immunity if no charges were being brought, the source said.

"[Immunity] is issued because you know someone possesses evidence you need to charge the target, and you almost always know what it is they possess," the source said. "That's why you give immunity."

Mills and Samuelson also received immunity for what was found on their computers, which were then destroyed as a part of negotiations with the FBI.

"Mills and Samuelson receiving immunity with the agreement their laptops would be destroyed by the FBI afterwards is, in itself, illegal," the source said. "We know those laptops contained classified information. That's also illegal, and they got a pass."

Mills' dual role as Clinton's attorney and a witness in her own right should never have been tolerated either.

"Mills was allowed to sit in on the interview of Clinton as her lawyer. That's absurd. Someone who is supposedly cooperating against the target of an investigation [being] permitted to sit by the target as counsel violates any semblance of ethical responsibility," the source said.

"Every agent and attorney I have spoken to is embarrassed and has lost total respect for James Comey and Loretta Lynch," the source said. "The bar for DOJ is whether the evidence supports a case for charges - - it did here. It should have been taken to the grand jury."

Also infuriating agents, the New York Post reported, was the fact that Clinton's interview spanned just 3½ hours with no follow-up questioning, despite her "40 bouts of amnesia," and then, three days later, Comey cleared her of criminal wrongdoing.

Many FBI and DOJ staffers believe Comey and Lynch were motivated by ambition, and not justice, the source said.

"Loretta Lynch simply wants to stay on as Attorney General under Clinton, so there is no way she would indict," the source said. "James Comey thought his position [excoriating Clinton even as he let her off the hook] gave himself cover to remain on as director regardless of who wins."

The decision by Comey and Lynch not to prosecute has renewed FBI agents' belief that the agency should be autonomous.

"This is why so many agents believe the FBI needs to be an entity by itself to truly be effective," the senior FBI official told Fox News. "We all feel very strongly about it -- and the need to be objective. But that truly cannot be done when the AG is appointed by a president and attends daily briefings."

Adding to the controversy, WikiLeaks released internal Clinton communication records this week that show the Department of Justice kept Clinton's campaign and her staff informed about the progress of its investigation.

Leaked emails from Clinton campaign chairman John Podesta's gmail account show the Clinton campaign was contacted by the DOJ on May 19, 2015.

"DOJ folks inform me there is a status hearing in this case this morning, so we could have a window into the judge's thinking about this proposed production schedule as quickly as today," Clinton press

secretary Brian Fallon wrote in relation to the email documentation the State Department would be required to turn over to the Justice Department.

Jay Sekulow, chief counsel for the American Center for Law and Justice, who previously served in the U.S. Treasury Department in the Office of Chief Counsel for the IRS, where he was responsible for litigation in the U.S. Tax Court, said it was clear from the start that the FBI never intended to prosecute.

"This was a fake, false investigation from the outset," Sekulow said.

Washington Post
NSA contractor thought to have taken classified material the old- fashioned way
Wednesday, 12 October 2016
Byline: Ellen Nakashima, Matt Zapotosky

Washington - Harold T. Martin III is accused of stealing mounds of classified information from the government for at least a decade, and investigators also believe some of the information was taken the old- fashioned way -- by walking out of the workplace with printed-out papers he had hidden, according to U.S. officials.
The case against Martin, which was unsealed last week, raises new questions about whether the National Security Agency and other agencies are doing enough to detect and prevent their sensitive data from leaving the secure confines of government offices.

While investigators believe much of Martin's material was removed before stringent controls were imposed in the wake of 2013 disclosures linked to former NSA contractor Edward Snowden, some feel the system still failed.

When investigators searched Martin's home, they seized several terabytes of data, which Martin stored on dozens of computers and other devices, and thousands of pages of documents, according to the officials, who spoke on the condition of anonymity to discuss an open case. Investigators are still exploring whether he was connected in any way to the online leak of some of the NSA's most powerful hacking tools in August.

"Someone was able to walk out the front door with a whole bunch of stuff from NSA," said one congressional aide. "That's not supposed to happen."

Martin has been charged with theft of government property and unauthorized removal of classified materials. His attorney has said there is "no evidence" that he intended to betray his country. Martin previously worked in the Navy -- he left active duty in 1992 -- before taking a variety of tech jobs with government contractors, according to records and people who knew him.

In an interview, the head of the office responsible for setting policies aimed at deterring data loss said he thought the existing controls were sufficient. The question, said William Evanina, director of the National Counterintelligence and Security Center, is whether the controls were being successfully implemented.

"I don't believe there's anything new that we have to incorporate," said Evanina, who declined to comment on the ongoing investigation of Martin. "We just have to do a better job to see that what we already have in place is working effectively."

The NSA did not respond to a request for comment.

Martin worked at the NSA from 2012 to 2015. He was an employee of intelligence contractor Booz Allen Hamilton, which had also employed Snowden.

For some portion of that time, Martin was in the world's most elite hacker shop: the NSA's Tailored Access Organization, according to a former member of the group. One former TAO hacker said that Martin worked in the unit's front office carrying out support roles such as setting up accounts, instead of conducting actual operations.

Officials have not said how, precisely, they think Martin was able to take information home.

The NSA had strengthened its data controls even before Snowden. After a series of disclosures posted by the anti- secrecy group WikiLeaks in 2010, the president ordered the creation of a National Insider Threat Task Force, now led by Evanina. That group crafted a series of policies not only to avert compromises of classified information, but also to detect and deter insiders who might pick up a weapon and harm others.

Then, in the wake of the Snowden disclosures, NSA officials announced they were taking 41 specific technical measures to control data. They included "smart-tagging data" so each electronic file touched could be tracked, and imposing greater oversight of personnel using the networks, NSA Deputy Director Richard Ledgett said in a February 2014 interview.

The agency also imposed a rule requiring two people to be present anytime data in server rooms was being transferred or copied, he said. But the two-person rule did not apply everywhere. Operational personnel, for instance, were exempt, former officials said.

According to former NSA officials and TAO operators, the agency's measures were in a natural tension with a desire to get the best out of their personnel.

"The challenge remains that you at some level need to trust your employees," said John C. "Chris" Inglis, the NSA's deputy director from 2006 to 2014. "And [if you impose too many controls], you're not going

to get any initiative or creativity out of them. The challenge is how do you align that with your need to ensure that they don't abuse that trust."

The NSA, for instance, like other agencies, does not impose universal checks of personnel and their belongings as they enter and leave agency buildings. Security guards conduct random checks and use their discretion.

"If you have a bag full of stuff, you're probably going to get stopped," said a former TAO operator. But, in general, the employee said, "Disneyland has more physical security checks than we had."

Evanina said imposing universal body and bag checks "is not the solution we're looking to arrive at to keep and build the trust of our employees."

Despite all the measures that are in place, Evanina said, it is not always possible to detect an insider who is determined to find a way to thwart them.

"If someone is willing to make the decision that they're going to exfiltrate documents or data out of an organization," he said, "they're going to be successful at that."

Martin's alleged thefts took place at a number of workplaces over the years, officials said, including the NSA, the Office of the Undersecretary of Defense for Intelligence and the Office of the Director of National Intelligence.

He typically worked for a contractor. He was at Booz from 2009 to 2016, which said it fired him after his arrest. Before that he was at Tenacity Solutions, which provides information technology services, officials said. He also worked in the 1990s at CSC, another IT firm, officials said. While at Tenacity, Martin worked at ODNI.

CSC confirmed Martin's employment, but it declined to comment further. Tenacity did not return messages seeking comment.

Martin's last job was at the Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, which deals with the Pentagon's major procurement programs -- many of which are highly sensitive and classified. He also in recent years studied at the University of Maryland Baltimore County.

Roy Rada, a former adviser to Martin at the school, said Martin told him he was in a military transition program meant for soldiers who were suffering from post-traumatic stress disorder and that he was "experiencing some difficulties in adjusting to non-war-life." He said Martin was interested in researching PTSD, particularly by using what is known as an eye tracker, a device that analyzes a person's gaze, to detect brain malfunctions.

Australian Associated Press
Govt ministers defend PM's use of Whatsapp
Thursday, 13 October 2016

Canberra - Government ministers have defended their use of messaging service WhatsApp, despite warnings that it could pose a security risk.
Prime Minister Malcolm Turnbull, his cabinet colleagues and others - including chiefs of staff and media advisers - have been using the Facebook- owned application to communicate instead of other secure platforms.

It's believed the country's cyber intelligence agency, the Australian Signals Directorate, has not approved its use, prompting concerns from experts.

Dan Tehan, the minister assisting the prime minister for cyber security, refused to confirm if that was the case but was confident it was being used properly.

"All I will say is that the government, cabinet ministers, ministers, members of parliament, take their personal security and their security online very seriously," he told reporters in Canberra on Thursday.

He isn't aware of anyone doing anything wrong by using the third- party tool.

"The most important thing is that whatever they do, that they do it in a secure way if they're dealing with material which has a security classification," Mr Tehan said.

Ministers Steve Ciobo and Anne Ruston said they both use the app but not for confidential discussions.

"I don't think there's any security risk associated with using it," Senator Ruston said.

Shadow attorney-general Mark Dreyfus called on Mr Turnbull and his cabinet to stop using WhatsApp immediately.

He suggested the app was being used to avoid any obligations under the Freedom of Information Act.

"They are treating security with contempt," he told ABC radio.

Crossbench senators Nick Xenophon and David Leyonhjelm said they, too, have messaged the prime minister using various apps and have no issue with it.

"What do you want the prime minister to do, use smoke signals? Telepathy?" Senator Xenophon said.

"I think WhatsApp is a reasonable form of communication and safer than others, but I'd like to think the prime minister is smart enough to realise he's not going to be giving any state secrets over anything that isn't sufficiently encrypted."

CNN.com
Feds believe Russians hacked Florida election-systems vendor
Wednesday, 12 October 2016
Byline: Multiple reporters

Washington - Federal investigators believe Russian hackers were behind cyberattacks on a contractor for Florida's election system that may have exposed the personal data of Florida voters, according to US officials briefed on the probe.
The hack of the Florida contractor comes on the heels of hacks in Illinois, in which personal data of tens of thousands of voters may have been stolen, and one in Arizona, in which investigators now believe the data of voters was likely exposed.

The FBI, in the coming days, is preparing to provide updated guidance to state elections officials around the US aiming to help them spot suspicious activity on their computer networks. Several states have reported attempted scans of their computer systems, which often is a precursor to a breach.

Previously, Illinois officials have said data on fewer than 90,000 people may have been affected by a breach there, and Arizona officials said they saw no indications hackers accessed data in their systems.

The vendor hack in Florida prompted the FBI last week to coordinate an emergency call with county election supervisors who operate the election system in the perennial battleground state. CNN has not confirmed the name of the vendor that suffered the attack.

ABC News first reported that Florida election information was compromised.

Investigators believe a local contractor in California was the target of a hackers, but the systems accessed weren't related the elections, U.S. officials said.

A spokeswoman for the Florida Secretary of State said: "We currently have no indication of a Florida-specific issue. The Florida Voter Registration System database is secure. The Department of State does not utilize a vendor for voter registration services. The Department has in place many safeguards to prevent any possible attempts from being successful."

An FBI spokeswoman said the bureau and the Department of Homeland Security hosted a conference call with Florida state officials to address questions regarding the security of election systems and to share information regarding the general nature of the cyber threat. FBI and DHS continue to work closely with state officials to assist them in safeguarding their election infrastructures.

In the case of Arizona, US officials say the working assumption by investigators is that hackers were able to access data, even if there are no signs of tampering. Arizona officials maintain they've found no signs that hackers got in.

"We have no updates, our story hasn't changed," a spokesman for the Arizona secretary of state said. "We have seen no access into statewide registration database and no manipulation of that database."

FBI investigators believe the the hacks and attempted intrusions of state election sites were carried out by hackers working for Russian intelligence.

The cyberattacks on election registration sites are focused on parts of the US election system that wouldn't affect the votes cast or the vote counts, according to US officials. Instead, the intruders are targeting registration systems.

In a statement last Friday, the Director of National Intelligence and the Homeland Security Department formally blame Russia for hacking political organizations, including the Democratic National Committee, and orchestrating the release of private emails in an attempt to meddle in the US elections.

The statement said the US government wasn't yet ready to attribute the hacks of election registration sites.

Ottawa Citizen
A 'Stealth Takeover' of Canadian space tech
Monday, 17 October 2016
Byline: David Pugliese

Ottawa - An iconic Canadian space company, once the subject of an unprecedented move by the federal government to stop its sale to a U.S. firm, now has its operations controlled by an American corporation. Eight years ago, the Conservative government took the highly unusual step of blocking the sale of the British Columbia-based MacDonald Dettwiler and Associates, also known as MDA, to Alliant Techsystems of Minneapolis.

Prime Minister Stephen Harper's government intervened, saying the sale, which brought with it robotic arm technology and the high-tech Radarsat-2 satellite developed with money from Canadian taxpayers, was not of benefit to the country. The Conservatives were concerned about the U.S. controlling such a key Canadian aerospace and defence firm.

But over the last six months MDA, Canada's largest space company, has on its own significantly altered its corporate makeup to bring it within the U.S. orbit.

Its new chief executive officer, Howard Lance, is a U.S. citizen who now operates the company from its San Francisco headquarters. SSL MDA Holdings, Inc., registered as a corporation in Delaware, is now the operating company for all MDA businesses, both in the U.S. and Canada, the firm has announced.

On Oct. 3, the company made a series of new senior appointments, bringing in a retired U.S. air force general with a background in space operations as well as a former U.S. defence intelligence official who had worked for the CIA.

"What you're seeing is a stealth takeover of sensitive technology that Canadian taxpayers paid for," said Steve Staples, vice-president of the Rideau Institute in Ottawa, which was instrumental in the 2008 battle to stop the U.S. purchase of MDA's space division. "The very thing that the Conservative government was worried about has happened."

But Don Osborne, who is responsible for MDA's Canadian operations, said the company remains firmly Canadian. He acknowledged the Canadian and U.S. operations are now controlled by a U.S. corporation but pointed out that there are no changes to the way business is being done in Canada. The company still has its head office in Vancouver and is traded on the Toronto Stock Exchange, he added.

"From a management perspective, I have a boss who I report to who is in the United States," said Osborne, president of MDA's information systems group. "Companies have very complicated legal structures for all sorts of reasons."

Osborne said MDA has been very open about its need to expand and make inroads into the U.S. market.

"Part of the targeting of a U.S. market was to bring in management that can better access that market and we would structure ourselves legally in a way which would allow us to better access that market," he explained.

Chuck Black, an analyst in Toronto who operates a website dealing with commercial space activities, said Canada is losing control of its domestic space industry. Earlier this year, Canada's second largest space company, COM DEV, was purchased by a U.S. firm, Honeywell International, he pointed out.

"You have one company that has been bought outright by Americans," Black explained. "A second has reorganized so it is now operated out of the United States." Black said MDA's actions are aimed at winning lucrative U.S. military and government contracts, something its Canadian pedigree had hindered.

But both Black and Staples say MDA's initiative has security implications for Canada.

Black pointed out the U.S. government was able to delay for years the launch of Canada's Radarsat-2 surveillance spacecraft over its concerns about the type of data it would collect. As part of the ongoing dispute, the U.S. government prevented American technology from being used in the satellite and Canada had to rely on other nations for components.

Staples said MDA's restructuring gives the U.S. government more control over the firm's technology and how it is used.

"The company executives can say all they want about being Canadian, but the fact remains that U.S. national security interests apply to American companies and their subsidiaries wherever they are," he explained. "So U.S. law is now governing vital Canadian security and space assets."

MDA operates the Radarsat-2 satellite and is involved in other key Canadian spacerelated projects. It is also building a new generation of surveillance satellites for Canada.

After announcing the decision in April 2008 to stop the sale to Alliant Techsystems, then industry minister Jim Prentice said concerns over the transfer of Radarsat-2 technology to a U.S. company played a major role in the Conservative government's decision.

Jakarta Post
Indonesia's security strategies praised
Monday, 17 October 2016

Jakarta - Indonesia's efforts to handle global security matters including counterterrorism, deradicalization, migration and people smuggling was recognized during a recent inter-regional meeting.

The ASEAN-EU Ministerial Meeting (AEMM) in Bangkok on Thursday and Friday discussed current issues in Europe and Southeast Asia, regional security and counterterrorism efforts.

During the meeting, Indonesia emphasized strengthening cooperation on counterterrorism; strengthening the capabilities of anti-terror units and countering cyber terrorism; the mainstreaming of soft power through education, increasing the role of women, civil society and community and religious organizations.

"It is important to strengthen the cooperation between ASEAN and the EU, particularly against terrorism and extremism through the concrete cooperation of both parties," Foreign Minister Retno LP Marsudi said in a statement released by the Foreign Ministry.

A number of EU countries welcomed Indonesia's soft- power approach that focused on the values of tolerance and moderation in society.

In the future, the cooperation is expected to be increased through the dissemination of these values, in either bilateral or regional cooperation.

Retno also affirmed the importance of increasing maritime cooperation including illegal, unreported and unregulated (IUU) fishing as one of strategic cooperation.

She said that IUU fishing needed to be included in the transnational crime issue as it was related to people smuggling activities and drugs trafficking. On the sidelines of the meeting, Retno also discussed the planned visits of Polish and Dutch leaders.

Retno met with Polish Under Secretary of State for development Cooperation, Africa and the Middle East, Asia, Economic Diplomacy and Human Rights Joanna Wronecka, to discuss the planned visit of Polish President Andrzej Duda to Indonesia in 2017 to strengthen bilateral ties.

Meanwhile, Retno discussed the planned official visit of Dutch Prime Minister Mark Rutte to Indonesia, which is aimed at increasing trade and investment between both countries during a meeting with her Dutch counterpart, Bert Koenders.

Retno said the Netherlands would explore the possibility of cooperation in the field of infrastructure, particularly in seaport construction.

"The visit of Prime Minister Rutte is expected to further expand cooperation between the two countries that has already been working well and focused on Indonesia's development priorities such as infrastructure, trade and investment," Retno said.

The two governments have committed to realizing the Netherlands as a gateway for Indonesian products to Europe, meanwhile Indonesia as a gateway for Dutch products to the Southeast Asia region.

According to the Trade Ministry, Indonesia enjoyed a trade surplus of US$2.6 billion in 2015 in total trade between Indonesia and the Netherlands worth $4.2 billion.

The value of Indonesian exports to the Netherlands in 2015 reached $3.4 billion, while imports hit $785 million.

President Joko "Jokowi" Widodo visited the Netherlands on June 21 and 22, making it the first state-visit by an Indonesian president in 16 years, after late president Abdurrahman Wahid's visit in 2000.

Retno also held bilateral meetings with representatives from Denmark, Luxembourg, Latvia, Italy, Lithuania, and France on various issues.

Asharq al-Awsat
Surveillance Drones being Turned into Weapons by Extremists
Monday, 17 October 2016
Byline: Staff Report

London - Militant groups like Hezbollah and ISIS have learned how to weaponize surveillance drones and use them against each other, adding a new twist to Syria's civil war, a U.S. military official and others say.
A video belonging to an al-Qaeda offshoot, Jund al-Aqsa, purportedly shows a drone landing on Syrian military barracks. In another video, small explosives purportedly dropped by the Iran-backed so-called Hezbollah target the militant group Jabhat Fatah al-Sham, formerly known as al-Nusra Front, the Associated Press reported.

A U.S. military official, who spoke anonymously because he wasn't authorized to discuss the matter publicly, said the U.S. military is aware of the development. Commanders have warned troops to take cover if they see what they might have once dismissed as a surveillance drone, he said.

The head of the Airwars project, which tracks the international air war in Iraq, Syria and Libya, said the weaponized drones are clumsy but will scare people.

"There are a million ways you can weaponize drones -- fire rockets, strap things in and crash them," Chris Woods said. He added: "This is the stuff everyone has been terrified about for years, and now it's a reality."

The U.S. military official couldn't immediately authenticate the videos in question, adding that most of the incidents they are aware of involved weaponized drones that simply crash into their targets. But another former senior U.S. military official who viewed the videos said there was nothing to suggest they were fake.

A number of militant groups in the Middle East, including ISIS, Jund al-Aqsa and Jabhat Fatah al-Sham, as well as Hezbollah and Hamas, have all released videos indicating that they have surveillance and reconnaissance drones. Syrian anti-regime rebels and militias loyal to Bashar al-Assad were also flying cheap quad- and hexacopters as early as 2014 to spy on each other.

The surveillance drones allowed those groups to collect data on enemy bases, battlefield positioning and weaponry and improve targeting.

ISIS launched a sophisticated propaganda video in 2014, "The Clanging of the Swords, Part 4," boasting about its capture of the Iraqi city of Fallujah. The video opens with drone footage over the western Iraqi city before cutting to violent ground footage depicting its advance across Iraq.

Lebanon-based Hezbollah has claimed to have armed- drone capabilities for nearly two years, but a recent video of bomblets hitting a militant camp near the Syrian town of Hama is the first known documentation.

The majority of these groups have access only to store- bought drones, similar to those available in the U.S., ranging in price from $1,000 to $3,000 and weighing between 5 to 10 pounds -- certainly not enough to support a large bomb or rocket. Hezbollah is an exception, receiving most of its munitions -- including its drones -- from Iran.

Le Monde
Etats-Unis Relents de guerre froide dans le cyberespace
Monday, 17 October 2016
Byline: Martin Untersigner

Washington - L'administration Obama vient d'incriminer officiellement la Russie dans la cyberattaque qui avait ciblé, en juin, le Parti démocrate. Une accusation qui a encore envenimé les relations russo-américaines
La Russie tente " d'interférer avec le processus électoral américain " . Vendredi 7 octobre, après maintes tergiversations, l'administration Obama a officiellement confirmé, par la voix de son directeur du renseignement national (DNI) et de celle du département de la sécurité intérieure (DHS), l'implication de Moscou dans l'attaque informatique visant le Parti démocrate.

Cette accusation, au parfum de guerre froide et à un mois de l'élection présidentielle américaine, marque un tournant. Depuis des semaines, la Russie est suspectée d'orchestrer une série de piratages visant les Etats-Unis. Mais c'est la première fois que le gouvernement de Barack Obama incrimine directement Moscou dans " la récente compromission de courriels de citoyens et d'institutions américains, y compris d'organisations politiques " . Dans leur communiqué, le DNI et le DHS estiment

que " seuls les plus hauts responsables russes ont pu autoriser ces actions " , sans pour autant en apporter la preuve. Le Kremlin a qualifié cette allégation de " foutaise " .

Deux groupes pirates déjà soupçonnésMi-juin, le Comité national démocrate (DNC), l'organe du parti chargé d'organiser les élections pour l'investiture, avait prévenu que deux groupes de pirates avaient pénétré son réseau. Un mois plus tard, WikiLeaks publiait sur son site plusieurs milliers de courriels internes au parti, révélant que les caciques démocrates avaient pris fait et cause pour Hillary Clinton au détriment de son challenger Bernie Sanders.

Plusieurs incidents ont ensuite contribué à nourrir le climat de défiance vis-à-vis de Moscou. L'entreprise de sécurité informatique chargée de nettoyer les systèmes informatiques du DNC a indiqué que les pirates étaient liés aux services de renseignement russes. Le premier groupe, surnommé Cozy Bear (APT29), n'est pas un inconnu : il avait déjà été accusé au printemps 2015 d'avoir pénétré les réseaux de la Maison Blanche et du département d'Etat. Le second, appelé Fancy Bear (APT28), s'est lui aussi forgé une réputation : soupçonné depuis longtemps d'être lié au renseignement militaire russe, c'est vers lui que se dirigeait l'enquête sur le piratage, les 8 et 9 avril 2015, de la chaîne TV5Monde, selon une source judiciaire interrogée à l'époque par Le Monde . En juin de la même année, les services de renseignement allemands accusaient ce même groupe d'avoir espionné le Bundestag.

Plusieurs Etats américains ont également été victimes de piratages ou de tentatives d'intrusion visant leurs systèmes électoraux, en provenance, semble-t-il, de Russie. En juin 2016, le Federal Bureau of Investigation (FBI) avertissait l'Arizona d'une intrusion mineure visant sa base de données électorale. A l'approche des élections, la même police fédérale enjoignait l'ensemble des Etats à muscler leurs mesures de sécurité informatique, redoutant d'autres agressions. L'administration Obama est cependant moins affirmative quant à leurs commanditaires. " Dans la plupart des cas, - ces attaques - provenaient de serveurs gérés par une entreprise russe. Nous ne sommes cependant pas en mesure d'attribuer cette activité au gouvernement ", écrivent ainsi le DHS et le DNI dans leur communiqué.

Autre signe, plus indirect, de l'atmosphère irrespirable qui règne entre Moscou et Washington dans le cyberespace, la publication sur le Web, mi-août, d'outils sophistiqués d'espionnage numérique appartenant à l'Agence nationale de la sécurité américaine (NSA), considérée comme la plus puissante du monde en la matière. Que des pirates se soient procuré une partie de son arsenal et décident d'en publier son contenu a surpris la plupart des observateurs. S'agissait-il d'une fuite émanant d'une agence rivale russe, désireuse de lancer un avertissement? Les regards se sont tous tournés vers l'est, au moment où se précisaient les accusations d'une implication russe dans le piratage du Comité national démocrate.

La Russie est l'un des pays les plus actifs et les plus compétents en matière d'espionnage informatique. Le conflit en Ukraine a été l'occasion de constater son savoir-faire. De nombreuses attaques - de la fuite de courriels jusqu'à la saturation de sites Web, et même une brève extinction d'une partie du réseau électrique ukrainien - avaient alors été attribuées à des pirates russes par plusieurs laboratoires de

cybersécurité. La Russie est aussi classée par les autorités américaines, aux côtés de la Corée du Nord, de la Chine et de l'Iran, parmi les principaux adversaires des Etats-Unis dans le cyberespace.

Ces dernières années, au moins une demi-douzaine de groupes d'espionnage informatique, aux origines russes plus ou moins établies, ont été découverts par des experts basés en Allemagne, en Finlande, au Japon et aux Etats-Unis. Parmi les plus performants d'entre eux figurent ceux qui ont été identifiés dans les serveurs du Parti démocrate, notamment Fancy Bear. Ce dernier a été découvert à l'été 2014 par Feike Hacquebord, expert en sécurité informatique au sein de l'entreprise Trend Micro, basée au Japonet spécialisée en antivirus. M. Hacquebord assure aujourd'hui ne détenir " aucune preuve " de liens connectant Fancy Bear avec le Kremlin, précisant qu'il n'est pas " sage " de les voir nécessairement aux ordres de Moscou.

Mais leurs caractéristiques restent troublantes. Le groupe dispose, selon l'expert, " de très grandes ressources d'argent et de main-d'oeuvre " , dont l'activité diminue " pendant les vacances et pendant l'été ", signe qu'il s'agirait d'un groupe étatique. Les pirates de Fancy Bear, parmi les plus compétents observés, visent avec une intensité particulière " l'Ukraine, quasiment leur cible numéro un, les forces armées d'Europe de l'Est et les pays de l'OTAN " . Si des Russes figurent aussi parmi leurs victimes, ce sont pour l'essentiel des " activistes et opposants au régime " .

Quel intérêt aurait le Kremlin à s'attaquer au système électoral américain? Pour la Russie, " les cyberattaques sont des outils intégrés dans un effort plus large de maintien de sa domination politique et militaire sur un théâtre donné et, plus largement, sur les opinions publiques mondiales ", écrivait la chercheuse Jen Weedon dans un rapport de 2015 du Cooperative Cyber Defence Centre of Excellence (CCDCOE), un organisme de recherche consacré à la cyberdéfense patronné par l'OTAN.

" Instiller la confusion " " Les cyberattaques font partie d'une campagne pour instiller le doute et la confusion aux populations occidentales envers leurs institutions, embarrasser leurs gouvernements, affaiblir l'OTAN, les Etats- Unis et tout ce qui peut être un obstacle à la Russie ", estime de son côté Matthijs Veenendaal, également chercheur au CCDCOE. " Il ne s'agit pas tant de déterminer l'issue des élections américaines que d'entretenir le relativisme des Américains sur leur propre pays, de propager l'image d'élites corrompues, de nourrir la remise en cause des institutions ", précise Julien Nocetti, chercheur à l'Institut français des relations internationales (IFRI). Donald Trump, poursuit-il, " est le candidat idéal pour alimenter cette dialectique et attiser le sentiment que la démocratie n'est pas idéale ".

Les cyberattaques, discrètes et dont l'origine est difficile à déterminer, constituent les outils parfaits pour ce type de campagne de déstabilisation. Dans sa conception du cyber-espace et de la sécurité informatique, Moscou attribue autant d'importance aux contenus (informations, opinions) circulant sur le Web qu'au fonctionnement technique des infrastructures d'Internet. Ainsi, ses attaques informatiques comportent volontiers ces deux dimensions : provoquer la fermeture de sites et faire " fuiter " des informations. " Si les Américains se concentrent sur la sécurité des réseaux et des infrastructures, les Russes, eux, mettent l'accent sur le contenu ", explique le chercheur Julien Nocetti.

L'utilisation par le Kremlin de " fermes à trolls ", où des commentateurs sont payés pour influencer le débat en ligne, en Russie et aux Etats-Unis, est un autre volet de l'activité parfois délétère de la Russie sur Internet.

Le communiqué attribuant à Moscou la cyberattaque contre le Parti démocrate, quelques semaines avant le scrutin du 8 novembre, constitue un net palier dans la dégradation des relationsrusso-américaines dans le domaine de la cybersécurité. Il est rare que les Etats-Unis attribuent officiellement une cyberattaque, et plus encore qu'une puissance rivale soit ainsi désignée.

La Corée du Nord avait été mise en cause par le FBI, en décembre 2014, pour son implication présumée dans le piratage des serveurs du studio Sony Pictures. La même année, cinq militaires chinois avaient été accusés par la justice américaine d'espionnage informatique et de vol de secrets économiques dont auraient été victimes, aux Etats-Unis, les entreprises Westinghouse, Alcoa et United States Steel.

L'accusation portée contre la Russie est cependant d'une tout autre nature : les attaques chinoises et nord-coréennes visaient l'économie américaine, tandis qu'en ciblant le DNC à la veille des élections les pirates ont touché au fonctionnement même de la démocratie américaine, dans un contextede tensions entre Moscou et Washington. " Influencer le débat politique d'un pays, les Etats-Unis le font tout le temps - par la diplomatie, par exemple -, observe Adam Segal, du think tank américain Council of Foreign Relations. Mais attribuer l'attaque du DNC à la Russie est une manière de dire que ce pays a franchi une limite. "

Les Etats-Unis vont-ils apporter une réponse plus musclée à ces cyberattaques que cette stratégie du " name and shame " (" nommer et couvrir de honte ")? Cette dernière " peut avoir un impact si deux nations ont intérêt à s'entendre , explique Matthijs Veenendaal. Mais, actuellement, la Russie ne montre aucun signe de volonté à améliorer sa relation avec les Etats-Unis " .

Répondre par la force si besoinD'autres options sont envisageables par le président Barack Obama. Il pourrait ainsi appliquer l'Executive Order, adopté à l'été 2015 : un outil législatif inédit lui permettant de prendre des sanctions financières contre des organisations ou des pirates soupçonnés d'avoir orchestré des cyberattaques. Reste que les sanctions économiques occidentales à l'encontre de Moscou, déjà mises en place en réaction au conflit en Ukraine, n'ont visiblement pas découragé les Russes de s'en prendre aux Etats-Unis.

Une contre-attaque - les Etats-Unis disposent des moyens offensifs les plus aboutis du monde - peut également être organisée. Depuis 2011, la doctrine américaine établit que les Etats-Unis peuvent répondre, par la force si besoin, à toute cyberattaque dirigée contre leurs intérêts. Mais cette théorie se heurte à la perspective de nouvelles attaques contre le système électoral américain. A plus long terme, l'administration américaine n'aurait que peu d'intérêts à provoquer un affrontement incontrôlé dans le cyberespace, compte tenu de la dépendance de son économie et de son administration à Internet.

Cette option serait aussi contraire à l'objectif affiché des Américains en matière de diplomatie - la construction d'un " code de la route " pour le cyberespace -, alors même qu'ils ne donnent pas l'exemple en matière de surveillance et d'espionnage numériques. " Notre but n'est pas de provoquer un cycle d'escalade auquel on a assisté dans le passé pour d'autres types d'armement, mais plutôt de construire des normes afin que tout le monde se comporte de manière responsable ", a déclaré Barack Obama au sujet du piratage du DNC lors de sa conférence de presse au G20 de Hangzhou (Chine), le 5 septembre.

Deux pays aux intérêts contraires sur les réseaux peuvent toujours s'accorder sur quelques règles de principe. L'accord signé en septembre 2015 entre les Etats-Unis et la Chine l'a prouvé. Difficile pourtant d'imaginer que les relations russo-américaines suivent le même chemin. " La Russie n'a pas le même profil que la Chine : elle n'a pas de grandes entreprises aux Etats-Unis, ni d'investissements d'ampleur, le marché américain ne lui est pas crucial pour écouler ses biens et ses services, résume Scott Harold, spécialiste de l'Asie à la Rand Corporation, un think tank établi en Californie. En outre, il y a un important contentieux politique depuis la guerre entre la Russie et la Géorgie - en 2008 - . Vladimir Poutine prospère grâce à l'idée que l'Occident est injuste avec la Russie. C'est un paradoxe, mais les sanctions pourraient le servir politiquement. " Jon Lindsay, professeur de relations internationales à l'université de Toronto, abonde : " La Chine piratait pour son développement économique, mais voulait garder les choses sous contrôle. La Russie, elle, veut voir davantage de friction, de bruit, d'agitation. "

Au-delà de l'exemple russe, selon les experts, les escarmouches dans le cyberespace sont vouées à se multiplier. L'indécision américaine face à la Chine a-t- elle donné un blanc-seing à d'autres Etats pour intervenir dans le cyberespace? Au bout d'une décennie de cyberattaques, faute de sanctions et malgré des progrès avec la Chine, les Etats-Unis ne sont pas parvenus à se montrer assez dissuasifs. " Pékin ou Moscou n'iront pas jusqu'à des attaques destructrices, comme l'extinction du réseau électrique, par exemple , estime Adam Segal . Mais, à un autre niveau, la dissuasion est impossible . Nous allons assister à du harcèlement continuel entre Etats, avec une limite de plus en plus floue entre la guerre et la paix. "

" C'est une nouvelle forme de conflit du XXIe siècle : des attaques bon marché et difficiles à retracer ", avance Pasha Sharikov, chercheur à l'Académie des sciences de Moscou . Est-il encore possible de pacifier le cyber-espace? Oui, estime Matthijs Veenendaal, à condition de " travailler sur des normes internationales - l'approche la plus logique et la plus réaliste ". Même si la normalisation progressive des relations sino-américaines ne s'explique pas seulement par le traité signé en 2015, ce dernier a fait des émules. Le Royaume-Uni et la Chine sont parvenus à un accord similaire. L'Allemagne pourrait, à son tour, s'entendre prochainement avec le plus grand partenaire commercial asiatique de l'Europe.

Depuis plusieurs années, les efforts répétés des Russes en vue de faire adopter une résolution sur la cybersécurité aux Nations unies n'ont pas été couronnés de succès. Les discussions engagées entre Moscou et Washington ont été interrompues par les crises en Ukraine et en Syrie. Une poignée de hauts fonctionnaires se sont malgré tout réunis à Genève auprintempspour reprendre langue. L'accusation portée aujourd'hui par l'administration Obama pourrait bien repousser sine die ces tentatives d'apaisement.

Financial Times
Biden hints at US cyber revenge on Russia
Sunday, 16 October 2016

Washington - US vice-president Joe Biden has suggested the Obama administration may launch a retaliatory cyber strike against Russia in response to what Washington believes to be interference by Moscow in this year's election.
In an interview with NBC's Meet the Press on Sunday morning, Mr Biden said that "we're sending a message" to Russian President Vladimir Putin about the election-related hacking. "He'll know it."

"We have the capacity to do it. It will be at the time of our choosing, and under the circumstances that have the greatest impact," he told NBC.

This week the White House said the US would respond in a "proportional" way to the attempt to interfere in the election and that sanctions and covert action were under consideration.

Mr Biden's interview is the clearest hint that the administration will seek to use its own offensive cyber capabilities to retaliate. Asked if the public would ever find out about the nature of the US response, he said: "Hope not."

"Their capacity to fundamentally alter the election is not what people think," Mr Biden said. "And I tell you what, to the extent that they do we will be proportional in what we do."

The fact Mr Biden is talking so cryptically about US retaliation underlines one of the main difficulties the administration faces in mounting a response. One of the objectives would be to deter Russia or any other country from attempting to use cyber attacks to undermine US elections, yet the deterrent impact of any operation would be limited if it were kept completely secret.

Edward Snowden, the former National Security Agency contractor now exiled in Moscow, poked fun at this contradiction, noting on Twitter: "I get the feeling nobody told Joe Biden what 'covert operation' means."

The vice-president's comments follow the formal claim last week by the US intelligence community that Russia was behind the publication of thousands of election-related emails that have been hugely embarrassing to the campaign of Democratic presidential candidate Hillary Clinton.

"These thefts and disclosures are intended to interfere with the US election process. Such activity is not new to Moscow," said the Department of Homeland Security and Director of National Intelligence on Election Security in a joint statement, noting that "only Russia's senior- most officials could have authorised these activities".

Some former officials have suggested the US could make public financial information and emails collected by US intelligence that would be embarrassing to Russian leaders.

Writing in Foreign Policy magazine, former Nato supreme allied commander James Stavridis said the US should reveal the names of the Russian officials involved in "hacking of the American political system" and should also use cyber attacks to weaken Russian censorship of the internet, creating more room for criticism of Mr Putin and for political opposition.

"As a response to the Russian attacks on the US democratic system, this would be both proportional and distinctive," Mr Stavridis wrote.

Michael Morell, former deputy director of the CIA, said on Friday that Mr Putin was using the selective leaks of emails from Democratic officials to benefit Republican candidate Donald Trump.

"I am 100 per cent confident that he is aware of all this, he has approved it, he is directing it. This is Putin. This is not some bureaucratic part of the Russian government," he said on a call organised by the Clinton campaign.

Mr Morell said it was "a huge, huge deal" for the US intelligence community to publicly blame Russia for the hacking.

Sunday Mirror (UK)
Webcam blackmail terror (Canada)
Sunday, 16 October 2016
Byline: Jilly Beattie

London - The PSNI is investigating 100 webcam blackmail attempts and say cyberstalking is increasing in Northern Ireland.
The crime usually involves people being persuaded to take off their clothes in front of their webcam.

But the blackmailer only tells them they have been recorded after the event and threatens to post the video online or reveal details to people known to the victim unless they pay a fee.

PSNI cyber crime officers are dealing with new webcam blackmail cases "every week".

A spokesman said: "Cyberstalking is becoming a prevalent issue. So far there have been 100 webcam blackmails reported."

Parents were warned a Canadian pervert pretended to be a teenage girl to target thousands of boys.

The money demanded is usually a substantial amount and increases with the level of intimacy revealed by the victim, many of whom have been enticed into performing intimate acts.

A spokesman for Get Safe Online said there is no guarantee once the blackmail demand is met there will not be further demands, or that the criminal will not post the video anyway.

He added: "The consequences can range from embarrassment to humiliation and in extreme cases have resulted in self-harm of even victims taking their own lives.

"Males and females of any age, anywhere, can become victims.

"People are asked to take their clothes off as a dare 'nomination' with friends, only to be blackmailed either by those known to them or if the video or stills fall into the wrong hands."

Straits Times
New SMS public alert system launched to warn the public of nearby emergencies
Saturday, 15 October 2016
Byline: Jalelah Abu Baker

Singapore - Members of public near an emergency like a terror attack will get a text message informing them of what is happening, with a new public alert system by the Government.
Introducing the system on Saturday (Oct 15) at an emergency preparedness event, Deputy Prime Minister Teo Chee Hean said that that the new system will reach out to a wider audience, who may not have access to alerts through the recently launched SGSecure mobile app.

"Some might not have turned on the location function to receive the location-based alerts. Some of our seniors may not be familiar with apps, or have older 2G phones," explained Mr Teo, who is also Coordinating Minister for National Security.

The new SMS-based public alert system is an additional channel to reach out to the public, help warn residents about danger, and give them appropriate advice on how they can and should respond, he added.

The Ministry of Home Affairs said that the alerts will be sent out for related incidents including bomb blasts and gunman attacks, major public order incidents, and major fires and civil disasters.

The system has been on trial since August, and was used for the recent fires at the CK Building and Jurong West Street 41.

New York Times

Biden Hints at U.S. Response to Russia for Cyberattacks Related to Election
Sunday, 16 October 2016
Byline: David E. Sanger

Washington - Since the Obama administration formally accused Russia about a week ago of trying to interfere in the election, there has been intense speculation about whether President Obama has ordered the National Security Agency to conduct a retaliatory cyberstrike.
The strongest hint so far has come from Vice President Joseph R. Biden Jr., who either revealed American plans for a strike or engaged in one of the better bits of psychological warfare in recent times.

Taping an interview for NBC's "Meet the Press," Mr. Biden was asked whether the United States was preparing to send a message to the Russian president, Vladimir V. Putin. Days before, the American intelligence agencies and the Department of Homeland Security declared that the Russian leadership was responsible for attacks on the Democratic National Committee and the leaking of stolen emails.

"We're sending a message," Mr. Biden told Chuck Todd, the show's host. "We have the capacity to do it."

"He'll know it," Mr. Biden added. "And it will be at the time of our choosing. And under the circumstances that have the greatest impact."

Later, after Mr. Biden said he was not concerned that Russia could "fundamentally alter the election," Mr. Todd asked whether the American public would know if the message to Mr. Putin had been sent.

"Hope not," Mr. Biden responded.

His warning seems to suggest that Mr. Obama is prepared to order -- or has already ordered -- some kind of covert action after the stolen emails were published online. That would require what is known in the intelligence agencies as a finding -- a presidential determination authorizing covert action.

Such a finding would allow the United States to make use of its newly developed arsenal of cyberweapons, which are under the control of the military's Cyber Command, the N.S.A. and, in some circumstances, the C.I.A.

Mr. Biden's statement does not exclude the possibility of a response outside the realm of cyberspace. But most of the other options under discussion in the White House involve actions that would be public, such as economic sanctions under a 2015 presidential order on responding to cyberattacks. Such sanctions have never been invoked, but are well suited to cases like the presumed effort to influence the election.

Some experts, however, say they may be insufficient. James G. Stavridis, the former supreme allied commander of NATO, wrote in Foreign Policy last week that the first step could be making America's evidence against Russia public.

"Revealing the names of the officials who authorized the cyberattacks against the United States would put Moscow in an extremely uncomfortable position," wrote Mr. Stavridis, a former admiral who is now dean of the Fletcher School of Law and Diplomacy at Tufts University. "Ideally, the United States could reveal emails or conversations between Russian officials that demonstrated their intent to undermine the U.S. electoral process."

But that would run counter to Mr. Biden's "hope not" statement. Mr. Stavridis and others have advocated other steps, including knocking holes in the Kremlin's wall of censorship so that opponents of Putin could begin to conspire with one another.

"As a response to the Russian attacks on the U.S. democratic system, this would be both proportional and distinctive," Mr. Stavridis wrote. It might also be deniable -- a key to any covert action approved by the president.

Many others have advocated using cybertechniques to expose Mr. Putin's links to Russia's oligarchs and reveal his financial holdings overseas, which are believed to be vast. But such steps would risk escalation, and advisers have warned Mr. Obama that the United States is more vulnerable than most nations.

Mr. Putin initially denied any Russian involvement in the attacks. But in an interview several days ago, he said the important thing was not how emails from Hillary Clinton's campaign had been hacked, but what they said. Sergey V. Lavrov, the Russian foreign minister, went further. "We did not deny this," he said of the hacking. But he added that the United States had offered no proof.

A crucial question being debated in the White House is whether warnings like Mr. Biden's will be enough to make Russia, or others, pull back in their hacking. The calculus behind the decision to formally accuse Russia was that the mere publication of the conclusion could temper the activity.

If so, it may not have worked. WikiLeaks in the past few days has published thousands of emails stolen from the Gmail account of John D. Podesta, the chairman of the Clinton campaign. While Mr. Podesta has blamed Russia for the attack, intelligence agencies say they have not formally reached that conclusion.

There are only two known cases in which Mr. Obama has authorized an offensive cyberaction. One was the operation against Iran's nuclear program, code-named Olympic Games. That operation was not detected by the Iranians for years, until an accidental release of the computer code made it obvious that its centrifuges were exploding because of a cyberattack.

The other case has been action against the Islamic State, mostly to interfere with its communications or alter data in its systems. Those attacks were publicly announced by Defense Secretary Ashton B. Carter and others, though no details were offered.

The announcement seemed intended in part to cause Islamic State insurgents to question whether their internal communications were genuine.

Sunday Times (UK)
Chinese link as smart meters spook GCHQ
Sunday, 16 October 2016
Byline: Jon Ungoed-Thomas

London - Chinese electronic companies are manufacturing smart meters to install in millions of Britain's homes despite warnings by the intelligence agency GCHQ that the technology poses a potential threat to national security.
Two of China's biggest electronics companies -- one controlled by the Beijing government -- are providing some of the meters and software for the £11bn programme to install the technology in almost every home in the UK by 2020. One has already signed a deal with one of the "big six" energy companies and the other has been on an official list for trials.

The vetting of the Chinese manufacturers is set to be among the first tasks of the National Cyber Security Centre (NCSC), which opened in London earlier this month.

Nigel Inkster, a former director of operations and intelligence at MI6, said it was important the role of any Chinese firm was subject to a proper risk assessment.

"A Chinese corporation is always going to have to do what the state tells it when the crunch comes, although these corporations really do want to be proper international corporations and operate on this basis," he said.

Experts have expressed concern that the meters -- which communicate wirelessly with energy companies -- feature a switch that can be used to remotely turn off power, potentially blacking out homes and risking dangerous electricity surges at power stations. Meters made by Holley Metering UK, whose parent company is Chinese, and Kaifa Technology UK, which is controlled by the state-owned China Electronics Corporation, are being tested by one of the main government contractors for the UK project.

Last week Holley Metering, owned by a firm which is one of the biggest meter suppliers to China's state electric utility, said it had signed a deal with one of the big six energy companies and expected to start installing its devices in British homes early next year.

The smart meter programme was launched by Ed Miliband, the former Labour leader, in May 2009 when he was energy secretary. It was subsequently championed by Andrea Leadsom, now the environment secretary, when she was energy minister.

Data Communications Company, which has the government licence to manage the communications network for the project, is testing nine gas and electricity meters to ensure all systems are fully integrated. Five of the nine meters are manufactured by Holley and Kaifa.

Holley Metering was set up in Britain in 2014. Steve Roberts, one of its first senior executives, was recruited from the Department of Energy and Climate Change in March 2015, where he had been head of market intelligence.

Tony Hart, the managing director of Holley Metering, said he was aware of the sensitivities about involving Chinese businesses in critical national infrastructure, but that Holley was an independent company. He would not disclose which of the big energy companies Holley had signed its contract with.

Kaifa Technology UK is based in Milton Keynes in Buckinghamshire.It did not respond to a request for comment.

Nick Hunn, a director at Wifore Consulting who gave evidence to a parliamentary inquiry on smart metering, said a switch in the meters could, in theory, remotely shut down power to a home.

"If anyone was able to hack the system, it would not just have the effect of blacking out a million houses, it would blow out a part of the grid," he said.

It was reported earlier this year that GCHQ had intervened in the project to ensure the encryption keys for the meters could not be broken. All key products for the meter rollout will undergo product assurance by the NCSC.

The Department for Business, Energy and Industrial Strategy said the smart system was secure and it had been designed by cyber-security experts to prevent the possibility of hacking.

Security officials say the Chinese meters will not be subject to any more stringent testing, but would need to meet robust security standards to protect the national grid.

The NCSC said: "All components and software used in the UK Smart Meter programme must meet a stringent set of security characteristics and standards which we publish on our website. We're confident the Smart Meters System strikes the best balance between security and business needs."

Hackread Blog
Man Accused of Terrorism Over Encrypting his Blog Site
Saturday, 15 October 2016
Byline: Staff Writer

London - A 33 year old male in London has been charged with six terrorism counts under the terrorism act 2006 by the Metropolian Police. The man, named Samata Ullah, appeared in a appeared in a court in London the previous.
Ullah has been charged under the controversial Section 5 power in which the development of an "encrypted version" of personal blog site can be used against the suspect while fixing terrorism counts. Unsurprisingly, using this provision, the police force has charged Ullah for six counts of terrorism one of which was linked to the use of encryption and researching.

In a press release, the police department stated that Ullah has been charged with one count of aiding a person who was preparing a terrorist act by providing instructions about how to use encryption. The second charge is about using encrypted version of his own blog site and another is related to preparation of engaging in an act of terrorism.

London police maintain that Ullah was preparing for an act of terrorism himself through "researching an encryption program, developing an encrypted version of his blog site and publishing the instructions around the use of the program on his blog site."

The Section 5 statute can "criminalize acts that, on their own, would be completely legal -- if prosecutors can show that the end purpose of those acts might be terrorism," stated a human rights advocate Tayab Ali back in 2014.

Ali added that: "Often intention is proven using things like internet search history. It is often described as 'thought crime,' and it doesn't apply in any other aspect of criminal law."

It must be noted that nowadays, adding encryption to blog sites or websites is not a big deal at all because many websites adopt this strategy to offer their visitors enhanced privacy, better security, and full relaxation while they surf. That's not all, even Google supports encryption on websites and favors HTTPS sites in search results.

New Zealand Herald
Foreign spies hack NZ phones, laptops
Saturday, 15 October 2016
Byline: Matt Nippert

Wellington - Exclusive Agents accessed deleted files and installed spy software on trade officials' devices after breaking into hotel room

New Zealand government officials travelling abroad had their mobile phones and laptops containing classified information hacked by foreign agents after their hotel room safe was broken into, government cyber security officials have revealed.

According to an account of the incident prepared by the Government that does not name either the department involved nor the foreign power believed responsible, the incident occurred when two trade negotiators attended an overseas conference.

Precautionary efforts by the pair to delete sensitive materials from their devices prior to departure proved ineffective in protecting classified information.

A cloned copy of hard drives allowed foreign agents to "recover not only deleted protectively marked documents, but also intellectual property and sensitive information pertaining to trade negotiations", according to the account.

Following their return to New Zealand, malware designed to log all electronic activity was also found to have been installed on the devices.

Paul Ash, director of the national cyber policy office at the Department of Prime Minister and Cabinet, said the incident showed New Zealand's geographic isolation was no firewall.

"Cyber security's a complex area, and it's just become more complex ... We are seeing an upward trend in cyber security incidents," Ash said.

The National Cyber Security Centre - logging attacks against sensitive commercial and government organisations - logged 316 "incidents" in the year to April 2016, up 66 per cent from the year prior.

Details of the hotel-room break-in are contained in a case study prepared for a New Zealand Security Intelligence Service-run initiative to improve government information security.

A spokesman for the New Zealand Intelligence Community described the account as "factually accurate" but stripped of information that could identify actors involved.

Digital security specialist Adam Boileau said the hotel-room incident as described wasn't surprising - he had colleagues working in Australia who said such government security breaches happened "pretty often" - but such subterfuge was only rarely made public.

"When you talk to people who work in government, this is pretty common. It happens all the time, especially with trade-related stuff. Especially trade-related stuff in Southeast Asia," he said.

The revelations follow this week's claims by the White House that Russia was behind the hacking and disseminating of emails belonging to presidential nominee Hillary Clinton.

British ministers were also this week banned from wearing Apple Watches to Cabinet meetings following concerns the devices - capable of recording audio - posed a security risk as they were vulnerable to hacking by foreign powers.

Ash said events were moving swiftly and his office was still grappling with implications of the DNC hack where information gathered is claimed have been used for propaganda - rather than intelligence or financial - ends.

"This is reasonably new for cyber policy ... It's the application of older techniques to something new. It's taken people by surprise because of its audacity," he said.

Boileau said, that aside from the loss of sensitive information, there were also increasing indications that hacking attacks could have serious financial and physical effects.

He cited a little-reported attack on Saudi Arabian company Aramco - responsible for a tenth of the world's oil production - that saw 35,000 desktop computers junked, and a sustained Christmas 2015 cyber attack on Ukraine's power grid left 230,000 people in the dark.

While New Zealand has not publicly acknowledged any of its own offensive capability in this arena - the only member of the Five Eyes alliance not to do so - the Herald last year reported how the Government Communications and Security Bureau had hacked the mobile phones of a foreign government.

Relying on the documents leaked by National Security Agency whistleblower Edward Snowden, the GCSB was, in 2013, said to have used "Warriorpride" malware capable of targeting Android or Apple mobile phones to transfer data from an "Asean target" to a NSA server.

Washington Post
Trump refusal to accept government assessments on Russian hacks dismays former official
Saturday, 15 October 2016
Byline: Tom Hamburger

Washington - Former senior U.S. national security officials are dismayed at Republican presidential candidate Donald Trump's repeated refusal to accept the judgment of intelligence professionals that Russia stole files from the Democratic National Committee computers in an effort to influence the U.S. election.
The former officials, who have served presidents in both parties, say they were bewildered when Trump cast doubt on Russia's role after receiving a classified briefing on the subject and again after an

unusually blunt statement from U.S. agencies saying they were "confident" that Moscow had orchestrated the attacks.

"It defies logic," retired Gen. Michael V. Hayden, former director of the CIA and the National Security Agency, said of Trump's pronouncements.

Trump has assured supporters that, if elected, he would surround himself with experts on defense and foreign affairs, where he has little experience. But when it comes to Russia, he has made it clear that he is not listening to intelligence officials, the former officials said.

"He seems to ignore their advice," Hayden said. "Why would you assume this would change when he is in office?"

The Trump campaign did not respond to requests for comment.

Several former intelligence officials interviewed this week believe that Trump is either willfully disputing intelligence assessments, has a blind spot on Russia, or perhaps doesn't understand the nonpartisan traditions and approach of intelligence professionals.

In the first debate, after intelligence and congressional officials were quoted saying that Russia almost certainly broke into the DNC computers, Trump said: "I don't think anybody knows it was Russia that broke into the DNC. I mean, it could be Russia, but it could also be China. It could also be lots of other people. It also could be somebody sitting on their bed that weighs 400 pounds, okay?"

During the second presidential debate, Trump ignored what a U.S. government official said the candidate learned in a private intelligence briefing: that government officials were certain Russia hacked the DNC. That conclusion was followed by a public and unequivocal announcement by the Office of the Director of National Intelligence and the Department of Homeland Security that Russia was to blame.

"Maybe there is no hacking," Trump said during that debate.

"I don't recall a previous candidate saying they didn't believe" the information from an intelligence briefing, said John Rizzo, a former CIA lawyer who served under seven presidents and became the agency's acting general counsel. "These are career people. They aren't administration officials. What does that do to their morale and credibility?"

Former acting CIA director John McLaughlin said all previous candidates took the briefings to heart.

"In my experience, candidates have taken into account the information they have received and modulated their comments," he said. Trump, on the other hand, "is playing politics. He's trying to diminish the impression people have that [a Russian hack of the DNC] somehow helps his cause."

On Thursday, the ranking Democrat on the Senate Intelligence Committee, Sen. Dianne Feinstein (Calif.), said information she received has led her to conclude that Russia is attempting "to fix this election." She called on Trump and elected officials from both parties "to vocally and forcefully reject these efforts."

Trump has consistently adopted positions likely to find favor with the Kremlin. He has, for instance, criticized NATO allies for not paying their fair share and defended Russian President Vladi-mir Putin's human rights record.

"It's remarkable that he's refused to say an unkind syllable about Vladimir Putin," Hayden said. "He contorts himself not to criticize Putin."

Trump's running mate, Indiana Gov. Mike Pence, said in the vice-presidential debate last week that the United States should "use military force" against the Syrian leader Bashar al-Assad.

Trump disagreed. Rather than challenge Assad and his Russian ally, Trump said in the second debate, the United States should be working with them against the Islamic State. "Assad is killing ISIS. Russia is killing ISIS. Iran is killing ISIS," he said, using an acronym for the Islamic State. Russia and Syria have mostly been targeting opposition groups as well as civilians trapped in Aleppo -- not the Islamic State.

"That's the Syrian, Russia, Iranian narrative," Hayden said of Trump's assertion.

Fox News
CIA reportedly preparing major cyber assault against Russia in wake of hack attacks
Saturday, 15 October 2016

Washington - The Central Intelligence Agency reportedly is preparing a major cyber attack against Russia in response to the theft of records from the Democratic National Committee and its affiliates, allegedly by Moscow- backed hackers.
Vice President Joe Biden told NBC News, which first reported that the Obama administration was considering retaliatory measures, that the U.S. would be "sending a message" to Russian President Vladimir Putin. Biden added that any cyber action would come "at the time of our choosing, and under the circumstances that will have the greatest impact."

NBC also reported that intelligence officials have been asked to present the White House with ideas for a "clandestine" cyber operation designed to "embarrass" the Kremlin.

"We've always hesitated to use a lot of stuff we've had, but that's a political decision," a former CIA officer told NBC. "If someone has decided, `We've had enough of the Russians,' there is a lot we can do."

Last week, the U.S. formally blamed the Russian government for cyberattacks on the Democratic National Committee and the Democratic Congressional Campaign Committee. A statement from the

Department of Homeland Security and the Office of the Director of National Intelligence said that recent disclosures of alleged hacked emails on websites like DCLeaks.com and WikiLeaks, and by the Guccifer 2.0 online persona, are consistent with the methods and motivations of efforts directed by Russia.

"We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities," the statement said.

Earlier this week Putin told an investor forum in Moscow that it did not matter who was behind the hacks, but it was "what's inside the information that matters."

Democratic presidential nominee Hillary Clinton has claimed that the theft of the records proves that Russian intelligence is attempting to help her opponent, Republican Donald Trump, defeat her in next month's election.

"Hysteria started over the [allegation] that this is in the interests of Russia," Putin added, according to the Interfax news agency. "But nothing in it is in the interests of Russia, while the hysteria is merely caused by the fact that somebody needs to divert the attention of the American people from the essence of what was exposed by the hackers."

The Intercept
Hillary Clinton's Encryption Proposal Was "Impossible," Said Top Adviser
Saturday, 15 October 2016
Byline: Alex Emmons

Washington - Hillary Clinton's advisers recognized that her policy position on encryption was problematic, with one writing that it was tantamount to insisting that there was "'some way' to do the impossible."
Instead, according to campaign emails released by Wikileaks, they suggested that the campaign signal its willingness to use "malware" or "super code breaking by the NSA" to get around encryption.

In the wake of the Paris attacks in November, Clinton called for "Silicon Valley not to view government as its adversary," and called for "our best minds in the private sector to work with our best minds in the public sector to develop solutions that will both keep us safe and protect our privacy."

When asked during a debate in December whether she would legally compel companies to build a backdoor into their products to give law enforcement access to unencrypted communications, Clinton responded "I would not want to go to that point."

But she then called for a "Manhattan-like project" to develop secure communication while allowing the government to read messages.

Cryptography experts overwhelmingly agree that backdoors inevitably undermine the security of strong encryption, making the two essentially incompatible.

The day after the debate, Sara Solow, domestic policy adviser for the Clinton campaign, called Clinton's position "impossible" in an email with Teddy Goff, the campaign's chief digital strategist. "[S]he's certainly NOT calling for the backdoor now," Solow said, "although she does then appear to believe there is 'some way' to do the impossible."

Goff had written that he thought Clinton's reply was a "solid B/B+," and suggested that she "thread the needle" and "quickly pivot from encryption to the broader issue of working with tech companies to detect and stop these people." Goff also said that the Manhattan project analogy was something which Clinton should "truly, truly should not make ever again -- can we work on pressing that point somehow?"

Solow's suggestion was that the campaign quietly signal to Silicon Valley -- a major source of donations for the campaign -- that Clinton would support government hacking to circumvent encryption.

"Couldn't we tell tech [companies] off the record that she had in mind the malware/key strokes idea (insert malware into a device that you know is a target, to capture keystrokes before they are encrypted). Or that she had in mind really super code breaking by the NSA. But not the backdoor per se?"

The FBI has in fact used targeted hacking to get around encryption tools, quietly and effectively. In 2007, for example, FBI agents caught a teenager who was sending online bomb threats to a high school in Lacey, Washington, by sending him a link that installed malware on his computer.

The Clinton campaign had previously struggled to answer inquiries about the candidate's position on encryption. "This is going to be a challenge," Clinton foreign policy adviser Jake Sullivan said in a November exchange about how to respond to a press inquiry. "I think we should give a comment on the anonymizing tools and punt on backdoors."

During Clinton's tenure as secretary of state, the State Department aggressively funded the development of encryption and anonymous web browsing tools.

In Solow's email, she asked whether there was any actual evidence of terrorists using the technologies the State Department funded. "Is there evidence," asked Solow, "that bad guys -- not just dissidents but terrorists or whatever -- have also benefitted from the technologies supported by the [State Department's] Internet freedom agenda?"

In response to terror attacks, Clinton has repeatedly called for an "intelligence surge," but has provided little clarification about what she means.

CBC.CA
U of S security specialist gives tips on how to stay safe online
Saturday, 15 October 2016
Byline: Courtney Markewich

Saskatoon - There are a few simple things everyone can keep in mind to make sure they're secure online.
October is National Cyber Awareness Month and even in today's digital world, Lawrence Dobranski -- director of ICT security at the University of Saskatchewan -- said there are some things people do that make him shake his head.

The number one thing is how some people reuse passwords.

"They have a group of favourite passwords that they reuse at all the websites they go to. So if one of those sites gets compromised, the malicious actor will have your password and your email address," Dobranski said.

A few years ago, Dobranski said, an experiment was done at the U of S where they were able to crack about 80,000 passwords in 48 hours.

Dobranski pointed out that many social media sites are now helping people secure their accounts by adding a second factor. For example, you can activate it on Facebook and a pin number will be texted to your cellphone to verify you're the one logging into the account.

Another thing people should do, Dobranski said, is patch their computer. That means making sure your computer has the latest-available update as it will keep the system safer.

"We have to make sure we're accepting them and keeping the machine patched."

Lastly, Dobranski pointed out that people don't take the time to secure their wifi before connecting devices.

"Is it actually a trustworthy wifi connection? Or is it a malicious actor that wants to monitor our connection?"

Dobranski said tools are available to make sure you're connecting to a virtual private network.

Taking such steps, Dobranski explained, are important to keep your identity safe.

Jakarta Post
Indonesia, Australia to discuss maritime, cybersecurity in Bali
Monday, 17 October 2016
Byline: Liza Yosephine

Jakarta - Indonesia, Australia to discuss maritime, cybersecurity in Bali On guard - Indonesian Navy Academy (AAL) cadets parade on the deck of warship KRI Banda Aceh (BAC)-593 during an event at Eastern Fleet (Koarmatim) Port in Surabaya, East Java, on Oct.11.
Top ministers from Australia and Indonesia are scheduled to gather in Bali on Oct.28 to discuss the strengthening of cooperation on strategic security issues between the two countries, officials have said.

Foreign Ministry spokesperson Arrmanatha Nasir said foreign and defense ministers from Indonesia and Australia were ready to attend the fourth meeting of the pair ministers, which was initiated in 2010.

"Some of the issues to be discussed include strategic security issues, which have become prime concerns of both countries, and on how they can contribute to the stability and peace of the region," Arrmanatha said during a press briefing at the ministry in Jakarta on Friday.

The ministry's East Asia and Pacific director Edi Yusup said the meeting was expected to expand cooperation that had been established in previous talks, including on counterterrorism and deradicalization.

He further said the meeting would discuss maritime safety and security issues, especially those related to disputed territories in the South China Sea, and Sulu Sea security, which had been rife with kidnappings of Indonesian sailors in recent years. Australia wanted to know how Indonesia had addressed a string of hostage-taking situations, he went on. "There is also a possibility for the two countries to launch cooperation on cybersecurity during the event," Edi said.

The Australian
Security fears over Chinese watch a sign of the times
Tuesday, 18 October 2016
Byline: Rosie Lewis

Sydney -A Bluetooth watch given to Infrastructure Minister Paul Fletcher by Chinese company Huawei has come under heavy scrutiny after Labor suggested it could pose a security risk, but the piece has never been worn by its owner.
Labor Senate leader Penny Wong took interest in the watch after it was declared on Mr Fletcher's updated register of members' interests alongside a Chinese teapot from the same company.

Senator Wong used Senate estimates yesterday to ask the Department of Parliamentary Services if it had "any concerns" about a device provided by Huawei being connected to its computer network, noting there were a "range of security concerns" on the public record about the telecoms giant.

The former Labor government banned Huawei from participating in the rollout of the National Broadband Network on the basis of security advice from the Australian Security Intelligence Organisation and the Defence Intelligence Organisation.

The Abbott government kept the ban in place.

DPS said intelligence agencies recommended hardware such as USBs received from external sources should not be connected to the parliamentary networks.

But the department assured Senator Wong there was malware detection software that initiated anti-virus checks upon connection.

However, the line of questions and answers proved to be largely irrelevant when Mr Fletcher's office told The Australian the watch had never been used."Mr Fletcher does not wear or use the watch he received from Huawei, on the parliamentary network or anywhere else," the minister's spokesman said, though he did not reveal where the watch was kept.

Australian
Milk-bottle space odyssey gives spy force a boost (Canada)
Tuesday, 18 October 2016
Byline: Brendan Nicholson

Sydney - Satellites designed and built in Australia -- each about the size of a two-litre milk bottle -- will be used to improve the performance of the revolutionary JORN over-horizon radar network and help gather intelligence for the nation and its allies.

The "cubesats", each weighing less than 5kg, will also help prevent spacecraft colliding with each other or with space debris.

The first two satellites will be launched early next year, in missions tagged Buccaneer and Biarri, with more likely.

The new "mini constellation" of satellites will also form part of the Five Eyes intelligence-gathering and sharing network involving Australia, the US, Canada and New Zealand and Britain.

The satellites were designed and built by scientists from the Defence Science and Technology Group and the University of NSW.

Defence Minister Marise Payne said the research missions would help reinvigorate Australia's space engineering capability and met the promise in the -defence white paper for Australia to develop a space capability.

Senator Payne said the global space sector was being transformed. "Traditional actors such as wealthy nations and major international aerospace primes and traditional approaches, such as large and expensive satellites are now able to do some things but they're no longer the be-all and end-all of space capability," she said.

Advances in small, low-cost space platforms provided a unique opportunity to support the Australian Defence Force and rejuvenate local space research, Senator Payne said.

"It's a very happy day today -because we're launching a really important partnership, I think, for the future of space in Australia." She said although Australia had a long history of space -activity, it had been a long time since there had been such a program from Australian players.

Senator Payne said such a program could encourage Australian scientists to return. "I also wanted to reinforce ... the importance of the reverse brain drain, bringing some of our experts back from overseas," she said.

The Jindalee Operational Radar Network watches Australia's northern approaches and an extraordinary 37,000 square nautical miles of ocean.

While normal radars operate by line of sight and are limited in range by the Earth's curvature, JORN bounces its signal off the ionosphere so it deflects down onto its target. Most details about JORN are secret but it is believed to be able to see activity of crucial strategic importance, such as missile launches, far into Asia.

The ionosphere is part of the upper atmosphere starting about 60km above the Earth's surface.

Complex mathematical calculations are needed to find the most effective wavelengths for the system and to work with variations in the upper atmosphere.Crucial to the effectiveness of a radar or sensing system is signal processing, or the ability to constantly pull out signals of importance and understand what they are telling the operator.

Agence France-Presse
Le Canada "très inquiet" des menaces russes de piratage informatique
Tuesday, 18 October 2016

Le Canada est "très inquiet" d'être la prochaine cible des attaques informatiques de la Russie, a indiqué lundi son ministre des Affaires étrangères Stéphane Dion, qualifiant de "très difficile" la relation qu'entretiennent Ottawa et Moscou.
Le chef de la diplomatie canadienne était interrogé sur le risque de voir le Canada devenir la prochaine cible des pirates russes, après que Washington ait accusé la Russie d'avoir piraté des organisations politiques et des systèmes électoraux aux Etats-Unis.

Se disant "très inquiet" par une telle éventualité, le chef de la diplomatie a noté, en marge d'une intervention devant le Conseil des relations internationales de Montréal (CORIM), que ce danger soulignait "la nécessité d'avoir un cyberespace libre et sûr".

Son homologue à la Sécurité publique, Ralph Goodale, a d'ailleurs déclaré à Ottawa lundi que le gouvernement canadien a entrepris depuis quelque temps une révision générale des infrastructures internet du pays, en particulier des systèmes sensibles tels que ceux des banques, car "il y a eu des incidents par le passé au Canada durant lesquels des systèmes ont été corrompus".

Les relations avec la Russie sont "très difficiles pour plusieurs raisons, mais en particulier à cause de ce qui se passe en ce moment à Alep et en Ukraine", a fait valoir Stéphane Dion.

"Mais c'est une raison de plus de mener une politique de dissuasion convaincante, comme ce que nous faisons en Lettonie avec l'Otan", où Ottawa va déployer 455 soldats à partir de mai 2017 dans le cadre du renforcement des capacités de l'Alliance atlantique sur son flanc est, a relevé M. Dion.

Toutefois, a souligné le chef de la diplomatie canadienne, "rompre le dialogue (avec la Russie, NDLR) serait une erreur, ce n'est pas ce que le Canada fait".

Sydney Morning Herald
Cabinet has 'never' disclosed sensitive material on WhatsApp
Tuesday, 18 October 2016
Byline: James Massola

Sydney -Attorney-General George Brandis says confidential material has "never, ever" been communicated by cabinet ministers on WhatsApp - but he won't be releasing the proof.
And testy officials from the Department of Prime Minister and Cabinet dismissed security experts' concerns about the use of WhatsApp, insisting that the security clearances given to ministers and their staff were sufficient to protect sensitive information.

Those officials said that to the best of their knowledge, Defence's cyber security agency, the Australian Signals Directorate, had not approved the use of WhatsApp for classified or sensitive communications.

Fairfax Media reported last week that cabinet ministers, MPs, ministerial chiefs of staff and media advisers are using WhatsApp to hold confidential discussions about government business. That prompted Labor's legal affairs spokesman, Mark Dreyfus, to warn the arrangement was a "national security risk".

But Senator Brandis told a Senate hearing yesterday that using the app did not pose a security threat.

"I can assure you, having communicated with the Prime Minister and other cabinet colleagues on WhatsApp, there has never been an occasion, ever, in which the material on WhatsApp has been other than extremely routine, of an extremely routine nature," he said.

"Never, ever, ever has there been an occasion when a sensitive or national security matter has been reduced to that form, for obvious reasons."

At that point, Labor senator Penny Wong pounced, asking Senator Brandis about the existence of a cabinet WhatsApp group.

"That's a definitional matter."

"What do you talk about?"

"Nothing of public sensitivity" Senator Brandis replied.

"If that's the case, Are you prepared to give us a copy of your cabinet WhatsApp chat? You can export it is as a text file."

"No."

"So it's entirely unremarkable but you don't want it exposed to the public?"

"Well, Senator, it's entirely unremarkable."

Malcolm Turnbull's cyber security adviser, Alastair MacGibbon, told the Senate hearing that he regularly communicated on WhatsApp with the Prime Minister.

Mr MacGibbon said WhatsApp could, in theory, be more secure than a regular text message but was potentially less secure than an iMessage sent from an Apple phone. "The use of messaging apps can increase privacy and security based on their encryption, versus a telephone call or an email or an SMS," he said.

To ensure adequate security, "whether it's WhatsApp or other applications, we have to rely on people following instructions and the guidance they are given."

Departmental deputy secretary Allan McKinnon appeared to confirm that no inquiries had been made about the security of WhatsApp.

ABC (Australia)
Immigration Department confirms IBM will miss IT merger deadline amid security concerns
Tuesday, 18 October 2016
Byline: Matthew Doran

Canberra - The Department of Immigration and Border Protection (DIBP) has tried to downplay reports its rollout of a new $500 million computer system could lead to security breaches, and claimed its deadline for completion was always up for review.
Last month, the ABC reported serious concerns had been raised about .

Before Customs and Immigration merged in 2015, two companies had been delivering IT services -- IBM for Customs; and CSC, another US information technology giant, for Immigration.

The ABC had been told by those familiar with the project that IBM was increasingly unlikely to hit an October 31 completion deadline, and any system failure could compromise national security checks, including red- flagging terror suspects attempting to enter or leave the country.

Three weeks ago, the department had issued a statement to the ABC that stated the "schedule remains under active review".

"This is common to all major system changes in which the protection of operational capability and security protections remains the overarching priority," the statement said.

Deadline 'was never going to be exact'

Now, the department's Deputy Secretary Maria Fernandez has told a Senate committee the revised deadline for completion was early December, but said the revision was not as a result of the ABC report.

"That report was not accurate," the department's Maria Fernandez told a Senate committee.

"It is a complex transition, it takes critical border systems from CSC mainframe's onto IBM, it will take almost a year to undertake the migration.

"It is 17 years of data and very complex systems, and so it is a schedule that we review constantly, and it was never going to be exact."

CSC's contract had since been extended through until January 2017.

DIBP Secretary Mike Pezzullo said nothing would be done to jeopardise the security of the computer system, and its role in managing Australia's border.

"One of the factors [the team managing the rollout] have regard to is that there's no breach of the integrity of our border systems," Mr Pezzullo said.

"If there were to be by premature migration, switching over of data from one mainframe to another, if there were to be a risk the Commissioner [Roman Quaedvlieg] and I would have a very, very, very low threshold of risk appetite of any potential breach of our border."

Ottawa Citizen Online
The mystery of the listening devices at DND's Nortel Campus
Tuesday, 18 October 2016
Byline: David Pugliese

My colleague Jim Bagnall and I recently wrote a feature on the move by the Department of National Defence to the former Nortel campus in west end Ottawa. More than 8,000 military and civilian staff will make the move.
One of the issues that emerged when we were researching and writing the article had to do with the mystery of listening/spy devices that were planted at the Nortel Campus.

So what happened? Were listening devices found at the Nortel Campus or not?

The Department of National Defence keeps changing its story on that issue.

In 2013 the Citizen reported that workers preparing the former Nortel complex as the new home for the DND had discovered electronic eavesdropping devices. It shouldn't have come as a big surprise. The year before it had been revealed that Nortel was the target of industrial espionage for almost a decade, with the main culprits thought to be based in China. An internal security study by Nortel suggested that

hackers had also been able to download research and development studies and business plans as far back as 2000. The hackers also placed spyware into some employee computers.

Michel Juneau-Katsuya, a former senior officer with the Canadian Security Intelligence Service, said the spy agency also determined that Nortel had been targeted. "We knew it was well penetrated," he told the Citizen at the time. "When I was the Chief of Asia-Pacific we warned Nortel."

But after the Citizen article was published, Julie Di Mambro, spokeswoman for then Conservative Defence Minister Rob Nicholson, noted in a statement that, "security officials have assured us that they have not discovered any bugs or listening devices."

Government documents, however, obtained by the Citizen through the Access to Information law, showed that the year before concerns had already been raised about security at the former Nortel campus. Although the proposed relocation was already well publicized, then Defence Minister Peter MacKay had been warned not to make any announcement that the DND was moving into the complex before it could be properly secured. Security officials were concerned that someone might be able to slip into the site and plant spy devices before the move. "This not only raises the level of difficulty of verifying appropriate security safeguards in the future, it will probably dramatically increase security costs and cause delays to reach full operational capability," MacKay was told.

In December 2013 Public Works and the DND held a news briefing to outline the plans for the move to the former Nortel site. Again, a DND official dismissed concerns that listening devices could be hidden in the sprawling complex, noting that none had ever been found. But his claim turned out to be misleading. The official -at the same news conference - later admitted that only "limited" security sweeps had been done at the campus and he only meant that no spy devices had been found by DND officials. He couldn't speak about what might have been found by other security agencies.

Fast forward to August 2016. In an interview with the Citizen, Vice Chief of the Defence Staff, Vice Admiral Mark Norman refused to discuss the spy issue in detail. He said his organization was satisfied the site was ready to be occupied, despite "any legacy bits and pieces, whether they were intended to be there or not." The suggestion was that older spy devices might indeed have been discovered.

A short time later Norman provided more information in an interview with the Globe and Mail about the "legacy" devices that were found. "The whole facility was swept when we went through in preparation for our moving in," Norman explained. "Anything that was there was legacy to what I would characterize as industrial activity and we are completely satisfied now that this is a site we are able to move into and it meets all of our security requirements. I am assured anything that was there is no longer there. ... It was all legacy, old-school stuff associated with the previous occupant."

DND officials privately said to the Citizen that was a confirmation that spy devices that were found were older and not functioning.

Five days later in another statement to the Citizen - and contrary to what Norman had said earlier - the DND was once again claiming that no bugs, surveillance equipment or listening devices had ever been found.

Yonhap News Agency
Military mulls leasing reconnaissance satellite from Israel
Tuesday, 18 October 2016
Byline: Staff reporter

Seoul - South Korea is considering leasing a reconnaissance satellite possibly from Israel to independently obtain information on North Korea's military activities, military officials said Tuesday. South Korea has heavily relied on reconnaissance satellites operated by the United States when it comes to core military information involving the North's nuclear and missile-related moves, according to the Ministry of National Defense.

"The military is expected to have its own surveillance satellites as early as 2023 that will allow Seoul to closely monitor military activities in North Korea," said a ministry official.

"It is years behind the defense ministry's original schedule to deploy five surveillance satellites between 2021 and 2022 as part of the country's "kill chain" strike system to deal with missile threats from the North," according to the official.

Faced with increasing nuclear and missile threats by the North, the government is looking to lease a reconnaissance satellite from Israel or other foreign countries, the official said.

In addition, the military plans to purchase another 90 KEPD-350K air-launched cruise missiles from Germany's Taurus Systems GmbH. The initial shipment of 170 KEPD-350K is currently being transported to South Korea, with the remainder set to be shipped in 2017.

The Taurus missile can be mounted on the South Korean Air Force's main F-15K fighters and can be used to hit the capital city of Pyongyong while the planes are flying safely over Daejeon, 164 kilometers south of Seoul.

If the Taurus missile, with a range of over 500 km, are added to the Air Force's inventory, South Korea will be the first operator of fighter jets in Asia equipped with this advanced system.

Besides satellites and missiles, Seoul as part of the Korean Air and Missile Defense (KAMD) system plans to operate a total of four early-warning radars by around 2020 to counter the North's submarine-launched ballistic missiles. KAMD is designed to detect and destroy incoming missiles and other aerial threats, the military said.

Pyongyang has conducted five nuclear tests in the past decade and launched a series of missiles, including an intermediate-range ballistic missile which is believed to be capable of reaching U.S. territories in the Pacific like Guam.

Hindustan Times
India needs to counter cyber attacks by Pakistan
Tuesday, 18 October 2016

Mumbai - In the wake of cyber-attacks on Indian websites - allegedly made by hackers from Pakistan - in the backdrop of the recent surgical strikes and killing of Kashmiri civilians, cyber-experts from India said a lot needs to be done by the government and financial institutions to win the "cyber war".
A senior official of the state police said hackers disrupt economic activities and inconvenience customers by hacking into Indian websites. They steal confidential data and either sell it or demand money in exchange for not misusing it. The biggest problem here is the anonymity offered by the internet.

"Hackers can get away with anything due to geographical shrinking. Experts said the internet was first used to convert and radicalise people online. Now it is used to spread cyber terrorism, which hurts the economy, affects businesses, disrupts services and facilitates extortion and blackmail," he added.

"We have lost the cyber war to Pakistan. Our neighbours are very good at cyber-terrorism. We are not attacking them in cyber space. It is also difficult to gather evidence against the hackers," said cyber security expert Vijay Mukhi.

"Countries are deploying cyber warriors to attack vital organisations in other (enemy) countries is nothing new. Pakistan, China, Iran and North Korea have deployed cyber warriors by providing them with immunity from the consequences. Earlier, the websites of the Central Bureau of Investigation and the National Defence Academy were hacked into," said D Sivanadhan, former director general of police (Maharashtra).

"Even terrorist organisations such as the Islamic State have deployed cyber warriors to hack into websites and ridicule the American establishment and Malaysian airlines. The most vulnerable industries are banking, finance , energy, oil, electric power production and supply sector and nuclear power," he said.

"We have to establish robust protection mechanisms and develop mechanisms to safeguard against such attacks. We have to spend resources to upgrade our technology. A security audit needs to be done regularly by a third party. The Indian Computer Emergency Response Team (CERT) can conduct an investigation to find the people behind such attacks. Government websites are soft targets and so we have to create awareness among people working in such sectors," he said.

Mukhi stressed the need for a cyber-policy and an increased budget to tackle such attacks.

A hackers group calling themselves 'D4RK 4NG31' infiltrated the National Green Tribunal's website this month and posted profanities on it in an act of "revenge" against the Indian army's recent surgical strikes. "We are unbeatable. You... kill innocent people in Kashmir and call yourself defenders of your country. You...violate the ceasefire on border and call it 'surgical strikes'. Now kiss the burn of cyber war," posted the hackers.

The Government Law College's official website was hacked into this month by a group calling itself 'PakCyberPyrates'. Students who visited the website were directed to its homepage, which had the following message, 'National Securities Depository Limited...OOPSS.. To all Indians out there..surgical strike...lolx..hahahahaha!!!'.

The accounts of about 50 IT companies accounts were attacked by Pakistan-based hackers over the past 10 days.

Jakarta Post
Kaspersky Lab warns about financial cyberthreats in Asia Pacific
Tuesday, 18 October 2016
Byline: News Desk

Jakarta - One of the key topics of Kaspersky Lab's Cyber Security Weekend for Asia Pacific Countries that took place earlier this month in Indonesia was financial cyber-security. The company's experts and guests discussed financial threats that are currently on the rise globally and starting to penetrate the APAC region.
"Financial threats vary, from online fraud and banking Trojans that affect PCs, tablets and smartphones, to attacks on financial organizations, ATMs and even point-of-sale terminals. Analyzing our statistics, we see that as the financial sector in Asia-Pacific countries is developing fast, cybercriminals are increasingly looking for ways they can profit from it. Since a lot of organizations and individuals often forget about security when adopting new technologies, we believe it's important to remind them about cyber security principles that will help them stay safe," said Vitaly Kamluk, Kaspersky Lab's Director of Global Research and Analysis Team in APAC.

The Consumer Security Risks Survey 2016, conducted by B2B International and Kaspersky Lab, showed that 67 percent of respondents in APAC countries are worried about online banking fraud and 63 percent said they often worry about their vulnerability when making financial transactions online. 62 percent stated they would use online payments more often if they had reliable protection for financial transactions. Consumer concerns about financial security are well-founded; 5 percent of consumers globally have lost money online as a result of scams or fraud, with the average sum lost reaching USD 476.

"Spam, phishing and banking Trojans are among the most widespread financial threats. So users should be attentive to fake web pages, unexpected e-mails asking to provide financial information, and secure their mobile devices if transactions are made from them. While organizations should also regularly check their IT infrastructure and especially computers from which financial transactions are made," explained Kamluk.

Banking Trojans remain one of the most dangerous online threats. They are often propagated via compromised or fraudulent websites and spam emails and, after infecting users, steal personal information such as bank account details, passwords, or payment card details. According to Kaspersky Security Network data, in the third quarter of 2016 compared to the same period of 2015 the number of banking Trojans increased in the Philippines (by 24 percent), India (by 31percent), China (by 43 percent) and Vietnam (by 104 percent). Vietnam and India were the countries with the largest number of victims. Other countries saw decrease in the number of victims, one of the reasons for which might be the effect of the raised awareness of users, new government initiatives or even a geographical preference defined by the criminals behind banking Trojan malware campaigns.

Arab News
Saudi Arabia tightens noose on cybercrime
Tuesday, 18 October 2016
Byline: Rashid Hassan

Riyadh - The Kingdom is making concerted efforts to tighten the noose on cybercrime with work on novel solutions pertaining to information security.
The Kingdom will host the Global Internet Forum and Exhibition early next year, with the main objective of highlighting the government's efforts in combating cybercrime, ensuring cybersecurity and facilitating e- governance and its mechanisms concerning Vision 2030.

The forum will be held in mid-March in Jeddah with the participation of experts, authorities and companies specialized in the field of Internet and communications from across the world, said Khalid Naqro, supervisor of the exhibition.

The Cabinet meeting here on Monday approved a number of procedural arrangements relating to security and safety projects, including provisions that government agencies have to verify, when implementing their projects, their compliance with regulations and instructions on security and safety.

The Cabinet was briefed on the Kingdom's participation in the second committee of the 71st session of the UN General Assembly, during its discussion on "Exploitation of Science and Technology for Development," and the Kingdom's confirmation that it will continue its march in the ongoing support for the implementation of the results of the world summit on the information society.

This emanates from its belief in the significant importance of the outputs of the summit and its contribution to achieving the goals of sustainable development.

Moreover, the Cabinet expressed condemnation on all acts of terror, confirming the Kingdom's rejection of terrorism in all its forms and manifestations.

Earlier, commenting on the Global Internet Forum on Combating Cybercrime, Nagro said the forum, accompanied by an exhibition, aims to empower people from Arab states, including the Kingdom, to present their innovations and allow participants to build strong relations to enhance the Arabic content on the Internet, and to overcome information security challenges in order to move forward toward a knowledge- based economy, as envisioned under Vision 2030.

Asharq al-Awsat
Saudi Arabia Set to Host Global Exhibition on Combating Cyber Crimes
Tuesday, 18 October 2016
Byline: Fahd Baqmi

Jeddah - Saudi Arabia will host the Global Internet Forum and Exhibition, which highlights the Saudi government's efforts in dealing with cybercrimes, the e-government and its mechanism concerning the 2030 Vision; the event will be held with the participation of experts, authorities, and companies specialized in the field of internet and communication from across the world.
Khalid Naqro, supervisor of the exhibition said that this event will be held for the first time in the Middle East and is considered one of the most prominent events called for - by the Kingdom - amid international growth of use and demand on the internet; forecasts have showed that users who benefit from the internet service around the world have reached 3.2 billion, which represents around half of the world's population.

Naqro added that the exhibition, which targets governmental entities, the private sector, organizations of civil society and companies of e-commerce, in addition to research and e-banking centers, will showcase many projects, services, and apps; the event will also embrace special initiatives on the Arabic content, projects, and new ideas aiming at attracting international apps, exchanging expertise. The event will also focus on highlighting Saudi Arabia's efforts in the field of information technology (IT) and on providing many chances of partnership between the private and governmental sector.

The exhibition will discuss 20 different topics by featuring global speakers; topics are expected to include services provided by global companies for the Arabian customer, innovations, successes of websites and apps, and how these apps contributed in developing the community, in addition to themes like internet and the family, globalization and intellectual invasion, entertainment, and internet as a bullying platform.

The event will also showcase many global experiences on the role of educational entities and institutions in stimulating efforts of students to enrich the Arabic content, reasons behind this latter's weakness, experiences of the Global Arab Network (GAN) and news of the internet.

It's worth mentioning that official figures have showed that internet users in Saudi Arabia reached around 21.6 million by the end of 2015 representing 68.5% of citizens and residents, which shows the leap of internet growth over the past years; users of Twitter in the Kingdom exceeded three million who post more than 1.5 million tweets daily; as per Facebook, its users in Saudi Arabia have reached six millions while a million people use LinkdIn, YouTube, and different mobile apps.

FCW.com
Official: you can still trust the NSA
Tuesday, 18 October 2016
Byline: Sean D. Carbery

Washington - It might not be as momentous as knocking down the Berlin Wall, but tearing down the barriers between Signals Intelligence and Information Assurance inside the National Security Agency is revolutionary, an NSA official in the thick of those efforts contends.
The NSA is six weeks into "NSA21," which the agency calls the most substantial organizational reform in its 60-year history. Announced earlier this year, NSA21's primary change is flattening the organization and moving it from a mission-based construct to a functional model.

Curtis Dukes had been until recently the deputy director of NSA's Information Assurance directorate. Now, he's deputy national manager of national security systems in charge of the IA portfolio of the new operations directorate.

"We have a 60-year history of having two missions separate and distinct with common leadership at the top," he said. "Both missions have been highly successful, but where we found difficulties was in sharing between those two missions."

Dukes said that the current reforms have been in the making for the last decade. He said that NSA director Adm. Mike Rogers had two primary objectives.

"One was to propel us for the next decade -- make sure that we're tightly integrated between the two missions -- and that also more importantly was that we're optimized when it comes to cyber, both from exploit as well as from the defense standpoint," he said.

Dukes said that by removing the separation between signals intelligence (offense) and IA (defense), the two groups can better share information about potential vulnerabilities and exploits to further each other's missions.

"What this new organization construct brings is that we can put the best athlete to help with incident response and mitigation," explained Dukes. "We also can have the best athlete help with building better architectures to help the defensive mission. I think that's what we're trying to strive for in that regard."

The reorganization is hardly without controversy, however, in no small part because of the inherent contradiction between the NSA's primary missions. The Signals Intelligence directorate has been responsible for spying and increasingly looking for cyber vulnerabilities to exploit in intelligence gathering.. The Information Assurance directorate has been responsible for protecting systems -- government, private sector and international partners -- from exploitation.

Some clients have often wondered if the NSA's guidance came with strings, or more specifically, back doors, to help the signals intelligence mission. And since the announcement of NSA21 there has been more grumbling from some in industry that the NSA cannot fully be trusted.

NSA's reputation in the information assurance business took a hit from leaks by former contractor Edward Snowden that included confirmation that an NSA-approved cryptographic algorithm was deliberately compromised. Still, Dukes said that there has been trust in the past, and that should continue under the new system.

"We understood how things would be attacked from an adversarial standpoint, again from the signals intelligence perspective, and then we would go engage with industry and with international partners and also produce security configuration guidance and best practices based on that information," he said. "We strongly believe in our configuration guidance and our best practices."

One risk Dukes acknowledges is the possibility of compromising aspects of the signals intelligence mission because other nations can use unclassified NSA information to improve their cybersecurity.

"I think there will always be that argument that, well, how do I know if I'm talking to NSA I'm talking to the information assurance mission or to the signals intelligence mission?" Dukes said. "The short answer is that we do wall that off internally here [so that] if we're engaging with industry to help them better secure the product we're doing it for all right and honorable reasons."

So, despite the wall being torn down, Dukes said there will continue to be some degree of internal separation, and the current practice of vetting the release of information about vulnerabilities will continue.

"Prior to NSA21, regardless who found the vulnerability, whether it was the signals intelligence or the information assurance missions, we kick that up to an issue resolution process where both missions debate and discuss the vulnerability," said Dukes. "If one mission said that 'you know we need to release' or another mission said that 'we need to restrict,' it's fiercely debated."

In the last three years, the NSA created the Vulnerabilities Equities Process (VEP) to evaluate whether vulnerability information should be shared with interested parties so they can protect their systems, or whether disclosure would compromise intelligence gathering. Dukes said these tensions, procedures and discussions will continue under NSA21.

"I'm the senior NSA officer that represents NSA in the VEP process, and I'm a fierce advocate for, you know, if I think the nation's at risk, I highlight that, I make that argument both to Admiral Rogers and to [White House cybersecurity advisor] Michael Daniel in that regard," he said. "But it is a vote and each member can have a say in that and ultimately Michael will make a decision whether to disseminate or to restrict."

Dukes said the U.S. needs to do some soul-searching over its cyber defense structures and protocols in general. NSA has authority for national security systems, but does not have the authority to support agencies like the Office of Personnel Management, State Department or Environmental Protection Agency.

"That's where we work closely with DHS and FBI and we use their authorities to go in and do incident response and mitigation," said Dukes. "I don't think we're fully optimized as a nation yet in that regard. I think there's always going to be a bit of a lag for us to then provide support as we work though the authorities issue with DHS and FBI."

Dukes said by the time bureaucratic priorities are sorted out, "you've lost valuable time in order to do defense at cyber speed in that regard, and I think that's what we need to relook at as a nation."

Dukes said he's a fan of the United Kingdom's new National Cyber Security Centre, which puts emphasis on offensive capabilities as well as active cyber defense in collaboration with industry. "I think it's a model that should be looked at from a U.S. perspective as well," said Dukes.

Dukes said that NSA21 is still very much in its early stages and it's too soon to tell if it's on the right track or needs tweaking. He said there will be an internal review in about 90 days to see how things are progressing. One of the biggest challenges will be merging the public-facing culture of IA with the secret culture of signals intelligence.

"Over 60 years those cultures get pretty rigid, so we can't expect that in six weeks that we've, you know, totally changed the culture in the agency," said Dukes.

"In the sort term you'll still see us kind of inching along," said Dukes. "But I think a year out, it will just be, 'hey, who's available?' Whether you're signals intelligence or information assurance on this mission, you go in to do support for the nation."

The online JavaScript tidy website can optimize the JS code.

New York Times
Agencies Split on Classifying Clinton Emails
Tuesday, 18 October 2016
Byline: Eric Lichtblau, Steven Lee Myers

Washington - Documents released Monday in the Hillary Clinton email investigation show intense disagreement last year between the State Department and the F.B.I. over whether some of Mrs. Clinton's emails should be considered classified, including a discussion of a possible "quid pro quo" to settle one dispute.
The new batch of documents indicated that in one particular case, a senior State Department official, Patrick F. Kennedy, pressed the F.B.I. to agree that one of Mrs. Clinton's emails on the 2012 Benghazi attack would be unclassified -- and not classified as the bureau wanted.

What remained unclear from the documents was whether it was Mr. Kennedy or an F.B.I. official who purportedly offered the "quid pro quo": marking the email unclassified in exchange for the State Department's approving the posting of more F.B.I. agents to Iraq.

Officials at both the F.B.I. and the State Department said Monday that no deal had been struck, or even offered, over the classification of Mrs. Clinton's private emails. They noted that the Benghazi email in question had been made public with a sentence blocked out, meeting the F.B.I.'s demand for classification. They also said no additional F.B.I. agents had been posted overseas.

There is no indication from the documents that Mrs. Clinton was aware of the discussion.

Donald J. Trump and other Republicans nonetheless quickly seized on the new documents as evidence of what Speaker Paul D. Ryan called "a cover-up."

The F.B.I.'s latest release of 100 pages of internal investigative files prolonged the intense public scrutiny of Mrs. Clinton's use of a private email server as secretary of state, which has been perhaps more damaging to her presidential campaign than any other issue.

The new documents also cast particular attention on the role of Mr. Kennedy, a State Department civil servant for more than four decades, in working to oversee the review and public release of tens of thousands of Mrs. Clinton's private emails.

One of the F.B.I. reports said State Department employees who reviewed nearly 300 of Mrs. Clinton's emails on the Benghazi attacks in early 2015 in response to requests from Congress had "felt intense pressure" from Mr. Kennedy and other senior State Department officials to complete their review quickly and "not label anything as classified."

Mr. Kennedy was part of a long-running battle between the State Department and the intelligence agencies over Mrs. Clinton's emails. As the emails were prepared for release, officials from the intelligence agencies argued in some cases that information in them should have been marked classified, while State Department officials countered that they contained the routine business of American diplomacy. State Department officials, who argue that the intelligence agencies are overzealous in classifying information, remain sensitive to criticism that they were sloppy in handling the material.

In one of the newly disclosed documents, an unidentified F.B.I. employee told investigators that Mr. Kennedy, through another F.B.I. official, had sought in one case "assistance in altering the email's classification in exchange for a 'quid pro quo.'"

The F.B.I. had deemed the email classified, but the State Department disagreed.

The employee told investigators that "in exchange for marking the email unclassified, State would reciprocate by allowing the F.B.I. to place more Agents in countries where they are presently forbidden," according to the F.B.I.'s summary of the employee's questioning by investigators.

A second F.B.I. interview included in the documents provides a somewhat different version of the dispute over the classification of the Benghazi email, with the suggestion that the F.B.I. -- and not Mr. Kennedy -- had offered to make a deal.

In the interview, an unidentified F.B.I. official in the international operations division said Mr. Kennedy had complained to him that the F.B.I. classification of the document "caused problems for Kennedy" and that Mr. Kennedy had wanted to give it a different designation and file it in the State Department basement -- "never to be seen again."

The unidentified F.B.I. official said he was the one who then "told Kennedy he would look into the email matter if Kennedy would provide authority concerning the F.B.I.'s request to increase its personnel in Iraq."

The email they were struggling over was sent on Nov. 18, 2012, by William V. Roebuck, who oversaw the department's office for North Africa and is now the American ambassador to Bahrain.

In it, he notified five other officials of the arrest of "several people" in Libya on suspicion they were connected with the Benghazi attack two months earlier. It was subsequently forwarded to senior officials at the department and then to Mrs. Clinton on her private email account by her deputy chief of staff, Jake Sullivan, with a short "f.y.i." note.

Mark C. Toner, a State Department spokesman, said that no favors had been exchanged in the discussions of Mrs. Clinton's emails, and that there had been no change in the number of agents in Iraq

as a result of the conversations. "The allegation of any kind of quid pro quo is inaccurate and does not align with the facts," Mr. Toner said.

The F.B.I. also said there was "never a quid pro quo," but it said the accusations had been referred to the bureau's inspection division, which handles internal ethics issues, to investigate. The F.B.I. official who discussed the issue with Mr. Kennedy has since left the bureau, an official said.

One of Mr. Trump's foreign policy advisers, Michael T. Flynn, a retired general who headed the Defense Intelligence Agency, said the documents provided "undeniable proof" that Mrs. Clinton had "colluded with the F.B.I., D.O.J. and State Department to cover up criminal activity at the highest levels."

Two prominent members of the House -- Jason Chaffetz of Utah, the chairman of the Committee on Oversight and Government Reform, and Devin Nunes of California, the chairman of the Permanent Select Committee on Intelligence -- called on Secretary of State John Kerry to relieve Mr. Kennedy of his position pending an investigation.

In a letter to Mr. Kerry, they accused Mr. Kennedy, the State Department and the F.B.I. of collusion. They charged that the State Department had altered its normal process in reviewing Mrs. Clinton's emails, consulting directly with the Justice Department and bypassing the F.B.I.'s input. A spokesman for Mr. Trump's campaign, Jason Miller, said Mr. Kennedy should resign.

Mr. Toner said Mr. Kennedy would remain in his position with the full support of Mr. Kerry.

After the email issue emerged in March 2015, Mrs. Clinton insisted for months that she had never sent or received emails that contained classified information. But she was forced to backtrack, as the F.B.I. concluded this summer that at least 110 emails had contained classified information, even if they had not been marked as such at the time.

Washington Free Beacon
Clinton Email Server Hit in Cyber Attacks From Russians, Other Hackers
Tuesday, 18 October 2016
Byline: Bill Gertz

Washington - Hackers from Russia attempted to break in to Hillary Clinton's private email server although the cyber intrusions did not appear to be successful, according to FBI documents made public Monday.
FBI investigators issued a qualified assessment of whether foreign hackers broke into the email server, stating in the heavily redacted report that it could not confirm evidence of foreign hacking.

The FBI concluded that the unsecure email system was "potentially vulnerable to compromise" and was frequently attacked by unknown foreign hackers, according to part one of a four-part report.

Hacking attempts against Clinton's private email server increased sharply after the New York Times revealed its existence on March 2, 2015. The cyber attacks were targeted against the server, an associated domain controller, and Clinton's Apple iCloud account, the FBI stated.

The Times report did not identify Clinton's email address, but the FBI said hackers likely learned her email address from open sources after aide Sidney Blumenthal's AOL email was hacked in 2013. Among the hacked emails made public were emails between Blumenthal and Clinton writing under the email alias "hdr22."

The FBI stated that Blumenthal was hacked by the Romanian hacker Marcel Lehel Lazar, known as "Guccifer," and suggested he was linked to Moscow.

U.S. intelligence agencies announced on October 7 that the Russian government, operating through cutouts identified as Wikileaks, DCLeaks.com, and Guccifer 2.0, directed the hacks of American political organizations in a bid to influence the U.S. presidential election.

"Lazar disseminated emails and attachments sent between Blumenthal and Clinton to 31 media outlets, including a Russian broadcasting company," the FBI said.

Additionally, hackers from Russia and Ukraine tried to log in to Clinton's email accounts shortly after Guccifer's hack of Blumenthal.

"An examination of log files from March 2013 indicated that IP addresses from Russia and Ukraine attempted to scan the server on March 15, 2013, the day after the Blumenthal compromise, and on March 19 and March 21, 2013," the report said. "However, none of these attempts were successful and it could not be determined whether this activities was attributable to Lazar."

Lazar's claim to Fox News that he used information from Blumenthal's emails to break into the Clinton server was false, the FBI said after questioning the hacker.

Other cyber attacks on the server included numerous attempted break-ins described by the FBI as "brute force" attacks-- repeated log-in attempts, usually by automated hacking software.

Brian Pagliano, who was the system administrator for the email server, told the FBI that the brute force cyber attacks increased over time, although he asserted there were no security breaches to the system.

The server used for the emails also employed a Microsoft remote access protocol that the FBI described as having "known vulnerabilities" to hackers.

In January 2011, Justin Cooper, an aide to former President Bill Clinton who helped set up the private email, notified Clinton aide Huma Abedin that the system was being hacked and that he had shut it

down in response. The FBI was unable to identify what it termed the "successful malicious login activity" from the hack.

Forensic analysis by FBI investigators determined that "scanning attempts" by outside cyber intruders took place against the private server and "one appears to have resulted in a successful compromise of an email account on the server," the report said.

The hack took place on January 5, 2013, when an anonymous user operating Tor software hijacked the email account of a woman described by the FBI only as a "President Clinton staffer." The hacker then browsed email folders and attachments.

The FBI also stated that potentially malicious hackers tried to exploit software vulnerabilities in the server on multiple occasions, although they were not successful.

The report stated there were major gaps in the investigation of cyber intrusions because the FBI did not have access to all 13 mobile devices Clinton used during her tenure as secretary of state.

"As a result, the FBI could not make a determination as to whether any of the devices were subject to compromise," the report said, noting the FBI also did not examine two of Clinton's five iPads for signs of compromise.

Clinton was the target of multiple email "phishing" attempts while using the private server, including a fake email from a State Department official's email account that contained a potentially malicious link.

Clinton sent a reply to the email asking, "Is this really you? I was worried about opening it?"

Another email quoted Abedin as telling a colleague Clinton was worried "someone [was] hacking into her email" after she received an email from an associate with a link to a website with pornographic material.

"The FBI's inability to recover all server equipment and the lack of complete server log data for the relevant time period limited the FBI's forensic analysis of the server system," the report said.

"As a result, FBI cyber analysis relied, in large part, on witness statements, email correspondence and related forensic content found on other devices to understand the setup, maintenance, administration and security of the server systems."

More than 15 pages of the 47-page FBI report were cut out according to declassified guidelines that allow information to be withheld on national defense and foreign policy grounds, and to prevent the disclosure of techniques and procedures used for law enforcement prosecutions that would be useful to cyber criminals.

Wall Street Journal
Flight System Draws Concern
Tuesday, 18 October 2016
Byline: Andy Pasztor

New York - U.S. and European aviation authorities are focused on cybersecurity threats that could affect a basic data-transmission system widely used by airlines around the world.
Such concerns about the decades- old system called Acars -- primarily used for air-traffic purposes and to provide information about the status of various aircraft components during flights -- have surfaced in the past few months on both sides of the Atlantic.

The issue has been raised in U.S. government contracting documents, as well as in comments by industry officials and high-level European safety regulators.

The information sent by the Acars network from planes to the ground isn't considered safety critical, nor does the system handle any data that could immediately imperil safe operation of flights.

No specific hacking attempts or intrusions have been detected, government and industry officials said.

But as the industry moves to revise 1980s-vintage transmission protocols and methods, including use of new frequencies and expanded messaging formats, experts have expressed heightened worries about the vulnerabilities of Acars to hackers or other types of outside intrusions. Because of its age, the system lacks some of the safeguards embedded in newer onboard messaging networks.

Disruptions of Acars could result in major problems for airline scheduling, maintenance or other operational functions, experts interviewed over the past few months said.

Acars stands for Aircraft Communications Addressing and Reporting System, originally designed to send short air-to-ground messages.

Future uses envision dramatically greater capacity and a wider range of messages.

In September, the Federal Aviation Administration awarded a first-of-a-kind contract to Milwaukee-based Astronautics Corp. to develop comprehensive risk-assessment tools to pinpoint cybersecurity vulnerabilities of aircraft electronics.

Acars is slated to be the first onboard system that will be examined using those tools.

At the time, Astronautics said it planned to devise an "efficient, timely and repeatable process" to identify cyberthreats and risk-mitigation strategies.

FAA officials have declined to comment specifically about Acars or details of the contract. In an email last week, the agency said it "will continue to further strengthen its capabilities to defend against new and evolving" cyberthreats. Earlier, a top official of the European Aviation Safety Agency singled out Acars as a prime example of the need for stepped-up cybersecurity reviews of onboard data systems. Luc Tytgat told an FAA-EASA conference in Washington in June that work was under way "to see if we should not go back to certification" studies of Acars vulnerabilities.

Mr. Tytgat indicated Acars was at the top of the list for cybersecurity reviews, but added that EASA also planned to screen newer air-traffic-control technologies ready for deployment as part of a "total systems approach" that is "not something which is easy to implement."

Since then, several industry officials familiar with the details confirmed that the agency is specifically delving into such matters.

An EASA spokesman this month said the Acars studies are part of a broader effort to update certification requirements for new aircraft, anticipated to take effect starting next year. He said the agency also is looking at possible enhanced safeguards for Acars and other existing systems on today's fleet of commercial aircraft.

The activity comes amid escalating worries about cyberthreats to commercial aviation in general. Those threats have prompted a variety of government and industry responses, including devising future standards to ensure that any successful hacks will be detected and neutralized.

In addition, the FAA's top outside technical advisory group in September agreed to pay greater attention to cybersecurity threats across the full range of onboard equipment, internet connections and air-traffic-control communications. The updated guidelines are intended to affect areas including aircraft design, flight operations and maintenance practices, among others.

Reuters
Ecuador cuts Julian Assange's internet access
Tuesday, 18 October 2016
Byline: Mark Hosenball

Washington - Anti-secrecy group WikiLeaks said on Monday that its founder Julian Assange's internet was shut down by the government of Ecuador, deflecting blame from the U.S. or British governments which have sparred with Assange for releasing sensitive material.
"We can confirm Ecuador cut off Assange's internet access Saturday, 5 pm GMT, shortly after publication of (Hillary) Clinton's Goldman Sachs speechs (sic)," the statement from WikiLeaks said.

Assange has lived and worked in Ecuador's London embassy since June 2012, having been granted asylum there after a British court ordered him extradited to Sweden to face questioning in a sexual molestation case involving two female WikiLeaks supporters.

WikiLeaks said Assange lost internet connectivity on Sunday night.

"We have activated the appropriate contingency plans," added the Twitter message on Monday. People close to WikiLeaks say that Assange himself is the principal operator of the website's Twitter feed.

The Ecuadoran government offered no immediate comment on the question of internet access, but the country's foreign minister, Guillaume Long, said Assange remained under government protection.

"The circumstances that led to the granting of asylum remain," Long said in a statement late on Monday.

The government of leftist President Rafael Correa has long backed Assange's right to free speech, though the Wikileaks saga has caused some strain in relations with the United States, including the expulsion of diplomats in 2011.

Correa, whose term will end next year, has said he is behind Democratic candidate Hillary Clinton, who he says he knows personally, in the U.S. presidential election.

"For the good of the United States and the world ... I would like Hillary to win," Correa told broadcaster Russia Today last month.

Over the last two weeks, Democratic Party officials and U.S. government agencies have accused the Russian government, including the country's "senior-most officials," of pursuing a campaign of cyber attacks against Democratic Party organizations ahead of the Nov. 8 election.

WikiLeaks has been one of the most prominent internet outlets to post and promote hacked Democratic Party materials. While denying any connection with a Russian hacking campaign, Assange has refused to disclose WikiLeaks' sources for hacked Democratic Party messages.

Sources close to both the Democratic Party and WikiLeaks say they believe WikiLeaks has acquired as many as 40,000-50,000 emails hacked from the personal accounts of John Podesta, the former White House advisor who now chairs Clinton's presidential campaign.

Despite Assange's complaint that his internet connection was cut, WikiLeaks posted on Monday afternoon what it said was a fresh batch of Podesta's emails.

According to a summary of the latest emails posted on Russia Today, a media outlet with close links to the Russian government, highlights include campaign staff discussions about "galvanizing Latino support" and about how to handle media queries about Clinton's "flip-flopping" on gay marriage.

New York Times
British Bank Abruptly Drops Russian Network's Accounts
Tuesday, 18 October 2016
Byline: Neil MacFarquhar, Kimiko de Freytas-Tamura

Moscow - Russia's main English-language satellite network complained on Monday that its British bank was abruptly closing its accounts. The network, which reported on the decision, called it a British-government- sanctioned attempt to interfere with freedom of speech.
It was the latest controversy for the network, RT, originally and still commonly known as Russia Today. The broadcaster presents itself as an alternative to the Western media, but critics call it a Kremlin-financed mouthpiece that seeks to create an alternative to reality.

"Long live freedom of speech!" Margarita Simonyan, the editor in chief of RT, wrote sarcastically on Twitter, adding that the bank had offered no explanation for the step.

The network released a letter from the bank, NatWest, telling the broadcaster to take its business elsewhere. In the letter, the bank said that it would stop serving RT on Dec. 12, that the decision had come after "careful consideration" and that it was not subject to appeal. (The broadcaster initially reported that its accounts had been frozen, but it later clarified that the bank was closing the accounts, not freezing them, and that RT was still able to withdraw its money.)

NatWest's corporate parent, the Royal Bank of Scotland Group, said in a statement on Monday that "these decisions are not taken lightly." "We are reviewing the situation and are contacting the customer to discuss this further," the company said. "The bank accounts remain open and are still operative."

Britain's Treasury said the government was not involved in the bank's decision. "This is a matter for NatWest, not for the government," a spokeswoman said, speaking on condition of anonymity under government protocol. "We as the U.K. government haven't changed the sanctions and obligations related to Russia since February 2015. For that reason, this is a decision that only NatWest has made, possibly based on their own risk appetite."

RT presents itself as an independent and credible alternative to mainstream Western media, but its broadcasts repeatedly show the West as a sea of chaos. Ofcom, the British broadcast regulator, has singled out RT repeatedly for its lack of impartiality.

RT's defense has been that its viewers expect alternative viewpoints.

Maria Zakharova, a spokeswoman for the Russian Foreign Ministry, linked the bank's decision to the June 23 referendum in Britain, when voters opted to leave the European Union, an outcome that has plunged the country into economic and legal uncertainty. "It appears that in leaving the E.U., London has left all of its obligations on free speech behind in Europe," she wrote on Facebook.

In a statement on its website, RT called the bank's decision "incomprehensible and without warning." The network said the decision was part of a pattern in Britain and Europe in recent years to "ostracize, shout down or downright impede the work of RT."

Dmitry K. Kiselyov, the head of RT's parent organization, was placed on the European sanctions list in 2014 over his encouragement of the annexation of Crimea. Barclays, the company's previous bank in Britain, closed its accounts in July 2015.

In Moscow, the management of RT said on Monday that its lawyers were dealing with the banking situation and that the network would remain in operation.

"We have no idea what this is connected with, because nothing new happened to us, and we received no threats -- neither yesterday, nor a day before yesterday, or a month ago," the RBK news website quoted Ms. Simonyan, the editor in chief, as saying.

Jonathan Eyal, assistant director of Russian and European security studies at the Royal United Services Institute in London, said that the bank's action might have reflected concerns over RT's links to the Kremlin. "Certain questions are being raised over the corporation and its sources of funding," he said, "and the bank must have been aware that this is not a happy commercial transaction."

Mr. Eyal noted that some financial institutions had recently faced large fines for handling questionable accounts, and he speculated that NatWest may "prefer the controversy of closing the bank account over dealing with a business that may have tainted money."

Beyond that, he said, the bank may be following a lead, either directly or indirectly, from the United States, which has been weighing its response to Russian hacking of American computers and servers. The bank's action could be a kind of "veiled sanction," he said, aimed at "trying to convey to the propaganda sources that they are increasingly finding their life difficult in the West."

RT started in 2005 as Russia Today, a television network meant to sell Russia abroad through soft features. Very few watched. In 2009, it switched tracks, becoming a snarky anti-West outlet. It changed its name to RT and erased any obvious Russian link.

RT portrays itself as an independent alternative voice. It trumpets the slogan "Question More," yet generally sticks to the same major news that CNN or the BBC is covering.

The difference is less in subject matter than in tenor: On RT, the West is portrayed as grim, divided, brutal, decadent, overrun with violent immigrants and unstable. The network tends to make favorable remarks about Donald J. Trump, the Republican nominee for president; the former CNN host Larry King, who now appears on RT, scored a rare direct interview with Mr. Trump in September.

In RT's coverage, Russia seems to brim with multicultural tolerance; President Vladimir V. Putin is depicted as a modernizing leader protecting Russia's sovereignty with no dreams of empire; and the enormous civilian toll in Syria represents the unfortunate many who are caught in the crossfire as the Syrian government battles terrorists.

Most analysts interviewed by RT toe the line, and any who do not are rebuked. When one analyst recently said on the air that the Kremlin's 2014 annexation of Crimea remained an issue, the questioner quickly cut her off. "Crimea is off the table," he exclaimed, echoing a Putin statement.

In Britain, a study by the Institute for Statecraft found that despite its claims of neutrality in the European Union referendum debate, RT gave an edge to the "leave" camp.

Public accusations about a general Russian bias toward what is known as Brexit grew so loud that the Russian Embassy in London issued a statement saying that Moscow had no position on Britain's place in the European Union.

It is unclear how many viewers RT actually reaches. Figures released by the Broadcasters Audience Research Board in Britain for the week of the Brexit vote, for example, showed that the network had 926,000 viewers in the country, or 1.57 percent of the overall audience.

RT boasts that it is the "most-watched news network on YouTube" with over three billion views. Millions of those hits, however, were for raw disaster footage like the 2011 Japanese tsunami that had nothing to do with RT.

Washington Post
Documents show State Dept. official wanted FBI to change classification of one of Clinton's emails
Tuesday, 18 October 2016
Byline: Matt Zapotosky

Washington - A top State Department official tried to pressure the FBI to change its determination that at least one of the emails on Hillary Clinton's private server contained classified content, prompting discussion of a possible trade to resolve the issue, two FBI employees told colleagues investigating Clinton's use of a private server last year.
One FBI official conceded that he told the State Department employee he would "look into" changing the classification of a Clinton email if the official would lend his authority to an FBI request to increase its personnel in Iraq, according to documents released by the bureau Monday.

Another bureau official described the arrangement as a "quid pro quo" and said he believed that the State Department official, Undersecretary of State for Management Patrick F. Kennedy, was interested in "minimizing the classified nature of the Clinton emails in order to protect State interests and those of Clinton," the documents say.

No tangible swap ever came to pass. The email was classified in accordance with the FBI's original wishes, and the bureau was not given any additional personnel in Iraq. Both the FBI and the State Department denied that a quid pro quo ever existed.

Clinton's use of a private email server while secretary of state has dogged the Democratic presidential nominee's campaign and has proved to be an issue that resonates with voters. The new documents could add to perceptions among voters that Clinton is not trustworthy, and they come with the final presidential debate days away and the election in just a few weeks. The revelation of possible backroom dealing was immediately seized on by her critics.

In a video statement posted to his Twitter page Monday, Republican nominee Donald Trump said: "This is very big, and frankly, it's unbelievable. What was just found out is that the Department of Justice, the State Department, and the FBI colluded, got together, to make Hillary Clinton look less guilty, and look a lot better than she looks. This is one of the big breaking stories of our time, in my opinion. This shows corruption at the highest level, and we can't let it happen as American citizens."

Clinton campaign spokesman Brian Fallon said in a written statement: "It is well known that there was strong disagreement among various government agencies about the decisions to retroactively classify certain material in emails sent to Secretary Clinton. Agencies that took issue with this overclassification did so based on their own beliefs, and we were not part of these disagreements that played out inside the government."

The FBI said in a statement that it had referred the matter to the "appropriate officials for review." The agency did not respond to a message seeking comment on who those officials are. The official at the center of the matter -- who is not named in the documents -- has since retired, the bureau said.

The FBI and the Justice Department declined to bring charges against Clinton for mishandling classified information while she was secretary of state, and FBI Director James B. Comey has repeatedly and forcefully defended that decision. He also has pushed the bureau to be unusually transparent in showing the public how the probe was handled, testifying personally before Congress for hours and releasing hundreds of pages of documents.

The documents released Monday include summaries of more than three dozen interviews with technology company employees, FBI agents and Diplomatic Security officers who worked with Clinton.

The allegation of a "quid pro quo" -- first reported over the weekend by the Weekly Standard -- came from an official in the FBI's records management division, who was relaying an interaction between a colleague in the international operations division and Kennedy.

According to a summary of his interview, the international operations division had been trying to reach Kennedy on an unrelated matter for some months, and Kennedy called back wanting to talk about

Clinton's emails. Kennedy, the international operations official told investigators, said he wanted to change the classification of a Clinton email that was causing problems. The State Department was reviewing the emails for release under the Freedom of Information Act. It had submitted some emails -- all of which were marked unclassified -- for the FBI to review, and the FBI determined that at least one appeared to contain classified information.

Not knowing the email's content, the international operations division official said that he would "look into the email matter if Kennedy would provide authority concerning the FBI's request to increase its personnel in Iraq," according to a summary of his interview. The official seems to have called his colleague in the records management division.

That official told investigators that he had been "pressured" to change the email to unclassified and that Kennedy offered his colleague in international relations a "quid pro quo." It is unclear who first broached the purported deal. As part of his job at the State Department, Kennedy helped Clinton with her BlackBerry, though he has said he was unaware of her private server.

The international operations division official eventually called Kennedy back and told him he could not change the classification of the email, which was related to the attacks on the U.S. Consulate in Benghazi. Kennedy also was allowed to press his concerns with Michael Steinbach, who heads the FBI's national security branch, and Steinbach was similarly unyielding.

According to the documents released Monday, Steinbach told Kennedy the bureau would not change its classification decision, but it would also not discuss the matter publicly. Within an hour of that conversation, according to the FBI documents, the Associated Press published a story in which Clinton denied having sent classified emails on her private server.

Both the FBI and the State Department disputed that their employees had engaged in a quid pro quo. The agencies, though, acknowledged that Kennedy had inquired about the classification of an email, and the FBI said that in the same conversation, a bureau official "asked the State Department official if they would address a pending, unaddressed FBI request for space for additional FBI employees assigned abroad."

The FBI said its official was not a part of the criminal Clinton email investigation.

"The classification of the email was not changed, and it remains classified today," the bureau said in a statement. "Although there was never a quid pro quo, these allegations were nonetheless referred to the appropriate officials for review."

State Department deputy spokesman Mark Toner said in a statement that the allegation of a quid pro quo was "inaccurate and does not align with the facts."

"Under Secretary Kennedy sought to understand the FBI's process for withholding certain information from public release," Toner said. "As has been reported, there have been discussions within the interagency on issues of classification. Classification is an art, not a science, and individuals with classification authority sometimes have different views."

Kennedy did not immediately return an email seeking comment. In his own interview with the FBI, he disputed that he had ever tried to interfere with the Freedom of Information Act process.

The documents released Monday also contain other potentially damaging allegations.

One former Diplomatic Security agent, for example, told FBI investigators that Clinton "blatantly" disregarded State Department security protocols while she was secretary of state. The former agent alleged that Clinton would ride to foreign diplomatic functions with top aide Huma Abedin, instead of the local ambassador, which the agent said violated normal procedure and embarrassed and insulted the ambassadors.

The former agent also said that on an early 2009 trip to Jakarta, Indonesia, Clinton insisted on visiting a troubled area to promote an initiative, despite a request from Diplomatic Security that the visit be scrapped for safety concerns. The agent said Diplomatic Security officials thought the trip placed staff, security agents and even reporters in danger, all for a photo opportunity "for her election campaign."

The Independent (UK)
Cyber crime 'costs UK residents £210 each'
Tuesday, 18 October 2016
Byline: Josie Clarke

London - The UK lost almost £11bn to cyber criminals in the past year, figures suggest. The figure equates to approximately £210 per person over the age of 16 living in the UK, but is only based on incidents registered with the national reporting centre Action Fraud, Get Safe Online and the National Fraud Intelligence Bureau (Nfib).
A survey suggests the actual figure could be much higher, with respondents who had been victims of online crime losing an average of £523 each. More than a third of those who said they had been victims of online crime (39 per cent) said they had not reported the incident. The survey found more than half (53 per cent) had received fraudulent emails or messages which attempted to direct them to websites where their personal information could have been stolen and 28 per cent said they had been contacted by someone who was trying to trick them into giving away personal information. A tenth had had their email or social media accounts hacked.

Of those who said they had been a victim of cyber crime, more than a third (38 per cent) believed that the matter was too trivial to report and 37 per cent said they felt there was nothing that could be done. Get Safe Online's chief executive Tony Neate said: "The fact that the UK is losing nearly £11 billion to

cyber criminals is frightening and highlights the need for each and every one of us to make sure we are taking our online safety seriously. It is clear from our survey that people are very concerned, and rightly so."

"Let's not let cyber criminals get away with it anymore by ensuring that each and every one of us is updating the operating systems of our various devices and ensuring security software is always updated. What's more, we all need to ensure that we have a different password for each online account we own and website we visit. Online safety needs to be part of our everyday routines." The national lead detective for economic crime, Commander Chris Greany, said: "The huge financial loss to cyber crime hides the often harrowing human stories that destroy lives and blights every community in the UK.

"All of us need to ask ourselves are we doing everything we can to protect ourselves from online criminals. Unfortunately, people still click on links in unsolicited emails and fail to update their security software. Just as you wouldn't leave your door unlocked, so you shouldn't leave yourself unprotected online."

Get Safe Online said people should review their passwords to make sure they are strong and not use the same ones for more than one account, check social media privacy settings, update operating systems and software programs or apps if prompted, back up information using "the cloud" and check that internet security software and apps are up to date and switched on.

Fars News Agency
Iranian Air Force Exercises Electronic Warfare Tactics
Tuesday, 18 October 2016

Tehran - The Iranian Air Force F14 and Mig29 fighters as well as Falcon 50 jets exercised combat operations and electronic warfare tactics on the second day of the massive wargames in the Central province of Isfahan on Tuesday.
"At this stage, the operations to jam simulated enemy radar waves were successfully carried out using electronic-warfare special Falcon 50 jets under a research project named Sayeh (shadow)," Spokesman of the Fadaeeyan-e Harim-e Velayat-6 wargames Brigadier General Massoud Rouzkhosh said Tuesday.

"Also, the F14 and Mig29 fighter jets successfully exercised combat situations in a real-like battle scene in the operations," he added.

The Iranian Air Force kicked off 3 days of military drills in Central Iran on Monday.

A variety of Air Force fighter jets, fighter bombers, transport planes, reconnaissance aircraft, drones and refueling planes took part in the military exercises today.

The drills started at the order of Lieutenant Commander of the Iranian Air Force Brigadier General Alireza Barkhor.

In recent years, Iran has made great achievements in the defense sector and gained self-sufficiency in manufacturing essential military hardware and defense systems.

Yet, Iranian officials have always stressed that the country's military and arms programs serve defensive purposes and should not be perceived as a threat to any other country.

The Iranian Air Force displayed several squadrons of its operational fleet in an air show on the national Army Day in April.

Different types of fighter jets and fighter bombers took part in the air show staged over the mausoleum of the Founder of the Islamic Republic, the late Imam Khomeini, South of the capital Tehran.

The home-made 'Saeqeh' (Thunderbolt) fighter jets as well as F4, F5, F7, F14 and Mig 29 fighter jets in several squadrons flew over the sky of Southern Tehran.

Aerial refueling operation was also conducted by a Boeing 707 refueling tanker aircraft to an F4 and two F14 fighter jets during the air show.

Also, different helicopters, including Chinook, Cobra 206 and Cobra 214 flew over the military parade zone.

International Business Times (UK)
The Snoopers' Charter 'should terrify us all' says former MP
Tuesday, 18 October 2016
Byline: Jason Murdock

London - A former MP who previously sat on the Home Affairs Select Committee has spoken out against the incoming Investigatory Powers Bill - called the Snoopers' Charter by critics - which he brands a deeply intrusive piece of surveillance legislation "that should terrify all of us."
Dr Julian Huppert, a lecturer at the University of Cambridge and former Liberal Democrat politician, claimed the bill has avoided any real public debate or scrutiny and slammed its proposals as a "real threat" to technology firms operating in the UK.

"Some of the powers in the Bill are deeply intrusive, and with very little possible justification. All of us want to be safe, and protected from terrorists and the like - but the evidence that these powers are all needed is thin indeed. However, the cost to all of our privacy is huge," he wrote on OpenDemocracy.

The Investigatory Powers Bill (IPBill) contains a number of proposals aimed at bulking up surveillance powers open to the UK intelligence agencies MI5 and GCHQ, while allegedly increasing the oversight regime available to the politicians at Whitehall.

The more controversial aspects of the law include forcing technology firms to store internet metadata for 12 months, the massive collection of Bulk Personal Datasets (BPDs) and the bulk retention of communications data from phonecalls and text messages.

According to Huppert, who once worked to kill a previous snooping charter (the Draft Communications Data bill), many problems have persisted over the years. Indeed, even a number of political committees have slammed the latest proposals for lacking clarity.

"The political divide of the future won't just be left and right. It is also between a liberal, internationalist, open, tolerant view of the world, and a closed, nationalistic, authoritarian approach," he wrote. "We should all be very worried that both the government and the opposition have gone for the latter."

Many of the powers included in the bill - which the UK government claims are not new and already in use by British spooks - were exposed by former NSA whistleblower Edward Snowden back in 2013. At the time, he branded the UK's GCHQ as "worse than the US" over its use of the Tempora programme.

"There are many other problems with the legislation - real threats to tech companies in the UK, risks of inappropriate interference with telecoms equipment, pervasive bulk powers, far too little oversight, and a huge bill," said Huppert.

"25 October is the crucial date. That will be the third reading of this legislation. If the House of Lords let it go through, then there is nothing more to do to stop this. There will be the quaint process of parliamentary ping-pong to tidy the last few words up, but from then on, the state will have powers to monitor your behaviours on and offline to a far greater extent than ever before."

Nevertheless, with the sunset clause on the current surveillance law expiring in December 2016, the government appears to want the legislation in place as soon as possible. Sources familiar with the matter have previously told IBTimes UK the bill - at least in the intelligence community - is widely expected to pass.

As the next debate date quickly approaches, a new court judgement was disclosed which found UK surveillance agencies including GCHQ and MI5 collected communications data "in secret" and without the necessary oversight in place for over a decade.

Released by Privacy International, and detailed in a court judgement, the campaigning group called the ruling "one of the most significant indictments of the secret use of the Government's mass surveillance powers since Edward Snowden first began exposing the extent of US and UK spying in 2013."

Solicitor Mark Scott, who worked with Privacy International during an unprecedented legal challenge, said: "[The] judgement confirms that for over a decade UK security services unlawfully concealed both the extent of their surveillance capabilities and that innocent people across the country have been spied upon."

It World Canada
Snowden says Trudeau afraid to kill anti-terrorism bill
Wednesday, 19 October 2016
Byline: Howard Solomon

Whistleblower. Hero. Traitor. Patriot.
These words and more have been used to describe former cybersecurity contractor Edward Snowden, who in 2013 copied and distributed thousand of documents to reporters and whose stories of Western intelligence agencies -- including Canada's Communications Security Establishment (CSEC) -- shook the world.

This morning Snowden told the the annual SecTor cyber security conference in Toronto that Prime Minister Justin Trudeau want to amend the controversial Bill C-51 anti-terrorism law and not repeal it because he "is afraid of being attacked for being soft on terrorism."

Speaking by video from Russia, where he fled to avoid prosecution by U.S. authorities, Snowden said the legislation, needs three fixes: First, a judicial body should have oversight over federal intelligence agencies that has the power to prosecute authorities that have broken the law. Second, because intelligence agencies are trading personal information of citizens "like baseball cards" citizens should be told if the data sharing hasn't led to an arrest for criminal activity. And finally, what Snowden called the criminalization of speech through vague definitions of terrorism should be taken out of C -51.

A lot of what police call terrorism is the activity of what he called "common criminals" or those who are trying to make a political point but don't constitute a "super criminal threat."

He also said that governments are "lazy" for demanding software vendors put backdoors into their systems that can be accessed by law enforcement or intelligence agencies with a warrant. Any backdoor can also be access by a government like China, he said.

He also offered several ways people can better secure their personal information. Corporations should work for their customers first, not governments, he said, so they should only hold personal records for as long as they need and not indefinately.

He also said that in addition to following the usual safe online practices citizens should talk about government surveillance and civil rights with their families and friends and support civil rights organizations.

Snowden is a polarizing person.

"No doubt about it: Edward Snowden opened the windows and let the sun shine in on government surveillance," tweeted Canadian privacy expert Ann Cavoukian last month. On the other hand. Also last month the U.S. House of Representatives intelligence committee issued a 36 page report into his illegal

downloading of classified documents that called him a "disgruntled employee." The vast majority of the documents he stole had no connection to privacy or civil liberties, the report said. "Snowden's actions did severe damage to U.S. national security, compromising the Intelligence Community's anti-terror efforts and endangering the security of the American people as well as active-duty U.S. troops."

Since his revelations legislators and intelligence agencies in a number of Western countries -- including Canada have been sensitive to explain what kind of personal information they've been collecting and why, although a number insist they have lawful authority and the need to confront terrorists. While the new Liberal government has issued a consulting paper on new legislation to change the controversial Bill C-51, critics complain the discussion paper frames the debate in terms that give little doubt the government is leaning towards the police.

For example, it repeats Canadian police claims that "without specific legislation designed to permit access, law enforcement and national security agencies have had difficulty getting timely and effective access to BSI (basic subscriber information)" since the Supreme Court said they need a search warrant. There are also complaints the proposed intelligence oversight mechanism isn't independent or very powerful.

The last time Snowden spoke about this country was in 2015 when he spoke by teleconference to Canadian reporters. He criticized Canada for having one of the weakest intelligence agency oversights among Western Nations. However, he didn't comment directly on Bill C-51, saying it was up to Canadians to decide what was best.

Over the years he has made a number of statements about how the public and private sectors should face security. He's called for end to end encryption in all forms of messaging, for the protection of citizens, arguing that it would force spy agencies to focus on suspicious people rather than vacuuming up data from thousands of people at a time.

CBC News
Chinese billionaires take interest in Canadian clean technology
Wednesday, 19 October 2016
Byline: Katie Simpson

Canadian clean technology companies could be the next major investment for China's business elite. But cyber-security experts and the opposition are warning that the keen interest from Chinese investors must be treated carefully.

"For us at the moment, natural resources is not the top priority," said Wang Chaoyong, the chairman and CEO of ChinaEquity, one of the country's most successful independent venture capital firms.

"We are more interested in investing in environment technology, clean tech [and] innovative sectors such as creative industries," Wang said in an interview with CBC News.

The investment mogul is part of a delegation from the elite China Entrepreneur Club, which is touring Canada to get a closer look at potential investments.

The group, which is often called China's club for billionaires, met with Prime Minister Justin Trudeau on Tuesday.

"Canadian product, brand and innovative design are very popular in China, so we see the synergy between the Canadian product and the Chinese market," Wang said.

He explained his firm is looking to become a minority stakeholder in companies with products or systems that could be successful in China's massive market.

Wang said he's noticed a new spirit of willingness for economic co-operation between China and Canada.

"At the moment, I think we see the Chinese government and the Canadian government are doing a lot of work to help us."

'Attractive target'

According to a report by Ottawa- based Analytica Advisors, Canada's clean technology sector is made up of nearly 800 companies employing about 55,000 people.

The industry is expected to grow, as countries around the world become more environmentally conscious.

But because the industry is still developing, one cyber- security expert says Canadian companies could be vulnerable to hacking attacks.

"It's very much a new industry, and they can get in at the ground floor," said Keith Murphy, the CEO of Defence Intelligence, an Ottawa based cyber-security firm.

"It makes for a very attractive target," Murphy said.

Murphy said he understands Canadian businesses want to grow their companies, but owners should be wary of major investments from Chinese firms.

"Especially with a lot of the history we've seen with Chinese businesses, they've been used to attack the Canadian government, Canadian citizens, Canadian businesses in the past. And certainly the U.S. has fallen victim to this as well."

In 2014, Chinese state-sponsored hackers were accused of breaking into the computer system of Canada's National Research Council. The Chinese government adamantly denied the claim.

Former technology giant Nortel said extensive cyberattacks by Chinese spies played a role in the company's downfall.

Security checks in place, Ottawa says

As the federal government tries to strengthen ties with China, it is also downplaying concerns about investment and security.

"There's a well- established Canadian process for dealing with these issues under the Investment Canada Act with all of the appropriate safeguards in place," said Public Safety Minster Ralph Goodale.

"Canada's a country that welcomes foreign direct investment. Obviously, it needs to be a net benefit to Canada and all the security requirements need to be met. The procedure is there already in the law to deal with that," he added.

The opposition is warning the government to move slowly and to vet foreign investors carefully, for all sectors.

"We should ... do a little due diligence on the history of these individuals, how their billions were acquired, their relationships with state-owned industries in China," said Conservative foreign affairs critic Peter Kent.

"Canada is open for business, and should be open for business. But I think we have to be very careful about who is doing the buying and how that purchase will look down the road in terms of the Canadian economy and Canadian security interests."

Toronto Star
Toronto man detained after flying drone in Cuban square
Wednesday, 19 October 2016
Byline: Alicja Siekierska

Toronto - As Chris Hughes lay in the dark two-by-two-metre cell, with no electricity, a small hole in the wall for a window and just a hole in the ground for a toilet, he wondered if his wife Grace and three young children knew he was still alive.

"Nobody knew I was there," he said. "I had disappeared. I thought, my family must think I'm dead."

On Sept. 30, a few days before the Canadian man found himself in a Cuban detention centre, Hughes had flown a drone above the Plaza de la Revolucion in Havana.

A photographer with a media business in Toronto, Hughes said he had been travelling through the Americas, previously going to Panama and Colombia. He had brought a drone with him, which he used to shoot photos and videos. He said he did not have any issues using it the drone in other countries, and no problems bringing it in through Cuban customs on Sept. 28.

But two days later, the drone proved to be a significant problem.

Hughes said he and a Cuban friend and tour guide were questioned by police about the drone at the Plaza de la Revolucion, a historic square home to the Cuban administration. The pair was taken to a police station, where Hughes said they were interrogated for around 12 hours. He said he was brought to his rental apartment to pick up his clothes, and then brought to a detention centre, where he would remain for nearly two weeks -- but never charged.

Global Affairs confirmed that consular officials at Canada's embassy in Havana provided services to a detained Canadian citizen. "To protect the privacy of the individual concerned, further details on this case cannot be released," Global Affairs spokesperson Austin Jean said in an email.

The Star reached out to the Policia Nacional Revolucionaria office near the plaza, but was referred to a Havana-based immigration office. A receptionist at that number told the Star police was "not to give any information by phone." Another official advised the Star to submit requests through the Canadian Embassy in Cuba.

Hughes said he was held at what appeared to be an immigration detention centre and was again interviewed by Cuban authorities. Based on the questions, he believes Cuban authorities thought he was a spy.

After Hughes' wife hadn't heard from him in three days, she decided to alert the Canadian embassy. She said they were able to locate him after making contact with the family of his Cuban companion.

She then paid for Orlando Ismael -- a friend and project manager of Hughes' business -- to fly from Canada to Cuba to try to find answers.

Ismael, who arrived in Havana on Oct. 6, said he went to the police station at the plaza and was told about a detention centre for foreigners. He said officials at the detention centre confirmed Hughes was there and that he was arrested for flying a drone in the square. Although he briefly saw Hughes, Ismael was not able to speak with him at length.

Hughes said that the fifth or sixth day of his detention -- "I didn't know exactly how long I'd been there" -- he was able to meet with a woman from the Canadian embassy.

But it wasn't all good news; he said she told him the government had to let the investigation play out. "The investigator had told me that if I'm found guilty on any level, or if they find out I'm working with the American government, that I'll spend the rest of my life in jail," Hughes said.

Then, on Oct. 11, Hughes said he was brought into a room, asked to review the contents of his bag and informed that the following morning he would be taking an 8 a.m. flight back to Toronto. The next day, he was at Pearson International Airport, being embraced by two of his children and his wife.

"This whole thing felt like something out of a movie," his wife said.

Although it was harrowing, Hughes said he understands why he was detained, and doesn't begrudge Cuban authorities. He plans to return one day -- he said authorities told him he is welcome to come back.

"If you're under your mother's roof, you play by your mother's rules," he said. "My issue with the whole thing is that I had no clue whether I was going to be there for 13 days or 13 years. I just didn't know what was going to happen."

CBC News
Rigorous rules proposed for recreational drone flyers, documents show
Wednesday, 19 October 2016
Byline: Ashley Burke

Transport Canada is proposing that anyone flying a drone bigger than a tiny toy should have to register their devices, pass a knowledge test and pay for liability insurance, CBC News has learned.
Through an access to information request, CBC obtained the proposed regulatory framework for unmanned aerial vehicles (UAVs) that were sent to Transport Minister Marc Garneau in April 2016.

The department is proposing that anyone operating a drone weighing more than 250 grams, including recreational users, should fall under more rigorous regulations expected to be introduced in 2017.

"The proposed floor for very small UAVs is intended to minimize the risks to persons, based on the speed and potential lethality," the briefing note says. It adds that even "very small" drones can travel quickly and impart so much energy upon impact that there is a 30 per cent "likelihood of lethality."

'Just getting too strict now'

The department's plans are "overkill," said drone user Nick Howe.

"I think it's just getting too strict now."

Howe spent more than $2,300 on his recreational drone, including special parts, and has travelled across Canada making videos to showcase aerial views of the country online. Just because some people are acting irresponsibly doesn't mean all recreational users should have to pay the price, he said.

"It just means more money I'm going to have to spend," said Howe, who also started producing videos for real estate companies. "It's a lot more of a hassle than anything."

Safety concerns

Transport Canada staff began looking into regulations for drones in 2010. Since then, the industry has boomed, prompting safety concerns.

"We need to regulate that to make sure that we don't have a disaster," said Aaron McCrorie, Transport Canada's director general of civil aviation, in an interview. "The recreational users are going to have to meet more stringent safety requirements now."

McCrorie has seen a dramatic increase not only in the number of people buying drones, but also the number of users flying them dangerously close to airplanes and buildings.

In 2010, the department investigated one incident. In 2016, the department has investigated 82 potential infractions as of Sept. 1.

"We do have instances of these things crashing into vehicles, for example, so there has to be some means of accounting for the cost of those damages," McCrorie said, emphasizing the need for liability insurance.

Age restrictions

Transport Canada is also considering age restrictions for drone users, as exists for pilots. The department is proposing a minimum age of 14 to operate a very small drone and a minimum of 16 to operate a drone heavier than one kilogram, according to a briefing note from April.

The government also plans to stop regulating based on recreational versus commercial use. The new model is based on how much potential risk a drone could cause based on its weight and where it's flown, according to Transport Canada.

But recreational drone user Andrea Robertson believes 250 grams is "far too low" to fall under the new regulations.

Robertson, known as Lady Drone on YouTube, is afraid of heights, so she flies a Phantom drone to live the experience through her camera. She's glad there are new regulations coming and agrees drones can be dangerous, but has concerns about finding insurance to cover her if there's an accident.

"Because I'm a hobbyist, not a commercial flyer, I haven't been able to find any insurance companies that will provide insurance," Robertson said. "The insurance companies, at this point, are only interested in commercial fliers."

'Less red tape' for commercial users

Meanwhile, the proposed regulations could mean a lot less red tape for those using drones for commercial use, such as making real estate videos or inspecting construction sites. Instead of having to reapply at least every year for a certificate to fly drones commercially, it could get a lot easier.

"You go through the process once and then you'll have a licence just like having an automobile licence," said Mark Aruja, chairman of the Board for Unmanned Systems Canada, a group that co-chaired the working group to help develop the regulations.

"The expectation is we'll have less red tape going forward," added Aruja. "But there will be a significant bar to meet in terms of getting that operating licence."

Transport Canada launched consultations in 2015 and received more than 100 written submissions. Staff members are currently drafting the regulations that could still change, and working to develop the necessary licensing and exams before the regulations come into effect, likely sometime in 2017.

Press TV
Iran Air Force conducts e-warfare drills
Wednesday, 19 October 2016

Tehran - Iran's Air Force has successfully conducted electronic warfare as part of large-scale three-day military drills in the central province of Isfahan.
The e-warfare exercises were held on Tuesday, the second day of ongoing drills codenamed Fada'eeyan-e Harim-e Velayat 6 (The Devotees of the Velayat Sanctuary 6).

Brigadier General Massoud Rouzkhosh, the spokesman for the maneuvers, said the Air Force used advanced communications systems and secure wireless or wire-connected networks, flight apparatus systems, and tactical systems during the drills.

The application of deceptive jamming methods against mock enemy radars were among the electronic warfare tactics employed by Falcon 50 aircraft on the second day, he said.

Later through the day, interceptor F-14 aircraft conducted aerial surveillance and other operations, while F-14 and MiG-29 fighters engaged in dogfights.

The drills also deploy domestically-built Sa'eqeh, F-4, F-5, and Sukhoi Su-24 jets, transport aircraft and unmanned aerial vehicles, as well as a wide range of projectiles, including smart bombs and laser-guided missiles.

Rouzkhosh said among the maneuvers' points of strength were the amplification of the force's firepower and the enhancement of its precision targeting capabilities.

Iran says its military might poses no threat to other countries, stating that its defense doctrine is based on deterrence.

Bangkok Post
Cyberattacks growing threat to industry
Wednesday, 19 October 2016
Byline: Suchit Leesa-nguansuk

Bangkok - The growing adoption of intelligent automation and control systems in industry has made them a prime target for cyberattacks, says a pioneer in automation control serving industrial processes worldwide.
Cybercriminals are also using advanced methods to attack mission-critical systems, targeting critical infrastructure such as electricity and oil and gas plants.

"We've seen this trend coming since 2010 -- the industrial sector becoming one of the most targeted for cyberattacks," said Safdar Akhtar, business development director for Industrial cyber security of Honeywell Process Solutions, a division of Honeywell International Inc.

Stuxnet, a malicious computer worm discovered in 2010, specifically targets programmable logic controllers, which allow the automation of electromechanical processes such as those used to control machinery for factory assembly lines, amusement park rides or centrifuges that separate nuclear material.

In 2012, the worm's malicious activity served as a wake-up call to the energy industry, especially for potential security breaches at oil and gas companies.

Cybersecurity has since been recognised as a critical element for automation control systems in industrial sectors, especially outdated control systems whose vulnerabilities may not be known, said Mr Akhtar.

In addition, he stressed that the proliferation of the Internet of Things, which involves factory machines and industrial goods coinciding with the increased adoption of cloud computing technology, poses massive challenges for industrial companies.

He said plants can reduce the known risks by building private- owned cloud computing environments that can help prevent security problems, as they can limit access to cloud management functions.

Honeywell Process Solutions has expertise in automation control systems, providing industrial cybersecurity solutions and services including cybersecurity assessment and risk manager, a real-time data collection and analytic software platform that continuously monitors the process control system for indications of cyber security risks. The company has secured over 1,000 industrial cyber projects globally, he said.

Honeywell is targeting a wider range of industries including refining and petrochemical, oil and gas, chemicals, power generation, minerals and mining, and pulp and paper.

Honeywell has recruited at least 10 more cybersecurity experts for the group's operating units in Asia-Pacific.

The surge of cybersecurity threats has driven up demand for the cybersecurity workforce to increase by 10 times, said Mr Akhtar, adding that the industry needs 6-12 months to fill the positions. Thailand is an important market for Honeywell as it is a manufacturing base in Southeast Asia, he said.

The government's policy to push the development of a digital economy and Industry 4.0 are also increasing the country's already-high potential. Furthermore, cybersecurity has become a national priority for policymakers.

New York Times
Ex-F.B.I. Official Acknowledges Role in a New Clinton Email Controversy
Wednesday, 19 October 2016
Byline: Eric Lichtblau, Steven Lee Myers

Washington - A former F.B.I. official at the center of the latest controversy over Hillary Clinton's private emails acknowledged on Tuesday that an offer to swap favors with a State Department counterpart on an email classification issue had originated with him -- until he realized the deal involved Mrs. Clinton and the 2012 attack in Benghazi, Libya.
"When I found that out, all bets were off; it wasn't even negotiable," the former F.B.I. official, Brian McCauley, said in a telephone interview.

Republicans have seized on the episode to accuse the State Department of trying to protect Mrs. Clinton, but Mr. McCauley's account could undercut those attempts because he said he, not the State Department, had suggested the "quid pro quo."

Mr. McCauley recounted in the interview that Patrick F. Kennedy, a senior State Department official, called him in spring 2015 looking for help in getting the F.B.I. to agree not to classify the disputed email. Mr. McCauley said he had agreed to try to help him if Mr. Kennedy would help him get the State Department to restore two spots that the F.B.I. had lost recently in the Baghdad embassy.

"I'm the one that threw that out there," Mr. McCauley said of the offer. He said that he was concerned the two vacant posts posed a security risk at the embassy, and that the offer was typical of how federal agencies "help each other and work with each other."

In that initial conversation, Mr. McCauley said, "it was a quid pro quo; I don't deny it."

Mr. McCauley said he had quickly reversed himself, however, after calling another F.B.I. official and learning that the email in question involved the Benghazi attack -- a political cudgel for Republicans against Mrs. Clinton.

At that point, Mr. McCauley said, he abandoned any thought of exchanging favors and called Mr. Kennedy immediately to tell him that he could not help. "It was off the table; the quid pro quo was not even close to being considered," Mr. McCauley said.

His account was largely consistent with that of Mr. Kennedy, who made his first public comment on the controversy in a written statement put out on Tuesday by the State Department, a day after the email episode emerged in new documents released by the F.B.I.

The F.B.I. documents did not identify Mr. McCauley; The Washington Post first identified him and interviewed him about his account on Tuesday.

Mr. Kennedy, who also did not identify Mr. McCauley in his statement, said he called the F.B.I. official for help last year because he "wanted to better understand" why the bureau wanted to classify a portion of the Benghazi email before its release to the public.

Like Mr. McCauley, he said the issue of the F.B.I.'s positions in Baghdad had come up in the conversation, but he said that there had never been an implicit or explicit offer to exchange favors.

"At no point in our conversation was I under the impression we were bargaining," he said, adding that in nearly four decades in the Foreign Service, he served Democratic and Republican administrations. "My motivations were never political," Mr. Kennedy said.

He said he did not believe the information should be classified as "secret," but should instead be redacted, or blacked out, on the grounds that it contained information related to a continuing investigation.

"We take very seriously our responsibility to decide whether our documents are classified or not classified," Mr. Kennedy said. "We can't simply cede that responsibility to another agency."

Mr. McCauley said he remembered Mr. Kennedy's telling him in their initial phone conversation that he wanted to redact part of the email on different grounds so it could be "buried in the basement" of the State Department.

But State Department officials denied any intention to bury the email. In the end, the State Department accepted the bureau's argument and released the email with a sentence redacted as secret because it related to the F.B.I.'s Clinton email investigation.

Even so, Republicans continued to focus on Mr. Kennedy's handling of the emails. Donald J. Trump, for a second day, said on Tuesday that Mrs. Clinton's email server was a scandal "worse than Watergate." Representative Robert W. Goodlatte of Virginia, the chairman of the House Judiciary Committee, asked the Justice Department on Tuesday to open a criminal investigation into Mr. Kennedy and his role in the purported quid pro quo.

"Under Secretary Kennedy's attempt to barter away American national security interests for plainly political purposes is appalling and may rise to the level of a federal crime," Mr. Goodlatte wrote in the letter.

President Obama, appearing with Prime Minister Matteo Renzi of Italy at the White House, dismissed the controversy over the F.B.I. documents when asked if it disturbed him.

"Based on what we have seen, heard, learned, some of the more sensational implications or appearances, as you stated them, aren't based on actual events and based on what actually happened," he said, "and I think derive from sort of overly broad characterizations of interactions between the State Department and the F.B.I. that happen a lot and happen between agencies."

Mr. McCauley saw the episode in much the same way.

Mr. Trump and other Republicans, he said, "are grasping at straws."

"There was no political motivation in this at all," he added.

Mr. McCauley retired from the F.B.I. last summer after 35 years because of a medical issue. He said his retirement was unrelated to the email episode.

F.B.I. officials said that while they had referred the quid pro quo accusation to their inspections branch for an ethics review as a matter of policy, the issue had become moot because Mr. McCauley left the bureau. State Department officials said they had not conducted an internal review because they had seen no basis for one.

The Intecept
Ecuador Cuts Internet Access for Julian Assange to Preserve Neutrality in U.S. Election
Wednesday, 19 October 2016
Byline: Robert Mackey

Washington - The government of Ecuador confirmed on Tuesday that it had decided "to temporarily restrict access" to the internet inside its embassy in London, effectively cutting off Julian Assange, the editor of Wikileaks, who has lived there since he was granted political asylum in 2012.
Assange first reported on Monday that his internet connection had been "severed by a state party," and the organization was forced to resort to a back-up plan to continue its work.

"The Government of Ecuador respects the principle of non-intervention in the internal affairs of other states," the statement said. "It does not interfere in external electoral processes, nor does it favor any particular candidate."

As The Intercept reported in August, since Wikileaks began publishing emails hacked from the accounts of Democratic party officials, the site's editor has been accused of attempting to undermine Hillary Clinton's campaign for the presidency.

While a founding principle of Wikileaks was that its editors would not know the identity of those who supplied them with documents, the U.S. Intelligence Community said earlier this month that it "is confident that the Russian Government directed the recent compromises of emails" later provided to the site, in order "to interfere with the U.S. election process."

Intelligence officials have not disclosed evidence to support their attribution of responsibility to Russia, but private cybersecurity experts who investigated the hacking of the Democratic National Committee's servers pointed to what they called strong circumstantial evidence.

The communique released by Ecuador on Tuesday said that the country "does not yield to pressure from other states," but Wikileaks claimed to have learned from unnamed American sources that a request to shut down Assange's work had come from Secretary of State John Kerry.

Wikileaks most recently published emails hacked from the Gmail account of the Clinton campaign chairman, John Podesta, which included partial transcripts of paid speeches Clinton gave to Wall Street bankers after her tenure as secretary of state.

Ecuador's president, Rafael Correa, told the Russian government's news channel RT last month that a victory for Clinton would be better for the United States, and the world, but a Trump win could produce benefits for left-wing parties in Latin America.

"Obviously, for the U.S., it would be better if Hillary won. I know her personally and have a great deal of respect for her," Correa told RT.

"But, seriously, Trump would be better for Latin America," he continued. "When did progressive governments come to power in Latin America? With Obama or with Bush? Bush's primitive policies were rejected so much that it caused reaction in Latin America. Trump would do the same: maximize the contradictions."

"So, for the good of the U.S. and the world, and because of my personal esteem for her," Correa concluded, "I want Hillary to win."

New York Times
Ecuador Cuts Assange's Link to the Internet
Wednesday, 19 October 2016
Byline: Steven Erlanger, David E. Sanger

London - Ecuador said Tuesday that it had cut off Julian Assange's access to the internet in his exile in the country's London embassy, making clear that it feared being sucked into an effort to "interfere in electoral processes" in the United States by the activities of the WikiLeaks founder.
Ecuador said that it was not evicting Mr. Assange from its embassy, where he sought asylum four years ago. It said that its "temporary restriction" of internet services to Mr. Assange "does not prevent the WikiLeaks organization from carrying out its journalistic activities."

But it was clearly intended to keep the embassy from being the control center for that leaking operation. "The government of Ecuador respects the principle of nonintervention in the affairs of other countries," it said in a statement, "and it does not interfere in the electoral processes in support of any candidate in particular."

The internet cutoff was the latest twist in the odd tale of Mr. Assange's self-imposed exile, which began in 2012 when he sought refuge from a Swedish rape investigation that he said was a cover for an American effort to extradite him. Since then, his world has shrunk to a single apartment inside the small diplomatic compound in central London. He has communicated through the embassy's internet connections, visitors and, presumably, cellphones that would give him another form of internet access.

Ecuador's decision was the first sign that the government in Quito was beginning to wonder if its guest in London was overstaying his welcome.

It doubtless was considering the possibility that, should Hillary Clinton prevail in the United States election next month, it would have to explain its role as host to the man who, by remote control, appears to have coordinated the publication of emails purloined from people close to Mrs. Clinton, along with those of the Democratic National Committee and other organizations.

The announcement came a day after WikiLeaks said that Mr. Assange's connection to the internet had been severed shortly after the organization published speeches that Hillary Clinton gave to Goldman Sachs, the global investment firm. The transcripts, the latest in a series of disclosures, appear to have come from the hacked email account of John D. Podesta, the chairman of her campaign and a White House chief of staff when Mrs. Clinton's husband was president.

The statement clearly sought to separate Ecuador from the decision by WikiLeaks to publish Mr. Podesta's emails and, before that, those hacked from the national committee and elsewhere. In recent weeks, Mr. Assange, once the hero of the American left for exposing classified State Department and Pentagon documents, has been hailed by Donald J. Trump and his advisers for disclosures from Mrs. Clinton's campaign, which Mr. Trump has used almost daily to fuel his attacks on her.

American intelligence agencies have said that the D.N.C. hack was the work of the Russian government and had to be approved at the highest levels of the Kremlin. But it is unclear how the documents made it to WikiLeaks, which has never said where the emails came from, if it knows.

Only hours before Ecuador's announcement, WikiLeaks charged that Secretary of State John Kerry quietly urged the Ecuadorean government, in a meeting late last month, to stop Mr. Assange from publishing the emails or interfering in the election. The State Department issued a statement declaring that the reports were untrue.

Ecuador's action, experts inside and outside the United States government say, is not likely to slow the flow of leaked emails. Those emails are routed through servers around the globe, and if the United States wanted to shut them down covertly, that presumably would have happened years ago.

In fact, American officials have said, turning off the flow of WikiLeaks data is a legally complicated issue, especially if American citizens or American-based firms are involved. The Obama administration, they say, does not want to be accused of suppressing unwelcome speech -- in the manner of the Russians and the Chinese.

Efforts to reach WikiLeaks on Tuesday were unsuccessful. A sometimes spokesman, Kristinn Hrafnsson, did not return messages, and a telephone message and an email message to Sunshine Press, which represents Mr. Assange, were also unanswered.

Mr. Assange has insisted he does not know the source of the WikiLeaks material, though he has made no secret of his distaste for Mrs. Clinton. The United States government has said that much of the hacking was the work of Russian intelligence and was part of a broad effort to influence the election. So

far, the White House has not announced how it will respond, though several options have been discussed with President Obama, according to administration officials.

On Sunday, in a taped interview broadcast on NBC's "Meet the Press," Vice President Joseph R. Biden Jr., in what was either a warning or an effort at psychological warfare, said that "we're sending a message" to the Russians "at a time and place of our choosing" and that President Vladimir V. Putin will "know it" when the message arrives. That seemed to suggest some kind of covert action, perhaps a cyberstrike, in retaliation for what the American intelligence community has described as a broad and unprecedented effort by a foreign power to influence American voters.

It is possible that Ecuador feared that, because of its decision to give exile to Mr. Assange, it risked becoming a witting or unwitting participant in an effort at voter manipulation.

WikiLeaks provided no evidence to support its claim that Mr. Kerry had pressured Ecuadorean officials, during a private meeting in Colombia last month, to clamp down on Mr. Assange, and the State Department's spokesman, John Kirby, immediately denied the accusation. "Reports that Secretary Kerry had conversations with Ecuadorean officials about this are simply untrue. Period," he said.

The president of Ecuador, Rafael Correa, is a man of the left, and he recently told the Kremlin-backed broadcaster RT that he would support Mrs. Clinton.

At the same time, he suggested in the interview that a victory by Mr. Trump, who has made no secret of his admiration for Mr. Putin, would be good for Latin America because it would, paradoxically, bolster leftist parties.

"I sincerely believe that it would be better for Latin America if Trump won," Mr. Correa said. "When did progressive governments come to power in Latin America? During the Bush administration. His primitive policies were rejected so much that it caused reaction in Latin America. Trump would do the same."

Questions to the Ecuadorean Embassy on Tuesday were met with a reference to the embassy's website and a brief statement.

"In view of recent speculations, the government of Ecuador reaffirms the validity of the asylum granted four years ago to Julian Assange," the statement said.

Mr. Assange is the subject of an arrest warrant in Sweden, which wanted to question him about allegations of rape and sexual abuse dating to 2010, to decide whether or not to bring charges.

Mr. Assange, saying that he feared extradition to the United States on espionage charges stemming from the publication by WikiLeaks of secret documents given to the website by the former Army analyst Chelsea Manning, broke bail and took refuge in the Ecuadorean Embassy in June 2012. He has been in the tiny embassy since.

Given the statute of limitations, the one allegation Mr. Assange still faces in Sweden is rape. He is wanted for questioning but has not been charged.

There is no public indictment in the United States of Mr. Assange; if Sweden chose not to press charges, he would presumably be free to leave the embassy.

fed scoop.com (US)
Feds need clarity on cyber structures
Wednesday, 19 October 2016
Byline: Shaun Waterman

Washington - The federal government needs to get its act together on cybersecurity, and there needs to be a public debate about the proper role for agencies like the Department of Homeland Security and the National Security Agency, public and private sector leaders said Tuesday.
"We really need to define what we want our government to do in cybersecurity, former Rep. Mike Rogers told an audience at FedScoop's FedTalks. "We have lots of capability. The NSA has lots of capability," he told a packed auditorium in Washington at the annual event.

By giving DHS, rather than NSA, the lead in defending civilian government networks and working with the private sector to protect the nation's vital industries, the U.S. had "take[n] our best players off the field," complained Rogers, who chaired the House Permanent Select Committee on Intelligence.

"Candidly," Rogers said, that decision "was politically driven and not policy driven. People were a little nervous about having NSA ... dealing directly with them" and their networks -- even companies that had a prior relationship with the NSA or the Pentagon were nervous.

Despite the ongoing furor over the government's role in protecting the private sector from foreign state-sponsored cyberattacks, speakers said there wasn't clarity about the respective roles of the intelligence and law enforcement in the cybersecurity space.

There is an inherent difference in -- even conflict between -- the missions of intelligence, law enforcement, and network defenders in the federal cybersecurity space, RSA President Amit Yoran said in a morning keynote.

Intelligence agencies "watch ... and want to keep watching," malicious actors in cyberspace, Yoran said, whereas law enforcement want to watch only to gather evidence to prosecute them. Meantime network defenders "may not care at all who attacked them," he said.

"We need more clarity about roles, responsibilities and authorities between agencies," Yoran concluded.

"We have not yet fully engaged -- on the public side -- [in a discussion about] what we want our government to do. How engaged do you want the NSA to be in defending private sector networks?" Rogers added.

Is DHS the agency that should be in the lead [in cyber defense] in the US, given the level of threats? We could probably debate that for an hour and a half," he said.

Rogers said that while working on cyber threat information sharing legislation in the last congress, the intelligence committee had conducted a great deal of outreach to the private sector to see who they would prefer to deal with in the government when it came to cybersecurity.

"Candidly ... we did not find one example of someone saying yes, I want to deal with DHS," he said.

Another example of an unresolved issue, speakers said, is the dual-hatted job that Adm. Michael Rogers has as director of the NSA and commander of U.S. Cyber Command.

"This structure is now over six years old," Adm. Rogers said, joining the former Congressman of the same name for a cybersecurity chat at FedTalks.

"The reason we got this structure is, we were building Cyber Command and we wanted to harness the ... significant investments the Department of Defense had already made in cyber .. at the NSA," Adm. Rogers said.

There have recently been moves, both in Congress and in the executive branch, to separate the two jobs, and give Cyber Command its own commander.

"My position has always been, this is the right thing to do at the wrong time," said Adm. Rogers, adding "It's a reflection of the maturation of Cyber Command that we're even having this discussion."

"The challenge is: What's the right time, what's the right process, so that [we do it] with minimal risk," he concluded.

"I have candidly been going back and forth on this issue," said Rep. Rogers, who chaired the House Intelligence Committee. "The only thing I worry about is [if we split it up] does Adm. Rogers [of cyber command] have to talk to Director X of NSA to perform the same function he does today. If we can't eliminate that question then I'm not sure I can support it."

"We probably don't have this right just yet," he finished.

Yoran called out the General Services Administration's FedRAMP cloud security certification process as a successful effort to raise the cybersecurity bar in the federal government.

"It was painful at first, but it is driving security requirements into next generation of [IT] infrastructure," he said.

Reuters
Czech police arrest Russian man in connection with US hacking attacks
Wednesday, 19 October 2016
Byline: Staff report

Prague - Czech police have detained a Russian man wanted in connection with hacking attacks on targets in the United States, the police said, without giving further details.
The arrest was carried out in cooperation with the US Federal Bureau of Investigation, Czech police said on their website on Tuesday (Oct 18) evening. Interpol had issued a so- called Red Notice for the man, seeking his arrest, they added.

The Russian citizen was detained at a Prague hotel. Police said he collapsed and was hospitalised. Czech courts will decide whether he will be extradited, the police said.

A police spokesman declined to give further details on the arrest. It was not immediately clear what hacking attacks the Russian citizen was wanted for.

The US government this month formally accused Russia for the first time of a campaign of cyber attacks against Democratic Party organizations ahead of the Nov 8 presidential election.

Russian President Vladimir Putin has said a hacking scandal would not be in Russia's interests.

CNN.com
Ex-CIA chief: Russian hackers trying to 'mess with our heads'
Wednesday, 19 October 2016
Byline: Nicole Gaouette

Washington - A former head of the CIA said Tuesday that Russian hacking of US political groups is intended to "mess with our heads" and shake confidence in the American electoral system -- rather than influence the outcome on Election Day.
Retired Gen. Michael Hayden said that he doesn't believe Russian President Vladimir Putin is trying to sway the election in favor of Republican nominee Donald Trump, but using the hacked information to disrupt the electoral process.

"This is too much of a carom shot for Putin to think he knows where that ball's going to end," Hayden said, speaking at the Heritage Foundation in Washington. "I think they're doing this to mess with our heads, to erode confidence in our political process."

Hayden, also a former director of the National Security Agency and now with the Chertoff Group, was discussing cyber security challenges facing the next administration.

Russia's suspected cyber attacks fell into the category of normal state spying, Hayden said, until Moscow "weaponized" the information.

"My definition of what the Russians did is, unfortunately, honorable state espionage," Hayden said. "A foreign intelligence service getting the internal political emails of a major political party of a major foreign adversary? Ah, game on. That's what we'd do."

Hayden said it's "good spy stuff" for a country to try to learn "how much of those platform positions the potential president-elect believes in personally, or doesn't."

That "is good spy stuff, that's stuff we go for all the time," Hayden said.

But then, Hayden said, Moscow's conduct "went beyond espionage" and crossed a line.

First, by using "Russian criminal gangs as a way to create a little distance from the Russian state and the actual actors," Hayden said.

Second, to take internal emails "and then begin to use them to influence the American election, well, that's quite a different matter," Hayden said. "And in our terminology, that has now moved from an espionage activity to a covert or not very covert influence operation."

The Obama administration has pointed the finger at Russia for hacking attacks on the Democratic National Committee and certain targeted individuals, saying it blamed "Russia's senior-most officials."

WikiLeaks has been releasing thousands of emails daily from Hillary Clinton's campaign manager John Podesta, an embarrassment and distraction for the campaign. US officials familiar with the investigation have told CNN that there's mounting evidence Russia is supplying WikiLeaks with the hacked emails.

The hacks have become a campaign issue with Clinton's team accusing the Russians of interfering on behalf of Trump, who has showered praise on Putin.

The Trump campaign has strongly rejected the charge that the Kremlin is looking to boost it.

WikiLeaks founder Julian Assange has made clear his desire to see Clinton lose the election.

The administration has promised retaliation, which Vice President Joe Biden said on NBC's "Meet the Press" Sunday would be covert.

"The message -- he'll know it," the vice president said, referring to Putin. "It will be at the time of our choosing and under the circumstances that have the greatest impact."

Hayden said he hoped the administration wouldn't be too subtle about using its cyber power.

"I hope that we've impressed upon bad actors that actions have consequences," he said, "and that we've demonstrated our will to use our weapons."

Inside Defence (US)
Rogers: 'We're working our way through' process to split NSA- CYBERCOM roles
Tuesday, 18 October 2016
Byline: Marjorie Censer

Washington - Adm. Mike Rogers, the chief of U.S. Cyber Command and the National Security Agency, said today he is thinking through the "right time" and "right process" to split the roles he holds. Speaking at a FedTalks event in Washington, Rogers said the idea behind the shared role was for CYBERCOM, in its early days, to harness the "insight, capabilities and knowledge" of NSA.

Now, he's asking: "Are the assumptions that we made still accurate? Have things changed? Is the environment different?"

The challenge in splitting the roles, Rogers added, is "what's the right time, what's the right process so that we do it in a way that enables both organizations to fulfill their missions with minimal risk?

"So we're working our way through that process," he continued. "In the end, this is a decision that the president of the United States is going to make, and we'll see where that process takes us."

Speaking on the same panel, Mike Rogers, the former Republican representative from Michigan, said the decision should be based on effectiveness, not on budgets.

"I heard the argument even when I was chairman [of the House Permanent Select Committee on Intelligence] that it's muddling the resources," he said. "I don't believe that should be our problem."

Ultimately, the former congressman added, he's focused on "does Adm. Rogers have to talk to Director X at NSA to perform the same function he does today?"

Financial Times
Social media: Challenging the jihadi narrative
Tuesday, 18 October 2016
Byline: Madhumita Murgia, Hannah Kuchler

London - On a sweltering September afternoon in a packed auditorium at Kingston College in south-west London, Humza Arshad is holding a crowd of more than 100 teenagers spellbound. Wearing a padded jacket and a woolly hat despite the heat, he tells the students that he has come to talk about radicalisation and extremism -- "a light topic for a Thursday afternoon", he jokes.
About a quarter of the audience raise their hands when asked if they are Muslim; all seem transfixed by the speaker, best known for playing a hapless south London Asian immigrant on his YouTube series Diary of a Badman.

Mr Arshad, 31, starts with a bit of dark humour, pointing to a photo of gun-toting terrorists -- and then reeling off the names of his cousins. Next, the face of a 15-year-old Bangladeshi girl in a hijab fills the screen and a murmur ripples across the room. Some recognise her as Shamima Begum, the straight-A student from east London who left her home in February last year bound for Syria. Shamima and her two friends, labelled the "jihadi brides" by the tabloids, ended up in Raqqa, an Isis stronghold. They have never returned.

"No one would ever have thought something like that would happen to them and it made me realise that if it can happen to a family like that, it can happen to anyone," he tells the crowd. "Imagine if this was your sister or best friend and she disappears."

Mr Arshad is one of a growing group of digital media stars who use YouTube videos, Facebook posts, tweets, photos and standup comedy to counter the barrage of extremist propaganda online -- particularly from social media-savvy terrorist groups such as Isis. His YouTube series, which tackles issues facing Muslim youth in London, has been watched more than 73m times. One video, "I'm a Muslim, not a terrorist" has been screened in more than 100 schools around the UK by the police.

"A lot of girls were being brainwashed by these guys online, on Facebook and Twitter, so I had to do something," Mr Arshad says.

Muslim content creators like Mr Arshad have been embraced by Google, Facebook and other tech companies, which have faced attacks from critics for what they see as their failure to effectively monitor and remove terrorist content. A report published in August by the UK parliament's home affairs committee accused tech groups of "undermining" counter-terrorism investigations by refusing to hand over potential evidence.

This embrace of so-called counter-speech goes beyond Silicon Valley: after seeing limited success with their own propaganda efforts, the US departments of justice and homeland security, the European Commission and the British government are all recruiting documentary filmmakers and university students to produce compelling, shareable content to battle the jihadi message. The US state department also this year launched the Global Engagement Center to counter Isis propaganda.

Tools of indoctrination

The Isis social media machine appears to have been diminished since mid-2015, but its presence on Twitter, YouTube and other sites has been the terrorist group's most powerful tool of persuasion, particularly in Europe and the UK. It has a 24/7 media wing, with five official video production houses. "Many say if it were not for the internet there would be no Islamic State," says Yasmin Green, head of research and development at Jigsaw, Google's think-tank that has been analysing radicalisation online.

While social media companies are keen to promote their efforts in this area, its effectiveness in preventing terrorism is unproven.

"It would be fair to say we are in a primitive stage. It's fantastic that Facebook or Google are sponsoring one or two projects, but that doesn't give you enough data to make viable statements about whether counter-speech works or not," says Professor Peter Neumann, founder and director of the International Centre for the Study of Radicalisation and Political Violence in London.

In particular, it is unlikely to change the behaviour of hardcore converts. "If someone has made up his or her mind and you then try to counter their view, it could produce a response known as reactance -- actually causing them to become even more resolute in their opinions because you are challenging their beliefs," Prof Neumann says.

"So it's not about counter-speech being good or bad, it has to be aimed at people in a particular stage of their decision-making. It has to be easy for these people to search out when they are googling different points of view."

Until now, taking down objectionable content has been the primary weapon in the battle against online extremism. Social media groups' complete control of user accounts means even governments are dependent on them to respond to urgent requests.

The major social platforms all rely on users to report inappropriate content, although Facebook and Google say they proactively take down accounts associated with known terrorists. "When we become aware of an account supporting terrorism, we look at their friends, and associated accounts, so we can remove them," says Monika Bickert, head of public policy at Facebook.

Twitter announced in mid-August that it had suspended 360,000 terror-inciting accounts since mid-2015, with the number of daily suspensions up 80 per cent. Account suspensions also rose in the aftermath of the terrorist attacks in Brussels in March and Nice in July.

But experts believe this is merely a temporary disruption to the extremists' efforts. In many cases when radical accounts are taken down, they either migrate to encrypted sites like Telegram or WhatsApp, or pop up with new accounts on the same sites. On Twitter, Isis propagandists openly boast about their 30th and 40th Twitter handles. "You can disrupt extremists and divert them, but you can't censor your

way out of that conundrum," says Prof Neumann. "It's an incomplete and ultimately ineffective strategy."

The UK parliament's home affairs committee went further in its report, accusing social media groups of "consciously failing" to prevent their sites from being used for terrorist propaganda. The committee's members said it was "alarming" that the tech companies have only a few hundred employees monitoring networks with billions of accounts.

Sophisticated propaganda

The Isis media operation publishes video and audio files, religious treatises and magazines every week, according to Zahed Amanullah, head of counter narratives at the Institute for Strategic Dialogue, a London think-tank.

"More importantly, the messaging is so well-designed: they have German expats speaking to Germans, British foreign fighters recruiting their peers. They have reach that they have never had before," Mr Amanullah says. "The migration of foreign fighters from Europe and Britain is a direct result of the sophistication of this propaganda."

Sensing that they were losing the propaganda war, business leaders from Silicon Valley, Madison Avenue and Hollywood gathered at the Department of Justice in February to watch and learn from Isis' videos.

The executives were not shown the videos of beheadings and burnings, but the sophisticated soft-focus marketing deployed by Isis to recruit young western Muslims. Designed to be shared on social media, the videos show Isis members giving treats to children -- candyfloss is handed out in videos targeted at Americans and Nutella in those hoping to lure Europeans. John Carlin, assistant attorney-general at the DoJ, appealed to content creators for help. "The most creative minds came up with this technology," he said. "Can you think up a way to stop this appalling nihilist group from doing this?"

Facebook invested 1m in a Berlin-based initiative in partnership with the ISD to spur creativity in this area, and Google has held eight counter-speech workshops this year on how to make compelling YouTube videos. Twitter has worked with the UK's Media Diversity Institute to develop a guide on how to challenge hateful views.

Another initiative has been developed by EdVenture Partners, a non- profit organisation. It runs a counter-speech competition in 150 universities around the world. Since its launch, 130,000 students from Afghanistan and Istanbul to the Netherlands have competed to design the most creative and effective counter-speech campaign, ranging from hashtags to short videos.

One campaign by a team of Afghan students called "Islam says no to extremism" reached more than 5m people on Facebook alone.

Under their skin

One of YouTube's earliest offerings, an animated series starring a fictional working-class Londoner called Abdullah-X, was put together by a former Islamist extremist and animator, who asked not to be named. Abdullah- X is not targeted at a general audience, like Mr Arshad's satirical comedy, but aimed squarely at people sympathetic to extremism.

One video, "Five Considerations for a Muslim on Syria", uploaded in March 2014, hit a nerve. "Within six weeks, we reached 50,000 people in our target audience, people literally typing 'I want to go to Syria' in Google search got the video in front of them," says Mr Amanullah of the ISD, which has worked on the Abdullah-X project.

Isis operatives issued an explicit 5,000-word line-by- line rebuttal, including arguments supporting the need for violence. "Islam is a tradition of jihad?...?and there will not cease to be jihad until the day of judgment," it said.

For Mr Amanullah, the response was a sign that the message was working. "It got under their skin," he says.

The Jigsaw pilot programme targeted vulnerable people by their search history, showing them ads on Google that led to a curated playlist of Arabic- and English- language YouTube channels. The clips include stories from ordinary people about the reality of life under Isis, and a soldier's first-hand narrative of what it was like to fight.

"I realised I had been sent to my death by Isis," a former fighter says in a video. "I was a victim. Apart from many other things I feel deceived."

More than 300,000 people watched the videos within two months. The playlists were clicked on almost four times more frequently than a regular ad campaign. Viewers watched more than 1.5m minutes of the videos. "That suggests a significant impact," says Ms Green.

Social media companies clearly have an incentive to promote counter- speech: governments are threatening the very openness that their users treasure, unless they are seen to be fighting terrorism on their platforms. But individuals such as Mr Arshad -- the people governments and social media groups hope can be the drivers of counter-speech online -- do not come with a bigger agenda.

"I'm not a politician, I don't want to pick a side," Mr Arshad says after the Kingston College show. "I just wanted kids to stop blowing themselves up."

The Hill

US denies asking Ecuador to cut off Internet to WikiLeaks
Tuesday, 18 October 2016
Byline: Katie Bo Williams

Washington - The State Department is emphatically denying that it asked the Ecuadorian Embassy in London to disconnect Julian Assange's internet connection to prevent more leaks of information about Democratic presidential nominee Hillary Clinton.
"While our concerns about WikiLeaks are longstanding, any suggestion that Secretary [John] Kerry of the State Department were involved in shutting down WikiLeaks is false. Reports that Secretary Kerry had conversations with Ecuadorian officials about this are simply untrue. Period," State Department spokesman John Kirby said.

Earlier Tuesday, WikiLeaks tweeted, "Multiple US sources tell us John Kerry asked Ecuador to stop Assange from publishing Clinton docs during FARC peace negotiations," referring to the Marxist rebel group in Colombia.

"The John Kerry private meeting with Ecuador was made on the sidelines of the negotiations which took place pricipally [sic] on Sep 26 in Colombia," WikiLeaks tweeted.

FARC signed a historic peace deal with the Colombian government on Sept. 26, which Colombian voters narrowly rejected in a referendum vote that has left the future of the peace process uncertain. Kerry was involved in the two-year negotiations over the deal.

Assange's internet was disconnected on Saturday, according to WikiLeaks. The anti- secrecy platform has been publishing daily batches of emails stolen from Clinton campaign manager John Podesta's email account. It has continued to do so even after Assange's claim of losing Internet access.

While Ecuador is aligned with the left-wing wave that dominated South American politics in the 2000s, Colombia is the United States's closest ally in the region.

Ecuador is reaffirming its decision to provide protection to the WikiLeaks founder, who has lived in the embassy in London since 2012.

"Faced with speculation of the last hours, the government of Ecuador reaffirms the validity of granted asylum to Julian Assange four years ago," the government said in a short statement on Twitter. "We reaffirm that the protection of the Ecuadorian state will continue while the circumstances that led to the granting of the asylum remain."

Assange is avoiding a rape charge in Sweden that he claims is political and will lead to his extradition to the U.S. over previous leaks.

The U.S. has not issued an indictment against Assange, despite widespread outrage after WikiLeaks published thousands of diplomatic cables leaked by former Army Pvt. Chelsea Manning.

The Ecuadorian Embassy did not address Assange's access to the internet.

Wired (UK)
Keeping Britain safe: how GCHQ's new cyber security agency will protect us from hackers
Tuesday, 18 October 2016
Byline: Matthew Reynolds

London - The Doughnut - GCHQ's vast, Cheltenham-based nerve centre - is a building straight from the pages of a spy novel. Its imposing circular walls are surrounded by fences topped with razor wire and multiple vehicle checkpoints. Visitors are seldom allowed inside the building which, Edward Snowdon's NSA leaks, is the centre of government mass surveillance in the UK.
The intelligence agency's latest spin-off, the National Cyber Security Centre, couldn't look more different. Occupying two floors of a commercial office block in Victoria, London, the NCSC is shedding its parent agency's secretive persona in favour of a more collaborative approach. There's even going to be a Shake Shack on the ground floor.

"NCSC as an organisation is going to be open by default," says Ian Levy, the NCSC's technical director. The fledgling agency only opened its doors on October 3, but it's already started its task of keeping the public and the UK's critical national infrastructure safe from cyberattacks launched by states, organised crime gangs and lone-wolf hackers.

For Levy, partnerships with the UK's cyber security community will be key to keeping the country safe online. To this end, 20 per cent of the new building has already been set aside for collaborative working. "We don't know what that means yet, but we know that you won't have to have a top secret security clearance to sit there," he says. "You coming to see me in the NCSC will be about as much of a ballache as me coming to see you."

Announced by then-chancellor George Osborne in November 2015, the NSCS is the first government agency devoted solely to cyber security. It will be responsible for keeping the public and private sectors informed about emerging cyber threats and making sure they are protected against an ever-growing number of cyber attackers. Heading up the NCSC is Ciaran Martin, former director general cyber at GCHQ.

High-profile hacks have barely left the headlines in 2016. In April, 11.5 million confidential documents taken from Panamanian law firm Mossack Fonseca were leaked to German press, sparking a chain of public protestations that eventually led to the resignation of the Icelandic Prime Minister, Sigmundur Davíð Gunnlaugsson. In July, almost 20,000 confidential emails sent by the Democratic National

Committee were published by WikiLeaks after a cyber attack for which the US Department of Homeland Security pinned the blame on the Russian government.

For Levy, however, all hacks can be boiled down to a software problem - and software vulnerabilities can always be fixed if they're caught soon enough. "If you actually look at what [hackers] do, very few of them - a vanishingly small number of them - are actually using advanced techniques," he says. "A lot of the attackers we see, including nation states, are using vulnerabilities from five years ago." Instead of worrying about who exactly the attackers are, Levy wants his agency to get on with managing the impact that their attacks could have.

"If we work together we can fix a lot of this stuff at scale," says Levy. One of the NCSC's starting points will be cracking down on fake emails and phishing scams which cost the UK public £174 million in 2015 alone. For over fifteen years the government has told citizens not to click on suspicious links, or open mail from senders they don't recognise, but, Levy says "as a piece of advice that's pretty dumb." There's no way to make sure people understand or act on that information and as malicious spam has gotten more frequent and sophisticated, this well-meaning advice has hardly made a dent in the growing number of people becoming victims of online fraud.

So the NCSC has decided to do something about it. Dmarc, which stands for domain-based message authentication, reporting and conformance, allows domain owners to set tight controls over what kinds of emails are sent from their own addresses, with the intention of cutting out on malicious emails that appear to originate from official organisations. Just one day after applying dmarc to the domain .gov.uk, the number of fake emails sent from @gov.uk tumbled by 50,000. "We're going to make government use dmark on every single government domain," Levy says. "And everything we say industry should do we're going to do to government first."

The NCSC will set cyber security standards for UK industry and business, but governmental departments are going to become critical testing grounds where, as with dmarc, cyber security innovations are tried and tested before being recommended to the country at large. "The NCSC doesn't run on hype. It runs on data. Everything we do we want to be able to generate data from it," Levy says. "And by default we're going to publish all that data."

Open data and collaborative working are unlikely to be the first phrases that spring to mind when people are asked to think about GCHQ, but, Levy points out, if his agency is to become the leading authority in UK cyber security, it has to start building public trust sooner rather than later. "The way of doing that is by being transparent and honest," Levy says. Part of that process will mean drawing a line in the sand between GCHQ and the NCSC. "Don't judge us on the way that we've been as our precursor organisations, as part of CESG, GCHQ, CPNI and MI5," Levy says.

For most of the past three decades or so, the damage caused by cyber attacks has mostly been limited to reputations and wallets. They've brought national infrastructure to its knees, exposed government atrocities and embarrassed CEOs of countless companies, but they've seldom - if ever - killed someone.

But imagine if, in the future, the software within one driverless car - or ten million driverless cars - was hacked so that its brakes no longer functioned above a certain speed. The FBI has already warned car owners about the risks of car-hacking, and it's entirely possible that in the future cyber attackers will be going after a lot more than just our data.

The biggest battle for the NCSC, then, might not be against attackers themselves, but the fear they create which limits how ready people are to accept new technologies. "If you're going to take machine learning and AI and have these things make decisions for you, the public need to be much more confident in their understanding of security," Levy says, "you're not going to do that with the fear that's currently out there."

ITAR-TASS World Service
Moscow says still no evidence from US proving alleged Russian hacker attacks
Tuesday, 18 October 2016
Byline: Staff report

Moscow - Moscow has received no evidence from the United States proving Russia's alleged hacker attacks on US institutions, Russian Foreign Ministry Spokeswoman Maria Zakharova said on Tuesday. "There have been no proof, do data, no passwords, no hyperlinks. Nothing," she said.

Washington's inability to provide any proof can only mean that such allegations target domestic audience and are part of the presidential campaign, she said, adding that attempts at reducing the presidential campaign to accusations against Russia are inglorious for a great power. "It is a global disgrace," she said.

Earlier WikiLeaks released on its website hacked emails from the Democratic National Committee. Hillary Clinton accused Russian hackers. US Director of National Intelligence James Clapper also suggested Russia was behind the hacks. Kremlin has repeatedly denied accusations.

National Post
Heeding the cyber-threat
Thursday, 20 October 2016
Section: editorial

A U.S. think tank recently suggested that North Korea could have enough material to produce up to 100 nuclear warheads by 2020. Rand Corp. says the country can already deliver nuclear weapons by aircraft or ship, and is testing missiles able to reach targets in Canada or the U.S.
It's a frightening prospect. Rand is taken seriously enough in Washington to be awarded a recent $509-million Homeland Security contract to bolster anti- terrorism activities. But you would search in vain for a serious discussion of the threat amid the avalanche of talk on the U.S. campaign trail. The Obama administration, which Democratic presidential candidate Hillary Clinton served in as secretary of state, has taken a largely hands-off approach, urging China to use its influence on North Korea's erratic dictator, Kim Jong-un. Republican presidential candidate Donald Trump has employed his usual shallow bluster, claiming, "There's a 10 per cent or 20 per cent chance I could talk him out of having his damn nukes, because who the hell wants him to have nukes?" The absence of sober debate is unfortunately typical of a political culture that pays too little attention to transformative geopolitical threats and too much to reality-TV spats and trendy activist preoccupations.

The U.S. government has been busy on the North Korean nuclear file for decades, including striking a deal under president Bill Clinton that helped win Jimmy Carter a Nobel peace prize. But other than prizes, it has little to show for its efforts. Pyongyang may be a greater threat to peace today than it has ever been, to the point Rand also warns both Japan and South Korea are "losing faith in the U.S. nuclear umbrella" and pondering programs of their own.

It is not widely appreciated how seriously cyber-attacks and rogue nuclear states threaten global stability. To call the modern world highly dependent on computer networks is a drastic understatement. Yet even at the highest levels, security is far from adequate.

The Pentagon has suffered major cyber-security breaches, as have top administration officials, the Internal Revenue Service, the Central Intelligence Agency director and even the National Security Agency, to say nothing of major banks, retailers and Internet giants like Yahoo, plus the Democratic National Committee. It has become increasingly evident that someone - whether a foreign power or rogue institution - is doing its best to interfere in the U.S. election. Yet the fact that Hillary Clinton is likely to be elected president after illegally using an insecure private email server while secretary of state tells you the issue it still not the priority it should be in the halls of power.

Without electronic communications, our power grid and food distribution systems would collapse in a matter of days. Even routine household dealings would be quickly paralyzed without email or electronic banking. A determined cyber-attack could shut down power plants, while a few wellplaced nuclear warheads could, by creating electromagnetic pulses, devastate computer networks over hundreds of kilometres and fry the electronics in our vehicles in the process.

It is astonishing how blithely we have disregarded massive evidence that the Internet is desperately insecure. Security breaches are treated more as a temporary nuisance, rather than evidence that the underpinnings of personal privacy, economic reliability and national safety are under a threat that can be resisted only as long as cyberdefences can stay one step ahead of cyber-attackers.

As has often been observed, politics is in danger of becoming just another arm of entertainment, able to hold the people's attention as long as it can keep them amused and diverted. Never has that been more so than in recent elections, in Canada and the U.S. alike, where optics, social media and the personalities of the candidates command far more attention than the vital matters for which the winner will be responsible. Every issue that arises during an election is important to someone, but progress is much more difficult in a society unable to guarantee its security and the basic infrastructure that keeps democracy in working order. Ours is a society that is easily distracted, and we are in danger of being distracted from the thing that matters most: the defence of the country and culture we've built, and which is the first responsibility of the people we elect.

Globe and Mail
Is your company's IT prepared for an attack by ransomware?
Thursday, 20 October 2016
Byline: Michael J. Armstrong and Tejaswini (Teju) Herath

Op-ed: October is Cyber Security Awareness Month and started with tantalizing reports that Internet giant Yahoo was secretly searching customer e-mails on behalf of American spy agencies.
But in recent press releases from the FBI, Ontario Provincial Police and Interpol, it is the soaring frequency and sophistication of ransomware that is highlighted.

Typical hackers obtain their illgotten gains by stealing valuable data such as credit-card numbers or passwords. They then find customers to buy that data.

Ransomware hackers instead sell data back to the owners. If ransomware infects your computer, it encrypts your files to render them inaccessible until you pay a ransom. This simplifies cybercrime by replacing theft with extortion.

This summer, ransomware forced the University of Calgary to pay $20,000 to unlock its employee e-mail system. And last month, a U.K. software services provider reportedly paid $31,500 to decrypt one of its servers.

Since CryptoLocker, a program that targets computers using Microsoft Windows, first appeared in 2013, ransomware attacks have soared. Cybersecurity firm Kaspersky Lab found ransomware on 50,000 corporate computers in 2015, double that of 2014.

The FBI estimated more than $209-million was paid in U.S. ransoms in the first three months of 2016, versus only $25million for all of 2015. Check Point Software reported a 30per-cent increase in ransomware attempts in August alone.

A survey of 540 international firms conducted this summer by Osterman Research on behalf of anti-ransomware provider Malwarebytes found that nearly 40 per cent had paid ransomware in the previous year.

About 37 per cent of ransom demands fell between $1,000 and $10,000, and 25 per cent exceeded $10,000. Canadian managers apparently felt the most confident about countering ransomware; but once infected, Canadian firms were three times more likely to pay the ransom.

Ransomware's sophistication is growing alongside its frequency.

Ransomware "worms" such as ZCryptor can spread themselves across networks, rather than needing a ride on infected e-mails.

Some ransomware specialists are selling their services to organised crime. This crime-as- aservice business model allows criminals to outsource their technology needs.

What might come next? Imagine ransomware combining with state- sponsored hacking. Host countries might give, or sell, permission for ransomware hackers to attack rival countries' computers. These cyberprivateers could plunder commerce abroad, without the host country's direct involvement. Think of regional rivals like Israel and Iran, or North and South Korea.

The Internet of Things might expose physical targets to ransoming. Control systems for factories and utilities are increasingly online. What if ransomware locked them out? If businesses begrudgingly pay thousands to recover e-mails, imagine what they'd pay to restart assembly lines.

Or how about virtual protection rackets? Instead of one-time ransoms to remove encryption, users might be "convinced" to pay ongoing fees for the "service" of avoiding encryption.

To defend themselves, computer users need to do the basics.

Run antivirus programs to detect threats. Keep operating systems and applications updated. Think before clicking on unexpected e-mail attachments.

Users should also backup files regularly. If ransomware strikes, backups allow ransom-free system recovery. But keep them on removable drives, to prevent their infection too.

Infected users can also try decrypting files with tools from sites like NoMoreRansom.org.

But these might work only on the simplest cases.

Software makers should do more to facilitate these safecomputing practices. For example, Windows now offers selfupdating antivirus protection by default. That's great, but unfortunately the system also makes it harder to create backups on removable drives.

Business insurers could also play a role by requiring that corporate systems be updated and backed-up to qualify for coverage.

Because ransomware ignores borders, law enforcement needs to co-operate across jurisdictions. Last month's InterpolEuropol Cybercrime conference was a good step in this direction.

If foreign hackers can effectively "tax" domestic businesses, ransomware will become a national security issue. So governments may need to negotiate agreements similar to those covering seaborne piracy.

Finally, firms might consider keeping key systems physically disconnected from the Internet, as some military computers always have been. Just because anything can be online doesn't mean everything should be.

Remember, there are all kinds of yahoos out there.

Michael J. Armstrong and Tejaswini (Teju) Herath are associate professors in the Goodman School of Business at Brock University.

CBC News
Government falling behind in clearing Phoenix payroll backlog by Oct. 31 deadline
Thursday, 20 October 2016
Byline: Chloé Fedio

Ottawa - The federal government all but confirmed it will not meet its self-imposed Oct. 31 deadline to deal with a backlog of Phoenix payroll issues despite doubling down on the promise just two weeks ago. Marie Lemay, the deputy minister in charge of the file, said the government is "tracking a bit behind," with 30,000 out of more than 80,000 cases still unresolved with less than two weeks to the deadline.

Lemay said the "bulk" will be cleared in time but that some of the most complex cases -- those requiring "time-consuming, manual calculations" -- might not.

"We're still driving for the 31st. We're going to give it our best shot," she said during a Wednesday afternoon update on the payroll mess. "We continue to make progress but we still have much work to do."

When the Phoenix payroll system was introduced across the country, employees began reporting problems. The government acknowledged in July that more than 80,000 public servants had reported trouble with their pay, with the majority being underpaid. Others were overpaid or not paid at all.

Some cases "date back several years" and require more research, said Lemay.

"It is important to note that we're focused on speed, as well as care. We must make sure that we're not creating new problems by solving old ones."

The government's deadline is for dealing with the cases filed by federal workers before June -- not new cases filed later.

The government has also committed to dealing with new, high priority cases within two weeks of a claims, and new priority cases within six weeks of the claims.

849 new priority cases

When the Phoenix payroll system was introduced across the country, employees began reporting problems. The government acknowledged in July that more than 80,000 public servants had reported trouble with their pay, with the majority being underpaid. Others were overpaid or not paid at all.

Lemay said during the last update on Oct. 5 that the government had resolved 38,228 cases and was "on target" to meet the Oct. 31 deadline. On Wednesday, she said an additional 12,824 cases had been resolved, for a total of more than 51,000 cases closed.

Since the last update on Oct. 5, Lemay said there have been 894 new priority cases. Those cases were prompted by employees going on maternity or parental leave, or employees leaving the public service.

"The majority of these employees are still receiving their salary but have yet to be transitioned to employment insurance or pension," she said, adding that these priority cases would be addressed within six weeks.

There have also been 79 new cases that are not considered high priority -- all of which have been resolved or will be resolved by the next pay period, she said.

Wednesday's technical briefing is the first since Rosanna Di Paola, the bureaucrat who oversaw the Phoenix pay system for years, was shuffled into another role at Public Services and Procurement Canada.

Lemay said Di Paolo has "worked diligently to launch Phoenix over the last three years," and remains a member of her executive team.

Ottawa Citizen
Government payroll woes likely not fixed by Oct. 31
Thursday, 20 October 2016
Byline: Kathryn May

Public Services and Procurement Canada will likely miss its promised Oct. 31 deadline to clear the backlog of pay problems caused by the federal government's bungled Phoenix payroll system, says the department's top bureaucrat.
Deputy Minister Marie Lemay confirmed Wednesday the department will have problems meeting the target because the remaining cases are older and more complicated than the front end of the pile and require more manual inputting and updating of information than originally expected.

She said the department is "driving" to clear the backlog but is braced for about 15,000 cases to remain after the deadline. As of Wednesday, the department had resolved the pay problems of about 62 per cent of the people caught in the backlog, which began with 82,000 cases.

"We are still driving for the 31st," Lemay said. "We're going to give it our best shot but ... the transactions in there are complex ones, so what we see that might happen is we might be left on the 31st with a number of transactions of the same nature, very complex."

The pay centre in Miramichi, N.B., already had a backlog of 40,000 cases when the government decided to go live with the first Phoenix rollout in February. Lemay was unable to say how many of the remaining cases came from that pre-Phoenix backlog.

The Oct. 31 deadline was the date Public Services had hoped to start the transition to what it calls a "steady state," with the bugs worked out and Phoenix running smoothly.

On the last payday - two weeks ago - Lemay insisted: "We believe we are on target and will clear the backlog by Oct. 31."

On Wednesday, however, she admitted she had no idea when Phoenix would be working "flawlessly" or operating in what she calls the steady state.

Public Services Minister Judy Foote said she is disappointed about the missed deadline but is "contented" with the work that has been done.

She said the government will keep the more than 200 compensation advisers hired to clear the backlog until "all issues" around Phoenix are resolved.

"The fact we have the majority of cases taken care of is good news. But I know there are still some people facing hardships and that bothers me. But we are going to continue to work hard to clear up the entire backlog."

Lemay said only about 30 per cent of transactions are now being handled within the service standards set by the department. She said the department had 79 new cases on Wednesday of public servants who did not get paid as they should have been.

They are the government's priority and will be paid before the next payday, Lemay said.

She said the number of people facing problems linked to leave jumped dramatically this week to 894, largely because of a surge in the number of people going on maternity and paternity leave. Their problems should be addressed within six weeks, she said.

Federal unions have increasingly voiced skepticism about meeting the Oct. 31 target, accusing the department of "playing with numbers."

The government's commitment only included the cases of the 46 departments, covering about 191,000 employees, that sent their pay transactions for processing at the pay centre in Miramichi by the end of June.

The other 55 departments manage their own compensation with in-house pay advisers but have also faced Phoenix glitches. It's unclear how many of these cases are outstanding or when their problems will be fixed.

Debi Daviau, president of the Professional Institute of the Public Service of Canada, said she believes the backlog is much bigger than 82,000 cases that accumulated by the end of June. She said new cases sent to Miramichi since July have problems, too, but they are sitting in a queue and are not considered part of the backlog.

"There is whole other backlog going on there that no one knows anything about," Daviau said.

Daviau said some of her members have complained their cases are being partially resolved, which takes then offthe backlog. The remaining problems have to be refiled and are handled as new cases.

The Phoenix pay system was rolled out to 300,000 public servants working in 101 departments and agencies, in two waves: one in February, the second in April. From the start, employees began reporting problems, which the government downplayed until July, when it acknowledged that thousands of employees had had problems.

Public Services opened a temporary pay centre in Gatineau, a new call centre and several other offices, and recruited more than 200 temporary pay advisers to clear the backlog.

Globe and Mail
Phoenix pay backlog likely won't be fixed this month
Thursday, 20 October 2016
Byline: Michelle Zilio

The federal government is warning that it is probably going to miss its self-imposed Oct. 31 deadline to resolve all problems related to its new Phoenix payroll system, leaving a potential 15,000 public servants waiting for compensation.
Marie Lemay, deputy minister of Public Services and Procurement Canada, said more than 51,000 of about 80,000 cases - or 62 per cent - had been cleared as of Wednesday.

"We are tracking a bit behind our projected schedule," Ms. Lemay told reporters at a technical briefing in Ottawa. "This is because of the complexity of the files that we're currently handling. Increasingly, we're seeing that many of the cases left in the backlog are very complicated and require time-consuming manual calculations."

Ms. Lemay said there could be as many as 15,000 outstanding cases after Oct. 31, some of which date back several years, before Phoenix was even in place. She said those cases should be resolved within one to two pay periods after the original deadline.

The Public Service Alliance of Canada (PSAC) said it saw this problem coming back in the summer.

"When they came out and said, 'Oh yeah, we're going to do this by Oct. 31,' we knew back in July that wasn't realistic," PSAC vice-president Chris Aylward said. "I believe we're going to talk about this well into 2017."

The government imposed the Oct. 31 deadline on itself in July, when it was revealed that nearly a third of the 300,000 public servants paid through Phoenix had experienced pay problems since the system went into operation in February. More cases have continued to emerge since then.

On Wednesday, Ms. Lemay said 79 new cases of public servants who did not get paid properly have come up in the past two weeks; she said those individuals will be paid by the next payday at the latest. Another 894 people facing pay problems related to leave also came forward. Ms. Lemay said those cases should be resolved within six weeks.

Ms. Lemay said any pay problems beyond Oct. 31 will probably concern public servants waiting for supplementary pay, such as acting pay and overtime.

She assured public servants that government compensation advisers are working tirelessly to reach the deadline.

In addition to the central pay centre in Miramichi, N.B., the government has opened temporary pay offices in Gatineau, Montreal, Shawinigan, Que., and Winnipeg, as well as a Toronto call centre where employees "triage" calls from public servants. Ms. Lemay said all of the staff at the temporary centres will remain in place until the government reaches a "steady state" where Phoenix is running smoothly.

In the meantime, the Treasury Board has opened a claims office to handle the reimbursement of out-of-pocket expenses, such as late-payment fees, incurred by public servants as a result of Phoenix pay problems. Alfred Tsang, who heads up the office, said that 92 applications for reimbursement had been received as of last Friday, including 20 requests amounting to more than $500 each.

Ms. Lemay said the price tag to fix the Phoenix system is set to ring in at about $50-million, excluding the costs associated with reimbursement for out-ofpocket expenses.

Jerusalem Post
South Korea mulls leasing Israeli spy satellite
Thursday, 20 October 2016
Byline: Yossi Melman

Jerusalem - South Korea is considering leasing an Israeli spy satellite, according to South Korean news agency Yonhap.
According to the report, South Korea is interested in becoming independent in space, rather than being dependent on American spy satellites.

The possibility of leasing an Israeli spy satellite is being considered as tensions have risen on the Korean peninsula due to North Korea's accelerated development of missiles and its threats to use nuclear weapons.

The development also suggests that South Korea does not completely trust that the US will provide the defense it has promised in the event of a military conflict. The Unites States and South Korea have a defense pact.

The possible leasing of a spy satellite is part of South Korea's effort to upgrade its military capabilities. This desire has also seen South Korea mull the purchase of German air-to-air missiles with which to arm its American F-15 fighter jets.

Sources in the South Korean Defense Ministry further stated that the possible lease of an Israeli spy satellite stems from delays in plans to develop a domestically produced satellite. According to the original plan, South Korea was supposed to have produced five satellites, but those plans have been pushed back to 2020 and are slated to be completed in 2023. The Israeli spy satellite would be a temporary solution until that time.

Israel currently has three Ofek spy satellites in space, produced by Israel Aerospace Industries (IAI). The last of these was launched just a few weeks ago and it was originally reported that there were some malfunctions, however, there have not been any further official reports on its status since then.

The Yonhap report did not clarify if South Korea wishes to lease an Israeli spy satellite that is already deployed to space or to ask the IAI to build a new satellite specifically for its needs.

If South Korea does indeed lease an Israeli spy satellite, it will give momentum to Israel's space program, which has been in a mild crisis since the communications satellite Amos blew up during launch in the US last month.

Wall Street Journal
Hackers Evolve to Serve the Kremlin
Thursday, 20 October 2016
Byline: Multiple reporters

Moscow - With the hacking of Hillary Clinton's campaign and the Democratic National Committee, U.S. officials say Russia has unleashed a strengthened cyberwarfare weapon to sow uncertainty about the U.S. democratic process.
In doing so, Russia has transformed state-sponsored hackers known as Fancy Bear and Cozy Bear from internet spies to political tools with the power to target the country's adversaries, U.S. officials and cybersecurity experts say.

The attacks are the harder side of parallel campaigns in the Kremlin's English-language media, which broadcast negative news about Western institutions and alliances and focus on issues that demonstrate or stoke instability in the West, such as Brexit. Moscow seeks particularly to weaken the North Atlantic Treaty Organization, which has expanded its defense against Russia.

"The underlying philosophy of a lot of these attacks is about establishing information as a weapon," said Alexander Klimburg, a cyber expert at the Hague Center for Strategic Studies. "Hacking for them is literally about controlling information."

President Vladimir Putin denies Russian involvement in the hacking, but in a way that telegraphs glee about the potential chaos being sown in the U.S. democratic process.

"Everyone is talking about who did it, but is it so important who did it?" Mr. Putin said. "What is important is the content of this information."

Former Central Intelligence Agency Director Michael Hayden said the Kremlin doesn't appear to be trying to influence the election's outcome, noting Russian involvement has provided fodder for both Republicans and Democrats. "They are not trying to pick a winner," he said on Tuesday at a

cybersecurity conference in Washington. Rather, Russia is likely unleashing the emails "to mess with our heads."

Pro-Kremlin commentators in Russia have seized on the DNC leaks to cast doubt on the American democratic process and argue that Washington has no right to criticize Moscow. They have said the hacked DNC emails, which showed party officials working to undermine primary runner-up Bernie Sanders, prove Americans are hypocritical when they malign Mr. Putin's authoritarianism.

The White House has threatened a "proportional response" against Russia.

Retaliating against murky cyberattackers is uncertain new territory, Western officials said. The group often called Fancy Bear has been active since at least 2007 or 2008, experts say. Multiple security companies have given the group different code names including Pawn Storm, Sofacy and APT 28, which denotes an "advanced persistent threat."

Another group, known as Cozy Bear or APT 29, has taken a lower profile, often targeting higher-profile individuals and uses more sophisticated tools to cover its tracks, cybersecurity experts said. It was active as early as 2008 and 2009, with targets related to Chechnya, a U.S.- based think tank and government institutions in Poland and the Czech Republic, according to security firm F-Secure Corp.

The methods are well known: Hackers trick targets into providing account information or downloading infected files through expertly faked emails and webpages, a tactic known as spear-phishing.

The link to Russia's security apparatus is based in part on technical clues. The two groups' malware is deemed too sophisticated for most criminal gangs.

Yet it is the groups' selection of targets that offers the most compelling evidence of Russian involvement, cybersecurity experts say.

"This all adds up to a strong indication of Russian sponsorship," said Laura Galante, director of global intelligence at U.S.-based security firm FireEye Inc. and a former Russia specialist at the U.S. Department of Defense. "The Russian government has very publicly stated its desire to have ability in this realm. They want the ability to shape the way people think about events."

Politico
Media vulnerable to Election Night cyber attack
Wednesday, 19 October 2016
Byline: Darren Samuelsohn, Hadas Gold

Washington - Despite spending hundreds of millions of dollars on security upgrades, U.S. media organizations have failed to properly protect their newsrooms from cyberattacks on their websites,

communications systems and even editing platforms -- opening themselves up to the possibility of a chaos-creating hack around Election Day.
In just the past month, BuzzFeed has been vandalized, and both Newsweek and a leading cybersecurity blog were knocked offline after publishing articles that hackers apparently didn't appreciate. Federal law enforcement is investigating multiple attacks on news organizations, and journalists moderating the presidential debates say they've even gotten briefings from the FBI on proper cyber hygiene, prompting them to go back to paper and pens for prep work.

"We do a lot of printing out," said Michele Remillard, an executive producer at C-SPAN, the network home to the backup moderator for all the debates.

Journalists are seen as especially vulnerable soft targets for hackers. Their computers contain the kinds of notes, story ideas and high-powered contact lists coveted by foreign intelligence services. They also work in an environment that makes them ripe for attack, thanks to professional demands like the need for a constant online presence and inboxes that pop with emails from sources whom they don't always know and which frequently contain the kinds of suspicious links and attachments that can expose their wider newsroom networks.

Senior U.S. officials, current and former lawmakers and cybersecurity pros told POLITICO the threat against the media is real -- and they fret the consequences. Specifically, the security community is worried The Associated Press' army of reporters could get hacked and the wire service -- the newsroom that produces the results data on which the entire media world relies -- inadvertently starts releasing manipulated election tallies or that cybercriminals penetrate CNN's internal networks and change Wolf Blitzer's teleprompter.

"It's the art of possible is what really scares me," said Tony Cole, chief technology officer of FireEye, a Silicon Valley-based cybersecurity firm that works with some of the country's major television and newspaper companies. "Everything is hackable."

"No site is safe," added Tucker Carlson, editor-in-chief of The Daily Caller. "If the federal government can be hacked, and the intelligence agencies have been hacked, as they've been then, can any news site say we have better cybersecurity than the FBI or Google?"

The media have long been a spy's best friend. Intelligence community sources say that foreign and U.S. agents use local newspapers to look for clues about their targets, and that strategy has only grown more sophisticated in an all-online era in which foreign intelligence is reportedly known to hover over a media company's servers searching for any kind of heads-up on relevant stories inching closer to publication. Reporters on the campaign trail and back in their home bureaus said in interviews that they've become increasingly aware of their status as potential hacking victims. The spate of recent attacks -- involving their sites and their competitors' -- are more than ample warning of what's possible. Several journalists said they now use email and other communication with the expectation they're being watched, and

under the assumption that their messages can and will be hacked and shared publicly with the wider world.

"We're a bigger target than the 7-Eleven down the street," said Mark Leibovich, chief national correspondent for The New York Times Magazine. "Presumably, we have really good, smart IT people who know what they're doing, who are taking all kinds of precautions, who are acutely in tune with what the risks are and what the threats are."

There is perhaps no greater target in election journalism than the AP, the venerable wire service that will have more than 5,000 reporters, editors and researchers working across the country, tabulating results, calling races and feeding a much wider network of subscribers. Often other news outlets refer to the AP before making calls on races, and AP projections on the East Coast can have effects on West Coast voting, which closes hours later thanks to the time differences. Multiple sources in media, government and the security industry fretted about the effect if the AP were to get hit, and what that would do to their ability to get the news out.

The AP will deploy reporters across the country to send up vote tallies, usually by phone, the wire service explained to The Washington Post in May. It also has multiple checks and balances in place to monitor for errors. But as with many other news organizations contacted by POLITICO, AP spokesman Paul Colford said the wire service's policy is to refrain from making public comments about its security measures.

"Given the extraordinary interest in the presidential election and thousands of other state and local contests, we would add that AP has been working diligently to ensure that vote counts will be gathered, vetted and delivered to our many customers on Nov. 8," he said.

Federal and state officials stress that even a successful hack on a major news outlet around Election Day would not affect the final results, which typically take weeks to certify. The vote tallies, after all, will be available on official sites and in many instances on special social media feeds. And if a news site did get defaced with incorrect information, the results would be more like a modern-day version of the famous 'Dewey Defeats Truman' headline that President Harry Truman triumphantly held aloft the day after his 1948 reelection.

Still, there is a widespread recognition -- from the White House down to the local precinct level -- that a hack on the media could be damaging given the role it plays in getting election news out to satisfy the country's insatiable information appetite. Misinformation circulated in the early hours of Nov. 8 about the race's trajectory, for example, could factor into a voter's decision to even show up during the election's final hours, especially in Western states. There's also concern that false media reports spread via a hacked news account could be a potential spark for violence in an already exceptionally charged atmosphere. On the flip side, there's a recognition that the media can help build public confidence in the final results, especially following a campaign that's been engulfed in its closing weeks by Russian-

sponsored hacking of the Democratic National Committee, the hacking of Hillary Clinton's campaign chairman's personal emails, and Donald Trump's unfounded charges of vote rigging.

"To the degree that foreign hackers could prevent the dissemination of good information around the election, that can be a problem," said Rep. Adam Schiff, the top Democrat on the House Intelligence Committee. The California congressman said he frets that media outlets, like many other industries, face "massive costs" in protecting themselves against cyberattacks with "no end in sight" to the potential risks. Schiff added that he is especially concerned about smaller news organizations without major IT budgets or the backing of larger parent companies. "They're much more vulnerable," he said.

Cybersecurity experts say media spending to protect news organizations against cyberattack has grown substantially in the past three years, especially in the wake of North Korea's attack on Sony Pictures in late 2014. The price tag for vulnerability audits and other techniques varies by the size of the newsroom and the surface area for potential attacks, but multiple sources said quarterly audits can easily cost $50,000 or more.

Cyber experts and media officials from newsrooms across the country said they're prepped to deal with a range of threats to their sites, including the kinds of malware that can infect a computer network and give hackers an entry point to manipulate a home site. They're also building backup capacity in the event of a DDoS attack, or distributed denial of service, that tries to overwhelm a website or server with fake traffic. News sites, they note, are already prepping for monster traffic around the election, which can surge as much as 30 times compared with other big events this cycle, such as a debate or primary.

At the staffing level, newsrooms have also been pushing for better cyber habits by hosting training seminars, requiring employees to take must-pass exams and requiring double-authentication before granting access to a newsroom's internal filing system and social media accounts.

But cyber experts warn that all the preparatory work in the world can matter little for a news organization if it's facing an attack from a more sophisticated actor.

"If all of a sudden your adversary becomes a nation-state, like Sony or the DNC with Russia, you see those kind of procedures aren't worth a darn," said Robert Anderson, a former senior FBI cyber official and a managing director at the Navigant consulting firm.

The press has indeed been a familiar target for hackers. In 2013, hackers hit the AP's Twitter account and posted a false report about a bombing at the White House, sending the stock market into a five-minute spiral. In more recent incidents, a USA Today columnist wrote an article in February admitting he was hacked midair while using his commercial flight's WiFi, and the New York Times reported in August that its Moscow bureau was targeted by what were believed to be Russian hackers.

Newsweek blamed hackers for a DDoS attack that took down its site last month soon after it published an article about Trump's company allegedly violating the U.S. embargo against Cuba through secret

business dealings in the 1990s. And BuzzFeed had several articles on its site altered earlier this month after it ran a story identifying a person allegedly involved in the hacking of tech CEOs and celebrities.

"I'm sure that lots of newsrooms are having this conversation right now, particularly as we get closer to the election and people have a lot more to lose when things don't go their way," said Brian Krebs, the cybersecurity blogger and former Washington Post reporter whose site went down last month after a major DDoS attack that he says was spawned by his reporting about the arrest of two Israeli hackers.

With the threat of hackings against the media reaching such a heightened pace, many election observers urged both reporters and the reading public to take a deep breath as the results start coming in.

"If Twitter is reporting that Jill Stein wins South Carolina, that should probably give you pause," said David Becker, executive director of the Center for Election Innovation and Research.

Associated Press
US, UK Cybersecurity Officials: Destructive Hacks Are Coming
Thursday, 20 October 2016
Byline: Staff report

London - The world should brace itself for more physically destructive hacks, two senior cybersecurity officials said Wednesday, warning that a more dangerous era of hacking was already upon us.
Paul Chichester, the director of operations at Britain's new National Cyber Security Center, told an event hosted by British defense think tank RUSI that electronic intrusions were on their way to becoming more "destructive, disruptive and coercive."

"That will be our future," he told a crowd of officers, academics and industry experts gathered for a two-day symposium in central London.

Chichester was seconded by Air Force Lt. Gen. James K. McLaughlin, deputy commander at U.S. Cyber Command, who told attendees that infrastructure-wrecking attacks were being seen "right now in the environment."

Neither official went into specifics about what they'd seen or why they felt the threat was intensifying, although McLaughlin invoked a cyberattack in Ukraine which knocked out three separate power distribution companies last year. The Dec. 23 incident, believed to have been pulled off by a team of hackers using stolen passwords, left 225,000 people without electricity, according to a U.S. Department of Homeland Security bulletin published two months later.

Cybersecurity experts long worried that hackers can hijack the vulnerable industrial control systems to wreak havoc in power plants, traffic systems, factories, dams or reservoirs. Still, publicly confirmed examples of real-world damage from hacking have -- so far -- been few and far between. The Ukrainian

incident provided a rare and dramatic demonstration of the physical consequences of a well-organized cyberattack.

McLaughlin said there was now no doubt such hacks were possible.

"Three years ago these were just theoretical," he said. "Now we see them. They're practically here in front of us."

New York Times
Trove of Stolen Data Is Said to Include Top-Secret U.S. Hacking Tools
Thursday, 20 October 2016
Byline: Multiple reporters

Washington - Investigators pursuing what they believe to be the largest case of mishandling classified documents in United States history have found that the huge trove of stolen documents in the possession of a National Security Agency contractor included top-secret N.S.A. hacking tools that two months ago were offered for sale on the internet.
They have been hunting for electronic clues that could link those cybertools -- computer code posted online for auction by an anonymous group calling itself the Shadow Brokers -- to the home computers of the contractor, Harold T. Martin III, who was arrested in late August on charges of theft of government property and mishandling of classified information.

But so far, the investigators have been frustrated in their attempt to prove that Mr. Martin deliberately leaked or sold the hacking tools to the Shadow Brokers or, alternatively, that someone hacked into his computer or otherwise took them without his knowledge. While they have found some forensic clues that he might be the source, the evidence is not conclusive, according to a dozen officials who have been involved in or have been briefed on the investigation.

All spoke on condition of anonymity because they were not authorized to discuss it publicly.

Mr. Martin, an enigmatic loner who according to acquaintances frequently expressed his excitement about his role in the growing realm of cyberwarfare, has insisted that he got in the habit of taking material home so he could improve his skills and be better at his job, according to these officials. He has explained how he took the classified material but denied having knowingly passed it to anyone else.

"As a contractor, he gets to see a slice of the overall picture," said one person familiar with the exchanges, summarizing Mr. Martin's explanation. "He wanted to see the overall picture so that he could be more effective."

The material the F.B.I. found in his possession added up to "many terabytes" of information, according to court papers, which would make it by far the largest unauthorized leak of classified material from the

classified sector. That volume dwarfs the hundreds of thousands of N.S.A. documents taken by Edward J. Snowden in 2013 and exceeds even the more voluminous Panama Papers, leaked records of offshore companies obtained by a German newspaper in 2015, which totaled 2.6 terabytes. One terabyte of data is equal to the contents of about one million books.

F.B.I. agents on the case, advised by N.S.A. technical experts, do not believe Mr. Martin is fully cooperating, the officials say. He has spoken mainly through his lawyers, James Wyda and Deborah Boardman of the federal public defender's office in Baltimore. They declined to comment before a detention hearing set for Friday in federal court.

In interviews, officials described how the Martin case has deeply shaken the secret world of intelligence, from the N.S.A.'s sprawling campus at Fort Meade, Md., to the White House. They expressed astonishment that Mr. Martin managed to take home such a vast collection of classified material over at least 16 years, undetected by security officers at his workplaces, including the N.S.A., the Office of the Director of National Intelligence and Pentagon offices. And they are deeply concerned that some of the mountain of material may, by whatever route, have reached hackers or hostile intelligence services.

Investigators discovered the hacking tools, consisting of computer code and instructions on how to use it, in the thousands of pages and dozens of computers and data storage devices that the F.B.I. seized during an Aug. 27 raid on Mr. Martin's modest house in suburban Glen Burnie, Md. More secret material was found in a shed in his yard and in his car, officials said.

The search came after the Shadow Brokers leak set off a panicked hunt at the N.S.A. Mr. Martin attracted the F.B.I.'s attention by posting something on the internet that was brought to the attention of the N.S.A. Whatever it was -- officials are not saying exactly what -- it finally set off an alarm.

The release of the N.S.A.'s hacking tools, even though they dated to 2013, is extraordinarily damaging, said Dave Aitel, a former agency employee who now runs Immunity Inc., an information security company.

"The damage from this release is huge, both to our ability to protect ourselves on the internet and our ability to provide intelligence to policy makers and the military," Mr. Aitel said.

The N.S.A.'s hacking into other countries' networks can be for defensive purposes: By identifying rivals' own hacking methods, the agency can recognize and defend against them, he said. And other countries, with some of the N.S.A.'s tools now in hand, can study past hacks and identify the attacker as the N.S.A., learn how to block similar intrusions, or even decide to retaliate, Mr. Aitel said.

Mr. Martin, 51, a Navy veteran who was completing a Ph.D. in information systems at the University of Maryland, Baltimore County, has worked for several of the contracting companies that help staff the nation's security establishment. After stints at the Computer Sciences Corporation and Tenacity Solutions, where he was assigned to the Office of the Director of National Intelligence, he joined Booz

Allen Hamilton in 2009. He worked on that firm's N.S.A. contract until 2015, when he was moved to a different Pentagon contract in the area of offensive cyberwarfare.

He has long held a high-level clearance and for a time worked with the N.S.A.'s premiere hacking unit, called Tailored Access Operations, which breaks into the computer networks of foreign countries and which developed the hacking tools later obtained by the Shadow Brokers. According to one person briefed on the investigation, Mr. Martin was able to obtain some of the hacking tools by accessing a digital library of such material at the N.S.A.

One possibility investigators are considering is that Mr. Martin did not knowingly share the Shadow Brokers material but that it was physically stolen from him -- conceivable given the descriptions of the chaos of his house, shed and car -- or more likely, grabbed by hackers. But the forensic examination of Mr. Martin's computers has so far turned up no evidence that he was hacked, officials say.

At the core of the investigation, if Mr. Martin deliberately shared the secret N.S.A. tools, is the mystery of his motive. People who know him call him deeply patriotic and say they do not believe he would have given classified information to another country. They also say he has never been interested in politics, making unlikely a politically motivated leak like that of Mr. Snowden, who thought the N.S.A. was violating Americans' privacy.

The F.B.I. is considering whether he might have sold the hacking tools or other materials for money. His annual salary in recent years has exceeded $100,000 and he owns his house without a mortgage. But he has long bought expensive suits and Rolex watches, according to an old acquaintance, and a person familiar with his finances says he has struggled with debt. Court records show one past lien, an $8,997 state tax bill imposed in 2000 and not paid off until 2014.

Some people who know Mr. Martin favor a psychological motive for taking the documents home -- one that echoes what he is himself telling investigators: a drive to distinguish himself and prove that his computer knowledge was equal to that of the N.S.A.'s top operators.

"He always thought of himself like a James Bond-type person, wanting to save the world from computer evil," said a person who knows him well but would not speak about him on the record for fear of being pulled into the criminal case.

Last year, commenting online on an article on the future of computer warfare, Mr. Martin struck a martial and patriotic tone.

"The battles ahead will require a special breed of warrior," he wrote. "It's really a calling, and something the individual has to want to do as a profession, due to the sacrifices required to be top flight in this new, electronic, version of the great game."

Mr. Martin's tone of confidence reflected his comfort in the world of computer experts. Mr. Aitel, who runs a popular email list on computer security called Daily Dave, said Mr. Martin regularly emailed the list and him privately, usually expressing his enthusiasm for a technical achievement: "Outstanding! You rock!" he wrote about one exploit, Mr. Aitel said.

But Mr. Martin's online self-assurance, people who know him say, masked a timid, introverted personality. Though he could be warm and generous, he had few friends, was socially awkward and often seemed lost in his work and doctoral studies, these people said.

For years, Mr. Martin struggled with obesity, and then had gastric bypass surgery and lost a lot of weight, according to acquaintances who did not want to be named because they also did not want to drawn into the investigation. But within a decade, he had gained most of it back, they said.

Not long before his arrest, Mr. Martin exchanged emails with Mr. Aitel about attending Mr. Aitel's annual security conference, called Infiltrate, scheduled for April in Miami.

"He sounded completely normal," Mr. Aitel said. "Making plans for the future."

New York Times
How Donald Trump Hacked the Politics of Foreign Policy
Wednesday, 19 October 2016
Byline: Max Fisher, Amanda Taub

New York - Donald J. Trump's foreign policy proposals, like forcing Mexico to pay for a border wall or withdrawing from NATO, have drawn unprecedented condemnations as incoherent, contradictory and unrealistic.
Yet for all the boos they elicit from experts, they draw frequent cheers at his rallies.

Scholars of American politics say this is because Mr. Trump, the Republican presidential nominee, is using international issues as a medium to connect with voters' gut-level fears and desires, an approach that works precisely because his foreign agenda falls far outside the mainstream.

As Mr. Trump and his Democratic opponent, Hillary Clinton, meet on Wednesday for their final debate, in which foreign policy is slated to be a main topic, a look at his wholesale reframing of this set of issues reveals much about Mr. Trump's improbable rise.

Studies show that most voters rank foreign issues low on their list of concerns, but they do listen and use those issues as a window through which they judge candidates' values and ideology.

Mr. Trump has exploited this dynamic, offering ideas that experts consider unworkable, but that tap into some voters' desire for a strong-handed leader. Foreign policy, some research suggests, provided an ideal medium for this message.

Typically, candidates cannot reach the national stage without first proving their fitness to certain institutions that care deeply about foreign policy: the news media that vets them, the parties that provide them with crucial support, the policy makers they will need once in office.

Because foreign policy is so complex and most voters do not follow its particulars as closely as they do domestic issues, those institutions play an outsize role in shaping the bounds of acceptable debate.

But Mr. Trump, a celebrity who largely self- financed his primary campaign, was able to bypass this process, hacking the politics of foreign policy to his considerable advantage -- and in ways that could outlast his candidacy.

A foreign policy not about foreign policy.

In a perfect world, each voter would dedicate months of study to the complexities of major global conflicts, evaluate the available options, then determine which candidate's plan best balances risks and rewards.

In the world we live in, voters choose whom to believe based on whose message feels truest.

"We have overwhelming evidence that voters don't know that much about the details of foreign policy," explained Elizabeth N. Saunders, a George Washington University political scientist.

"People tend to choose the candidate they like first," and then take on that candidate's views as their own, she added. "This is the way people make sense of a complicated world."

All candidates wrap their policy agendas in simpler values, such as strength or inclusiveness, or stories of heroes and villains, Professor Saunders said, "as a way of crafting a narrative that voters who don't follow the details can grab on to."

That is especially true for foreign policy, she said, because it is so complex.

Mr. Trump seems to have reversed this process, beginning with the narrative and values he wishes to convey, then designing policies to maximize his message's effect.

Because foreign policy requires difficult trade-offs, conventional candidates are limited in how emotionally appealing they can make their plans while keeping them workable. They also need to appease the hard-nosed policy experts or party officials those candidates rely on to get elected -- and, eventually, to govern. But Mr. Trump was under no such constraints.

The result: Mr. Trump's foreign policy is not a foreign policy at all, but rather a vessel for reaching voters on a purely ideological level.

The world according to Trump.

This explains how Mr. Trump has won support with, for example, threats to leave the North Atlantic Treaty Organization, though voters have expressed little interest in renegotiating the alliance and foreign policy professionals have warned it would risk disaster.

Paul Musgrave, a political science professor at the University of Massachusetts, summed up Mr. Trump's message: "NATO requires cooperation. Cooperation is something you do if you're weak. If you're strong, people go along with you."

As policy, that is dubious. But it is a powerful way for Mr. Trump to present himself as someone who will treat outsiders with suspicion and ruthlessly pursue economic gains. It is a message wrapped in foreign policy but meant to tap into more domestic concerns.

Colin Dueck, a George Mason University professor, wrote in a recent paper that Mr. Trump's worldview demands and offers "a sort of Fortress America, or perhaps a gigantic gated community, separated from transnational dangers of all kinds by a series of walls."

To voters "feeling displaced by long-term trends toward cultural and economic globalization," Professor Dueck wrote, Mr. Trump's policies promise "security, separation, and reassertion of control."

During the Republican primaries, for example, Mr. Trump alarmed those outside his rapidly growing base with proposals to kill the families of terrorists and with praise for President Vladimir V. Putin of Russia, as well as for China's 1989 crackdown in Tiananmen Square.

But for supporters, these and other statements suggested Mr. Trump could be trusted to impose order on the chaos they see in a rapidly changing world.

Because American voters have long approached international issues as a way to judge presidential candidates' values, they are willing to overlook the particulars; foreign policy became a powerful medium for Mr. Trump and his supporters to connect.

When Mr. Trump warns that the United States is getting swindled by the Iran nuclear deal or the North American Free Trade Agreement, he is speaking directly to a feeling among many Americans that they have been sold out by untrustworthy elites, that the game is rigged against them.

And when Mr. Trump promises to force Mexico to pay for a giant border wall or warns that Iranian boats will be "shot out of the water" if their sailors "make gestures" at American sailors, he is communicating

that he understands that his supporters feel fearful and humiliated, and that he will punish those responsible.

Promising order.

This message turned out to resonate with a surprisingly large audience -- but where did this seemingly new constituency come from?

Research published this spring by a group of social scientists, led by Brian C. Rathbun of the University of Southern California, suggests an answer: Mr. Trump has tapped into what scholars call conservation values.

People who hold those values prioritize security, conformity and tradition. They also tend to fear physical threats and people they see as outsiders, whether that means foreigners or those of different races or religions. And they often express those values as a particular set of "hawkish" foreign policy views.

That hawkishness is very different from that of neoconservatives like President George W. Bush or interventionist Democrats like Mrs. Clinton. It is characterized by a desire to shut out the world, ruthlessly promote American interests, reject cooperation and meet threats with overwhelming force.

The paper, though written before Mr. Trump's rise, details the worldview he would come to champion in surprising detail.

The distrust of cooperation shows up in Mr. Trump's call to stymie alliances from Europe to Asia. The instinct to impose order by force appears in his proposals for unchecked violence against the Islamic State. And the "America first" nationalism can be seen in his demand that the United States seize Iraq's oil.

Voters who hold conservation values are drawn to such policies not out of a sudden interest in global affairs, but as a way to express their fear of change and desire for order at home, the researchers found. They desire a strong leader who will protect "us" against an ever- more-menacing "them."

Mr. Trump, by redirecting voters' anxiety about demographic, cultural and economic changes toward foreign policy, gives his supporters a clearer set of villains -- and a promise to do whatever it will take to defeat them.

Supporters do not primarily hear a policy agenda, but a promise: that Mr. Trump understands their fears and will protect them.

Mr. Trump may never have a chance to test the experts' contention that his foreign policy proposals are unworkable. But the constituency he has surfaced and focused those policies on could demand them

from future candidates, risking a repeat of this year's campaign dynamic pitting the party establishment against its base.

Professor Saunders of George Washington pointed out that Republican leaders and Republican voters have diverged on foreign policy since Mr. Bush's 2003 invasion of Iraq.

Mr. Trump's legacy, she said, may be to widen those gaps.

The Guardian (London)
Snowden: 'Politics of fear' keep Trudeau from repealing Canada anti-terror law
Thursday, 20 October 2016
Byline: Ashifa Kassam

Toronto - Edward Snowden has waded into the simmering debate over Canada's controversial anti-terror law, saying that Justin Trudeau was reluctant to repeal the law out of a fear of appearing soft on terror.
Speaking to an audience in Toronto on Tuesday, Snowden pointed to a campaign promise by the Canadian prime minister to amend the sweeping legislation, which gives security forces heightened powers to apprehend suspected terrorists and disrupt their activities. "But he's been in office a little while now and we haven't seen that actually come to pass," said Snowden, appearing at the SecTor cybersecurity conference via videolink from Russia.

Bill C-51 was introduced in early 2015 by the country's then Conservative government, spawning protests across the country as it became law. Hundreds of thousands of Canadians, including legal scholars, civil liberties groups and pundits from across the political spectrum, spoke out against the law and its perceived attempt to supplant the country's democracy with a creeping police state.

Trudeau vowed to amend the "problematic elements" of the law, rather than simply repeal the legislation, noted Snowden. "Because he's afraid of being politically attacked on the basis of being soft on terrorism, regardless of whether or not this law actually helps prevent any terrorist attacks," he said. "This is just the way the politics of fear work."

Last month the Liberal government launched a wide-ranging consultation on national security, meaning any potential changes to the law will probably be delayed until next year. The extra time will offer the government the opportunity to get it right, said Ralph Goodale, Canada's public safety minister, as he announced the consultation. "A lot of people felt shut out, and we promised to give them the opportunity to be heard."

On Tuesday, Snowden suggested what he described as the minimum changes needed to the law, such as the creation of a judicial body that would carry out a case-by-case review of every individual exercise of

these powers. "And this means those individuals working in those spy agencies know simply that as long as they follow the law, they'll be fine," he said.

The law allows information on Canadians to be shared between more than a dozen federal institutions. "All the activities held in our private lives, our private records, are being used as a kind of currency to gain standing and status within this surveillance network," said Snowden. "We're being traded like baseball cards."

Any sharing of information - by those within Canada and with foreign agencies - that doesn't result in a trial or charges should be disclosed to individuals once a particular time frame has lapsed, he said, allowing people to ensure their rights have not been violated in any way.

Snowden also took aim at the law's vague and undefined language. "A lot of what classifies as terrorism in the political context - individuals that the news calls terrorist - are really common criminals," said Snowden. "But they do not constitute the kind of super criminal threat that is represented by our terrorism legislation."

He pointed to the obvious need for law enforcement to have the right tools to counter these threats. "But we do not want to sacrifice everything that makes our societies great," he said. "We do not want to reorder the boundaries of our rights for the convenience of law enforcement officials, if it's not truly necessary, if it means we lose everything that we're trying to defend."

New York Times
Czechs Arrest Man Wanted by the F.B.I. for Hacking
Thursday, 20 October 2016
Byline: Rick Lyman, Hana de Goeij

Prague - A man identified as a Russian hacker suspected of pursuing targets in the United States has been arrested in the Czech Republic, the police announced Tuesday evening.
The suspect was captured in a raid at a hotel in central Prague on Oct. 5, about 12 hours after the authorities heard that he was in the country, where he drove around in a luxury car with his girlfriend, according to the police. The man did not resist arrest, but he had medical problems and was briefly hospitalized, the police said in a statement.

David Schön, a police spokesman, said on Wednesday that the arrest of the man, whose name has not been released, was not announced immediately "for tactical reasons."

The police statement said that "the man was a Russian citizen suspected of hacking attacks on targets in the United States," and that the raid was conducted in collaboration with the F.B.I. after Interpol issued an arrest warrant for him.

The social media company LinkedIn said it believed it had been a victim in the case. The company, which acts as a virtual job network, said it had been actively involved in the F.B.I.'s case since it was hacked in 2012.

The F.B.I. said in a statement that the arrest was an example of the collaboration needed "to successfully defeat cyber adversaries," but declined to provide any further details.

The arrest occurred two days before the Obama administration formally accused the Russian government of stealing and disclosing emails from the Democratic National Committee and other institutions and prominent individuals.

But law enforcement officials in Washington, speaking on condition of anonymity because they were not authorized to comment while the investigation was underway, said Wednesday that the suspect did not appear to be related to the hacking of the Democrats' emails or to organizations like DCLeaks or WikiLeaks.

A judge in Prague has ordered the man to remain in custody, and a court will examine whether to extradite him to the United States.

The Russian Embassy in Prague called for the man to be released.

"We insist that the detained Russian citizen should be transferred to Russia," the state-run Russian news agency Tass quoted Aleksei Kolmakov, the embassy's spokesman, as saying.

Mr. Kolmakov said that the embassy had been notified about the detention, but that the Kremlin's spokesman, Dmitri S. Peskov, had told the news website RBK that it did not have details about the man's identity.

Jakub Janda, who studies the Russian government and is a deputy director of the European Values Think-Tank in Prague, said that the arrest served as confirmation that "the Czech Republic is so far considered a safe base for Russian intelligence and influence activities focused on Western targets."

He added, "Prague is unofficially considered to be a springboard for some Kremlin activities inside Europe, also using huge Russian diplomatic presence of approximately 140 staff."

Mr. Janda also said that the arrest showed that "Western governments are waking up and finally considering hostile Russian intelligence and disinformation operations to be an open and urgent threat, even at the level of the U.S. administration."

He added, "Open arrests of hostile individuals such as this one can serve as a deterrent element."

The United States director of national intelligence, James R. Clapper Jr., said in a statement on Oct. 7 that high-level Russian officials were trying to interfere with American elections.

"The recent disclosures of alleged hacked emails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts," Mr. Clapper said. "These thefts and disclosures are intended to interfere with the U.S. election process."

The antisecrecy organizations DCLeaks and WikiLeaks have been involved with the disclosures of illegally obtained emails from the hacked accounts of prominent figures including Colin L. Powell, the former secretary of state, and John D. Podesta, the chairman of Hillary Clinton's presidential campaign. Guccifer 2.0 is the assumed name of a Romanian "lone hacker" responsible for copying thousands of emails and other files from the Democratic committee, but experts are not certain if the hacker is a person or a front created by Russian intelligence officials.

It appears that the man arrested in Prague is not related to the hackers Mr. Clapper described.

Reuters
Microsoft to show code in Brazil to calm fears about spy 'back doors'
Thursday, 20 October 2016
Byline: Staff report

Brasilia - Microsoft Corp, still stung by accusations that it installed "back doors" for the U.S. government to access customers' communications, opened a center in Brazil on Wednesday where officials will be able to inspect its programming code, in an attempt to allay suspicions in the region that its software programs are vulnerable to spying.
Behind reinforced walls and with strict security settings, the world's biggest software company showed off its fourth 'Transparency Center' in Brasilia, where experts from Latin American and Caribbean governments will be able to view the source code of its products.

The effort to build trust follows heightened suspicions in the region after former U.S. National Security Agency contractor Edward Snowden leaked documents in 2013 that showed the agency was capturing massive amounts of data from emails handled by major U.S. technology companies, including Microsoft.

The leak, in addition to another Snowden disclosure that the United States had been spying on communications including those of former Brazilian President Dilma Rousseff, prompted Brazil and other governments around the world to reconsider how much they could trust U.S. technology companies not to install back doors at the request of U.S. intelligence agencies.

At the new site, visited on Wednesday by officials including the speaker of Brazil's Congress, no electronics will be allowed into the secure viewing room.

Microsoft prevents anyone from copying the massive amount of coding on display - as much as 50 million lines for its email and server products. Viewers inspect copies of source code on computers connected only to local servers and cut off from the internet. The copies are later deleted.

Viewers can use software tools to examine the code, Microsoft said, but it was not immediately clear whether experts would be able to run deep code analysis necessary to uncover back doors or other bugs.

It is by no means certain the effort by Microsoft will diminish concerns about spying, but Brazil's reaction to the generally secretive software company opening up its code was initially positive.

"This center is aimed at showing that there are no traps, it is a good step," a Brazilian government official, who asked not to be named because he was not authorized to speak about cyber security, told Reuters.

The Brasilia facility is Microsoft's fourth transparency center after the NSA scandal. It set up the first one at its Redmond, Washington headquarters in the United States in 2014, one in Brussels last year and one in Singapore earlier this month. It will soon open another in Beijing.

The centers allow for face-to-face discussions between government experts and developers. "Governments can verify for themselves that there are no back doors," said Mark Estberg, senior director of Microsoft's global government security program.

NBC News
U.S. Urged Ecuador to Act Against WikiLeaks Leader Assange
Thursday, 20 October 2016
Byline: Multiple reporters

Washington - Quiet pressure from the U.S. government played a role in Ecuador's decision to block WikiLeaks founder Julian Assange from using the internet at Ecuador's London embassy, U.S. officials told NBC News.
"It was a bit of an eviction notice," said a senior intelligence official.

Ecuador's government said Tuesday it had partly restricted internet access for Assange, the founder of anti-secrecy group WikiLeaks, who has lived in the South American country's London embassy for more than four years. A source familiar with the situation says the Ecuadoran government has been frustrated with Assange and his presence at the embassy in London for months and has been considering how best to proceed.

The action came after U.S. officials conveyed their conclusion that Assange is a willing participant in a Russian intelligence operation to undermine the U.S. presidential election, NBC News has learned. U.S. intelligence officials believe Assange knows he is getting the information from Russian intelligence, though they do not believe he is involved in helping plan the hacking, officials told NBC.

"The general view is he is a willing participant in the Russian scheme but not an active plotter in it. They just realized they could use him," said a senior intelligence official.

WikiLeaks has been posting the private emails of Clinton adviser John Podesta and other Democratic officials that the U.S. says were hacked by, or on behalf of, Russian intelligence agencies. WikiLeaks said Assange's internet access was cut off Sunday. In a statement, Ecuador said the decision was its own.

"Ecuador, exercising its sovereign right, has temporarily restricted access to part of its communications systems in its UK Embassy," the statement said.

"The Ecuador government respects the principle of non-intervention in other countries' affairs, it does not meddle in election processes underway, nor does it support any candidate specially."

A senior administration official said that the U.S. did not push Ecuador to cut Assange off from the internet: "Reports that the U.S. government, to include the Intelligence Community, pressured the Ecuadorian government to interrupt internet service within Ecuador's embassy in London are not accurate."

The State Department said it did not pressure Ecuador or play any other role in blocking Assange's internet access.

"While our concerns about WikiLeaks are longstanding, any suggestion that Secretary (John) Kerry or the State Department were involved in shutting down WikiLeaks is false," State Department spokesman John Kirby said in a statement.

However, U.S. intelligence officials told NBC that a message was conveyed to Ecuador that it should stop allowing Assange to carry water for Russian intelligence agencies, and that Ecuador, though run by a leftist, anti-American government, was receptive.

The U.S. moves come as bipartisan concern is growing about the alleged Russian interference amid a daily release of Podesta emails.

Marco Rubio, who is running to retain his Florida Senate seat after losing the Republican presidential primary to Donald Trump, urged members of his party not to seek to capitalize on emails stolen by Russian spies.

"As our intelligence agencies have said, these leaks are an effort by a foreign government to interfere with our electoral process, and I will not indulge it," Rubio told ABC News. "Further, I want to warn my fellow Republicans who may want to capitalize politically on these leaks: Today it is the Democrats. Tomorrow it could be us."

Dhaka Tribune
PM for stronger cyber security
Thursday, 20 October 2016

Dhaka - Stressing the need for increasing capability of cyber security, Prime Minister Sheikh Hasina has said that steps will be taken so that none can commit crimes by using digital facilities.
"Some problems linked to security have been created with digitisation, and for this, our capability of cyber security will have to be enhanced ... we will have to stay alert so that security of the financial sector and secret issues is not hampered in any way," the premier said while addressing the inauguration of the "Digital World 2016?at the International Convention City Bashundhara in Dhaka yesterday. She added that necessary manpower would be created alongside procuring equipment to check cyber crimes.

The prime minister also mentioned the role of her ICT Affairs Adviser and son Sajeeb Wazed Joy in building Digital Bangladesh. "He is the main architect of implementation of the Digital Bangladesh," she added.

In recognition of his contribution, Joy received ICT for Development Award 2016 for which, Hasina said, she was very much proud as his mother.

Referring to her government's steps for enacting the Digital Security Act 2016, the premier said under the law, the government would set up world standard forensic lab, constitute a Cyber Security Agency, and establish cyber incidents responsive team and a high-level digital security council.

The ICT Division has organised the three-day event with the theme "Non-stop Bangladesh" with the assistance of the Bangladesh Computer Council (BCC), Bangladesh Association of Software and Information Services (BASIS) and a2i Programme of the Prime Minister's office.

After her speech, the premier inaugurated the Digital World 2016 digitally by pressing a switch. Earlier a small robot invited her to open the expo.

The Digital World 2016 showcases the technology-based innovations and achievements, and facilitate in a single platform for sharing ICT knowledge and ideas.

Over 200 speakers including 43 from world famous organisations such as Microsoft, Facebook, the World Bank, ZTE, Huawei are expected to take part in 18 sessions. The mega event would include 12

seminars, IT career fair, soft expo, e-Governance expo, mobile innovation expo, e-commerce and Business Process Outsourcing (BPO) programme.

State Minister for ICT Division Junaid Ahmed Palak, Chairman of the Parliamentary Standing Committee on Post, Telecommunication and ICT Ministry Imran Ahmed, ICT Division Secretary Shyam Sundar Shikdar, BCC President Mostafa Jabbar, Executive Director of BCC SM Ashraful Islam, Project Director of a2i Programme Kabir Bin Anwar also spoke at the function.

The prime minister later inaugurated six "smart buses" having all ICT facilities for imparting training to the women on ICT.

As part of further ensuring capacity of digital security, Hasina said that steps had also been taken to connect Bangladesh with the second submarine cable as there is no alternate submarine cable in the country.

She said that Bangladesh had already joined the SEA-ME-WE-5 consortium and would get 1,300 GBPS bandwidth in the second submarine cable.

Citing that the work on installing country's first own satellite, the "Bangabandhu Satellite 1," she said that Bangladesh could even export satellite bandwidth after launching its journey in 2017 and meeting the demand.

Hasina said that her government had stopped bribes and unnecessary harassment of people using information technology, adding that tender manipulation was also stopped due to digitisation.

The premier said her government put highest importance on education to build Digital Bangladesh and made ICT education compulsory from class six to 12th class. As many as 5,500 labs including 2,100 Sheikh Russel Digital Lab had been set up in the country while more 10,000 Sheikh Russel Digital Labs would be established by the end of 2018.

Besides, she said, the government approved "Innovation Design Entrepreneurship Academy (IDEA)" project aimed at giving innovative works an institutional shape and expanding IT Start-up initiative alongside beginning wide ranging works titled "One Thousand Innovation by 2021."

The prime minister said that every upazila of the country had been brought under optical fibre connection and 3G network, while bandwidth price reduced to Tk625 from Tk76,000 in 2007.

"Steps have also been taken to introduce 4G network in 2017, she said adding that 130 million mobile SIM are being used while 640 million people are now using internet in Bangladesh," she said.

Hasina mentioned that rural people were receiving about 200 types of services from digital centres across the country. Apart from this, she said, about 3,000 post offices had been transformed into digital service centres.

The premier said Bangladesh was exporting software and ICT services to about 40 countries including some developed nations. Under the "Learning and Earning" project, 55,000 male and female youths would be trained up on freelancing to increase efficiency.

Financial Times
Yahoo calls for greater transparency from intelligence services
Thursday, 20 October 2016
Byline: Hannah Kuchler

San Francisco - Yahoo is demanding US intelligence services reveal how they monitor online services, after a report said the internet company secretly scanned customer emails.
In a letter to James Clapper, the US director of national intelligence, Yahoo said citizens in a democracy require more information to understand and debate how the US uses legal authorities to obtain private data.

Yahoo said it found itself unable to respond in detail to the accusations in a Reuters article earlier this month, which claimed that the company had secretly built custom software to scan users' incoming emails for specific information requested by US intelligence officials.

Ron Bell, Yahoo's general counsel, urged the director to confirm whether an order "as described in these media reports" was issued and, if so, declassify the order in whole or in part. He wrote that he wanted the office to make a "sufficiently detailed public and contextual comment to clarify the alleged facts and circumstances".

Mr Bell said recent news stories had "provoked broad speculation" about Yahoo's approach and the activities of the US government.

"That speculation results in part from lack of transparency and because US laws significantly constrain -- and severely punish -- companies' ability to speak for themselves about national security related orders even in ways that do not compromise US government investigations," he said.

Yahoo, which is simultaneously trying to curtail the impact of a large data breach, has responded to the Reuters investigation by saying it was a "law-abiding company" and "complies with the laws of the United States".

The letter specifically refers to the use of the Foreign Intelligence Surveillance Act, which became famous after Edward Snowden, the former National Security Agency contractor turned whistleblower, to surveil online activities.

Yahoo is fighting to prove it is a competent custodian of millions of people's data after it said last month that details of about 500m email accounts may have been stolen in a cyber attack by a state-sponsored actor.

The Silicon Valley company said on Tuesday that users had remained loyal to the platform despite the cyber attack, in a response to concerns that Verizon, which agreed to buy Yahoo for $4.8bn, could ask for a discount on the deal.

Verizon has not commented on the accusations of US surveillance activity at Yahoo but Craig Sillimen, Verizon's general counsel, said that it was up to Yahoo to prove that the cyber attack had not had a material impact on its business.

The office of the director of national intelligence did not respond to a request for comment.

FCW.com
NSA: Hackers find an easy path to U.S. systems
Thursday, 20 October 2016
Byline: Sean D. Carberry

Washington - For all the concern about zero-day exploits, a senior NSA official said that the high-profile hacks of U.S. networks in the last two years show there are far easier ways for cybercriminals to infiltrate government systems.
Speaking at the American Enterprise Institute on Oct. 18, Curtis Dukes, deputy national manager for national security systems at the NSA, said that none of the high-profile government hacks the NSA responded to -- Office of Personnel and Management, the White House, State Department, Department of Defense -- used zero-day exploits.

"Basically the adversary took advantage of poorly secured, poorly patched systems," said Dukes. "Once they had that initial foothold they the elevated privileges and then moved to mission objective," which ranged from stealing data to (in the case of the Sony hack) destroying it.

"We talk a lot about zero days, we talk about Shadow Brokers, things of that nature, but so far we haven't actually changed the equation for the adversary," said Dukes. "They still can easily attack us [and] achieve mission objective -- I want to actually raise the cost."

Dukes said that raising the cost means implementing a set of practices and protocols outlined in the NSA's Top 10 Mitigations publication. Dukes said that following those protocols, which include

controlling administrative privileges, updating and patching software and application whitelisting, would make it more difficult for cyber criminals and force them to consider zero-day exploits, which he described as precious commodities that hackers use only on their most difficult targets.

In his talk, Dukes expanded on comments he recently made to FCW about the bureaucratic hurdles that NSA must jump when responding to a hack of a non- national security system.

NSA has authority over national security networks, but must be asked by the Department of Homeland Security and the FBI through a Request for Technical Services in order to assist in investigations into breaches of other agencies.

"I just think by the time it's all orchestrated, you've lost valuable time in order to do defense at cyber speed in that regard and I think that's what we need to relook at as a nation," Dukes told FCW.

In his AEI remarks, Dukes said that "when we actually have to do incident response, and again if you look at the last 24 months we've done a fair amount of that ... it's typically days to a week before we can actually respond."

And by that point, Dukes said, the crime is over and it's difficult to determine if the adversary is still inside the system and what mitigation steps can be taken. Therefore, he said, the U.S. needs to revise its approach to cybercrime.

"Possibly even going so far as that we unite pieces of [DHS, FBI, and NSA] into one organization that does it on behalf of the whole of government," he said.

Dukes pointed to the U.K.'s new National Cyber Security Centre as an example of a single entity that responds to cybercrime against any government agency.

"It's one entity, they're in charge," said Dukes. "I think it's a model we need to look at, possibly explore how that best aligns with how we do cyberdefense on behalf of the nation."

Khaleej Times
28% govt entities in region hit by cyber attacks in H1
Thursday, 20 October 2016
Byline: Bernd Debusmann Jr.

Dubai - Eleven per cent of UAE organisations were subject to targeted cyber attacks between January and June 2016, according to statistics unveiled by cyber security company FireEye during Gitex technology week.

FireEye's EMEA Advanced Threat Report also found that 19 per cent of Saudi organisations were targeted, as well as 11 per cent of Qatari ones. Across the region, 28 per cent of government entities were subject to at least one targeted attack.

In an interview with Khaleej Times, Stuart Davis, Middle East and North Africa director for Mandiant - a wholly owned subsidiary of FireEye - said the turbulent geo-politics of the Middle East make it a prime target for cyber criminals.

"When we look at the Middle East, one of the interesting things is that right now it's a hotbed of activity of cyber espionage and cyber attacks," he said. "Many countries have neighbouring challenges. You need only to look at Saudi Arabia and Iran as an example."

The report also found that government entities, such as foreign and defence ministries; energy sector organisations such as oil production facilities; and financial services companies such as investment banks and sovereign wealth funds were among the most targeted institutions.

"If you look at the UAE specifically, there are definite parallels being drawn compared to the GCC, with government and energy infrastructures being targeted in common," Davis said. "The difference is telecommunications. There is targeted activity towards the UAE, but the UAE has a more mature cyber-resilience and has been dealing with these attacks for longer."

In addition to Russia and China-based groups, Iranian 'threat actors' feature prominently as the culprits of such attacks.

"We are tracking 13 suspected Iranian threat actor groups in the region," Davis noted. "They have motivations such as cyber espionage. Due to political instability, that ultimately shows that they have come to gather information, such as on future endeavours."

In Davis' opinion, such attacks will likely continue in the near future. "The geopolitical landscape is consistently in flux and tends to go up and down. As long as that's happening, there will be neighbouring countries that will want to know, early, what's happening with their neighbours," he said. "We also expect to see critical and national infrastructure be targeted, such as big banks or electricity and water systems."

Now Lebanon
Syria facing internet outages
Thursday, 20 October 2016Byline: Albin Szakola

Beirut - Syria is set to face widespread internet connectivity issues due to maintenance work on a cable off the country's Mediterranean coast, days after a Russian deep sea exploration vessel's presence in the area raised questions.

Syrian Telecom issued a statement Tuesday explaining that repairs will begin October 19 on a "major international cable" providing approximately "60% of the internet capacity in Syria," as well as service to other countries in the region.

The government-owned company added that the maintenance work--which it described as "unexpected, urgent and swift"--will last until October 28, causing "low level Internet quality."

Syria Telecom vowed that it was "following up on the issue with international operators to secure alternative international routes to ensure Internet service at its normal, full speed," but apologized in advance to subscribers for the circumstances "beyond its control."

Late last week, the Russian vessel Yantar was spotted off the northern coast of Lebanon sailing north toward Syria, raising fears it could cut the undersea fiber- optic cable providing internet to the war-torn country, according to a report in the Daily Beast.

The report noted that the Yantar is equipped with remote submarines that are "capable of severing the cables miles under the ocean's surface that carry global Internet communications."

For its part, Syrian Telecom made no mention of the Yantar, but did not go into details regarding the technical problems afflicting the cable.

Instead, the company's statements said merely that the undersea cable was "exposed recently to frequent and sudden crashes from time to time."

Khaleej Times
Emiratis told to 'clean e-devices' of illegal content
Thursday, 20 October 2016
Byline: Jasmine Al Kuttab

Abu Dhabi - Emiratis' reactions were mixed to a warning from the Ministry of Foreign Affairs and International Cooperation to those travelling to the United States to ensure their mobile phones, laptops and other electronic devices do not contain content that are illegal.
According to the ministry, US authorities have said they will be imposing new security measures at airports, which include the inspection of travellers' personal devices.

The warning comes just months after another from the UAE authorities, which urged male citizens to avoid wearing traditional garments and headdress while abroad for their own safety. The warning came after an Emirati businessman, Ahmed Al Menhali, was held at gunpoint and violently arrested in front of Fairfield Inn and Suites in Avon, Ohio, when a hotel clerk made a 911 call reporting 'suspicious activity'.

On Tuesday, the Ministry of Foreign Affairs and International Cooperation highlighted that the US National Transportation Safety Board (NTSB) would now start inspecting personal devices for materials that violate public decency or are found to be illegal.

First-Lieutenant Engineer Ali H. Al Madfaei, chemical biological radiological nuclear officer at Abu Dhabi Police, told Khaleej Times searching personal devices could be seen as invasion of privacy. "Is the US searching our personal devices considered Islamophobia?"

The 30-year-old pointed out: "Americans often rush quickly to defend their constitutional rights and amendments. They believe this is the founding cornerstone of their nation. Yet, no one seems to bat an eyelid when the same constitutional rights of minorities are violated."

He noted that US authorities at airports checking travellers' personal devices resembles the 'Stop-and-Frisk,' programme, which was supported by former New York Mayor and Donald Trump endorser, Rudy Giuliani.

The initiative was, however, criticised because it was deemed unconstitutional, as it was targetting African-Americans and Latinos.

"Many deemed the 'Stop-and-Frisk' search as unconstitutional because it targetted people based on their appearances. But just because the unconstitutional search happens on a digital field at airports does not in any way reduce its severity.

"Sounds like this initiative will too target Arabs and Muslims, so why is it standing?" asked Al Madfaei.

Khalifa Al Fahim, a senior systems analyst at ADNOC, agreed. "Searching content on mobile phones is certainly an invasion of our privacy."

The 30-year-old, however, noted that the recent warning would not stop him from travelling to the US. "I understand why US authorities are being strict, and I would understand if the UAE did the same thing. It's better to be safe than sorry."

Khalifa Al Shamsi, an associate at the Abu Dhabi Investment Authority, does not believe the move is racially motivated. "One cannot judge and believe that US authorities are targetting Arabs and Muslims.

"I don't think it's racist in any way, it is perhaps more about security measures because of all the recent global threats. I also don't think any normal and safe traveler would have illegal content on his phone."

39- year-old Abdullah Salem Al Shamily, a retired Emirati government employee on pension, told Khaleej Times that he definitely has no problem with the new American measures that may include inspection of phones for illegal content or that violate public decency in the US. "It is my duty to respect the law of other countries and those of mine as well," he said.

"We should seriously take the warning of the UAE Ministry of Foreign Affairs and International Cooperation and observe it because it is mainly for our safety."

Emirati national Rashid Ghanim Al Shamsi, member of the Hamriya Sports & Cultural Club, said there is no reason at all to cancel his travel plans to the States for such procedures. "I have nothing to hide, and I am afraid of nothing. Why should I care or feel worried. We should respect the laws of other countries."

Sydney Morning Herald
Ex-spy chief warns of net threats
Thursday, 20 October 2016
Byline: Deborah Snow and David Wroe

Sydney - The task of being an intelligence chief has become tougher with the rise of cyber threats and terrorism, according to the former head of the Australian Security Intelligence Organisation, David Irvine, who says he would like to see a "much stronger" national cyber industry.
Speaking during a rare interview in Canberra, Mr Irvine said "when you put cyber on top of [terrorism], it takes a bit of time off your sleep at night. The two issues have grown exponentially within a couple of decades and while the nature of the threats is the same, the vector has changed. And cyber is a new and very potent vector."

Mr Irvine, who led Australia's overseas spy agency ASIS before he headed up ASIO, said he'd been "horrified" at the revelations of Edward Snowden, the subcontractor to the National Security Agency who exposed vast top- secret US government programs for monitoring global communications. "People say, well nobody lost their lives as a result of Snowden, but how do you know that? You run through your mind all the possible consequences of having your capabilities, which are there to defend the country, exposed ..."

Mr Irvine expressed surprise at the "baldness" of the hacking of the Democratic National Committee data base (allegedly by Russia) in the US presidential election campaign, aimed at damaging Hillary Clinton.

"There has always been in the espionage/sabotage business the use of purloined information to obtain a political objective" he said. "But the baldness of [this] is a little bit surprising, the unsubtlety even more surprising.

"The tragedy is that it restricts the freedom of our politics in a whole variety of ways, it puts strictures on our political decision makers ... they have less free conversations, become more afraid to express themselves in emails. I certainly am much more careful in the way I express myself in emails than I might have been a few years ago." Mr Irvine was a guest at a series of security briefings for government agencies organised in Canberra this week by Australian cyber security firm Nuix. Also attending the

briefings was the company's US-based vice-president, Keith Lowry, who worked at the Pentagon at the time of the Snowden leaks and led a team trying to assess the damage from the revelations. He told Fairfax Media that many Australian government departments were "still exposed to serious data security risks because they do not conduct ongoing insider threat assessments".

Mr Irvine said cyber security was the area where those charged with protecting critical infrastructure in Australia "really had to focus in the next few years".

"You immediately think of cyber sabotage being the first tool of warfare in the 21st century but the tools that are available to nation states are increasingly available to non-state actors."

He said he wanted to see a "much stronger national cyber industry" and that while the government's recent and "probably overdue" paper on cyber security was very welcome, "the challenge now is to implement it".

Computer Weekly (UK)
Ireland to follow UK in setting up national cyber security centre
Wednesday, 19 October 2016
Byline: Warwick Ashford

Dublin - Ireland plans to set up a national cyber security centre, according to Denis Naughten, the country's communications minister.
The news comes less than a month after the UK's National Cyber Security Centre (NCSC) officially opened for business, combining all the government's cyber security agencies under one roof.

"I will bring a memorandum to cabinet next week to establish a national cyber security centre that will focus on securing government networks," Naughten told the (ISC)2 EMEA Congress 2016 in Dublin.

The centre will also cover the security of critical national infrastructure as well as assist industry and individuals to protect their digital assets.

"The centre will build on the existing computer security incident response team that has been in place in my department since 2011, providing incident response services to government departments and core state agencies," said Naughten.

As communications minister, Naughten said a key social, economic and political priority is Ireland's national broadband plan, which will bring fibre-to-the-home to rural Ireland.

"This means that the majority of consumers in rural Ireland will have access to services of up to 1 gigabit per second (Gbps), with symmetrical upload and download speeds for businesses," he said.

"In addition, in last week's budget in Ireland, funding was made available to facilitate the reallocation of the 700Mhz spectrum away from television broadcasting to support broadband and mobile telephony service plans, particularly in rural areas, which means a valuable spectrum band will be freed up to deliver mobile data, including 5G."

As a result, Ireland is now likely to be the first EU country to roll out 5G based on geographical factors rather than population density, putting it at the forefront of Europe and internationally in terms of connectivity and quality of service, said Naughten.

Three-quarters of consumers in Ireland reportedly manage their money or make payments using mobile devices, he said, which is nearly 50% higher than the EU average. Also, nearly 60% of 55 to 64-year-olds use a mobile device for banking, which highlights the level of trust they have in using technology, he added.

"This is an endorsement of the information security profession, but security of devices and data is continually under threat," said Naughten, which is why his department published Ireland's first national cyber security strategy last year.

"This builds on the longstanding recognition of the state's role in facilitating improved security in the online world, and set out how we would protect our digital assets, including personal data and infrastructure," said Naughten, pointing out that the planned national cyber security centre builds on this further.

"It is important that we have effective and accepted cyber security, which involves a balance of individual rights, particularly with regard to privacy and data protection with the interests of public safety and national security, but that is a difficult and challenging balance to achieve," he said.

Naughten said that in the light of the fact that the world is becoming ever more reliant on digital services, he stresses the need for a risk management process to be put in place.

"Our banks, our hospitals, our airports, airlines, shipping, road and rail vehicles, together with utility providers, need to be safe from cyber attacks, and I recognise that regulation alone will not be sufficient, and therefore I am committed to a programme of education and training so that the public, as well as business, are better able to protect themselves in a digital world," he said.

Le Soleil
400 experts à la conférence sur la radicalisation
Friday, 21 October 2016
Byline: Valérie Gaudreau

Québec - Impact des nouvelles technologies dans les discours haineux, rôle des villes contre la radicalisation ou encore des témoignages de familles de jeunes radicalisés : on en a appris davantage jeudi sur le contenu d'une grande conférence de l'UNESCO à Québec du 30 octobre au 1er novembre. La tenue dans la capitale de la conférence «Internet et la radicalisation des jeunes : prévenir, agir et vivre ensemble» avait déjà été annoncée en mai par la ministre québécoise des Relations internationales, Christine St-Pierre. Mais jeudi, le dévoilement de la programmation a permis d'apprendre que 400 experts et représentants de 70 pays convergeront vers Québec la semaine prochaine.

La directrice générale de l'UNESCO, Irina Bokova, sera présente. On entendra aussi le lieutenant général à la retraite Roméo Dallaire et Jehangir Khanm, directeur de l'équipe spéciale de lutte contre le terrorisme des Nations Unies, en plus de divers experts, universitaires et représentants du secteur privé. Le responsable de la liberté d'expression et des relations internationales chez Google, Ross LaJeunesse, participera notamment à un atelier.

Pour la ministre St-Pierre, la conférence Québec-UNESCO permettra de «faire rayonner l'expertise québécoise». «Mais également de démontrer notre volonté à participer activement au dialogue international sur la question afin de dégager des pistes de solution durables et efficaces», a-t-elle commenté en conférence de presse à l'hôtel de ville de Québec.

Si la radicalisation vers l'islam, au coeur de l'actualité, sera largement abordée, la conférence promet aussi des discussions sur divers types de propos haineux. Un ancien suprémaciste blanc devenu travailleur social, Daniel Gallant, participera notamment à une table ronde.

Journée du vivre ensemble

Jeudi, Christine St-Pierre a aussi déposé une motion à l'Assemblée nationale pour la création d'une journée nationale du vivre ensemble. Cette journée se tiendra le 15 janvier, en mémoire des Québécois, dont des résidents de Lac-Beauport, décédés dans les attentats de Ouagadougou au Burkina Faso le 15 janvier 2016.

Arab News
Govt cracks down on those who misuse social media accounts
Friday, 21 October 2016
Byline: Mohammed Al-Sulami

Jeddah - The increasing use of social media to harm the Saudi community, citizens, or Islam by some users in the Kingdom has prompted the Ministry of Interior to crack down on these users, arresting them on charges of acting in a manner that harms and deviates from the ways of the Saudi community and Islam. The ministry's response comes in light of repeated requests from the public to take action against the owners of these accounts. On Wednesday, Riyadh police were able to identify a citizen in this 30s who misused Snap Chat in a manner that angered many citizens and prompted them to call for his punishment. Riyadh police spokesman Col. Fawaz bin Jameel Al-Maiman said close monitoring allowed authorities to identify the man, who had been using his account to post clips of him making disrespectful and harmful comments. He was arrested and handed over to the branch of the Bureau of Investigation and Public Prosecution for violating anti-information crime regulations.

Indo-Asian News Service
India: 3.2 million debit cards 'hacked', data breach alarms customers
Friday, 21 October 2016

Mumbai - Prompting pre-Diwali panic among customers, an estimated 3.2 million debit cards of various banks are believed to have been "hacked" following a suspected security breach.
Investigations have begun into the causes behind the security risks. Several banks, including the State Bank Of India (SBI), have already started blocking their customers' debit cards and re-issuing fresh ones free of cost.

An estimated three million debit cards issued by various public or private banks are said to be affected by a potential data breach.

Debit or credit cards are prone to security issues when unauthorised parties gain access to the confidential data embedded on them, even as they are being swiped in an automatic teller machine (ATM).

In the current scenario, the SBI alone has blocked more than 600,000 debit cards while assuring that the malware-related security breach was reportedly detected in the non-SBI ATM network.

The move has been undertaken to ensure that customers' confidential personal data is not compromised while debit or credit cards are swiped for various transactions.

One of the card network companies, MasterCard said on Thursday that its "own systems have not been breached".

"We are working on the investigations with the regulators, issuers, acquirers, global and local law enforcement agencies and third party payment networks to assess the current situation," a MasterCard spokesperson said.

It has advised the consumers to review their account statements and activity, and if any unusual or fraudulent transactions are suspected, they should contact the concerned bank for more assistance.

Anxious customers have started enquiring with their banks over the seriousness of the problem, whether their personal data has leaked out and if that could lead to financial implications, especially with Diwali round the corner.

On Wednesday evening, the SBI said it has blocked cards of certain customers identified by the networks as a precautionary measure, though it did not reveal the exact number of cardholders who would be hit.

The SBI emphasised that its own systems have absolutely not been compromised and existing cardholders are not at any risk and can continue to use their cards as usual.

According to banking circles, several other banks have also experienced similar problems as a few ATMs have been hit by a malware which has a high potential to compromise customers data.

Official figures indicate that the SBI has over 200 million active debit cards, besides 47.5 million others of its associate banks.

In early September, the National Payments Corporation of India (NPCI), Mumbai, which controls all the retail payments systems in the country, had made it clear that there "is no compromise at NPCI and our systems are fully safe and secure."

NPCI handles over 25 million transactions daily, including RuPay cards, of which more than 290 million are currently in circulation.

Khaleej Times
Secure access to cloud a top priority for 41%
Friday, 21 October 2016
Byline: Sandhya D'Mello

Dubai - Cloud security is imperative and businesses have to adopt it for their growth, says Miguel Braojos, vice president of global sales, IAM Solutions at HID Global on the sidelines of the company's participation at the 36th Gitex Technology Week, under the theme 'Your Security Connected.'
"The company is focused in finance, governments and utilities - but in Middle East, it is the oil and gas sector. The organisations in the region are enhancing their security levels. Cloud adoption is beginning to take prominence, and by placing data and applications in the cloud, organisations gain a lot of flexibility in terms of accessibility. This is the upside; but in doing this, companies also expose themselves to risk and have to take steps to protect their assets," said Braojos.

"A robust security strategy and solutions with multi-factor authentication will suffice because the loss or damage of digital assets can have significant ramifications for an organisation. We are glad to find that organisations are assessing and evaluating their security strategies and reviewing implementing multi-factor authentication," he added.

As part of the company's mobility initiative, HID Global is demonstrating its ActivID Tap Authentication platform, which is powered by Seos, for convenient and secure multi-factor authentication to more than 2,400 cloud apps and web services on mobile devices with the simple tap of a smart card. HID Global will also emphasise the benefits of an enhanced user experience through its ActivID Authentication Appliance, an enterprise authentication solution that enables end users to securely access the door, data and cloud apps, anywhere, anytime.

A regional survey conducted by HID Global revealed that 47 per cent of organisations believe that securing access to cloud based data and application is as important as securing physical premises. With 41 per cent stating that secure access to cloud based data and applications was their number one priority.

Of the respondents who participated in the survey, 72 per cent said they relied on private cloud solutions and 48 per cent used it for collaboration solutions including databases, CRMs, and email. Around 33 per cent also said they stored mission-critical applications and data. In addition, 28 per cent of organisations said that they don't rely on cloud solutions at all. The most frequent reason cited for 39 per cent of respondents was that their organisation generated sensitive data, while 30 per cent found it too risky.

Other limiting factors for adopting cloud solutions in an organisation were found to be high cost for 11 per cent of respondents, and a lack of acceptance within existing company policy for 15 per cent of respondents.

Gulf News
Gitex shows how to imagine future on a grand scale
Friday, 21 October 2016
Byline: Naushad K. Cherrayil

Dubai - The 36 edition of Gitex Technology Week closed on a positive note on Thursday with a focus on robotics, 3D printing, virtual reality, augmented reality, drones, start-ups and live demos on latest technologies.
Etisalat tested 5G live trials, reaching 36Gbps speed to help it cope with the massive digital content explosion anticipated in the next few years while du in partnership with Nokia demonstrated the Middle East's first 4K 360 degree 3D virtual reality (VR) video streaming using 5G-ready network.

Robotics, along with drones and 3D printing, are three interrelated technologies that are rapidly decreasing in cost, advancing in sophistication, and driving innovation.

"Demand for 3D printing used to come from universities before but now it is even coming from schools. The intake by consumers is still not there yet but it is a matter of time," said Ashsih Panjabi, Chief Operating Officer of Jacky's Business Solutions.

UAE start-up DigiRobotics showcased the first virtual reality robotic simulator, first 3D-printed car and first 3D-printed humanoid robot.

"The UAE has shown how to imagine the future on a grand scale. Experts and futurists see the world changing in the near future, in a place where new ideas are especially welcomed," said Trixie LohMirmand, senior vice- president for exhibitions and events management at Dubai World Trade Centre.

The five-day event witnessed the most global weeklong start-up event in 2016, more than 410 start-ups from 60 countries and 1,200 tech founders.

"The opportunity to meet with start-up teams from around the world and from different industries in one place face-to-face is very valuable and highly effective," said Erich Sieber, Partner and senior vice-president of Inventages venture capital.

Raed Hafez, founder of Dubai grocery delivery app start-up el Grocer, praised the volume of opportunities at Gitex Global Startup Movement.

"In a span of three days, we met with ten investors. In the one-on-one meetings, we were able to meet a number of key investors who showed significant interest in our next funding round."

Ramkumar Balakrishnan, President of Redington Value Distribution, said that there has been an increased enterprise-focus over the past three years.

"There is a big change in the consumption model of IT. Customers are moving towards the Opex model. They want to consume IT like they consume other forms of utilities," he said.

Balakrishnan sees converged and hyper-converged infrastructure, adoption of cloud, Big Data and IoT as the main technologies that are going to drive future growth.

"This year, we connected with new prospects, further developed our brand awareness, and educated partners and customers about seamlessly managing data across different IT platforms," said Fadi Kanafani, Regional Director for Middle East and Africa at NetApp.

Next year's Gitex Technology Week will take place from October 8-12 at Dubai World Trade Centre.

Gulf News
UAE can and must play a larger role in global Internet security (Canada).
Friday, 21 October 2016
Byline: Harshul Joshi

Dubai - Cyber threats are more evident than ever before. On the one hand, data and communications technology have been embedded in everything from banking and municipal governance to cars, and in the process, they've sown the seeds for greater productivity and operational efficiency.
On the other hand, our vulnerability to cybercrime and sabotage has advanced in kind. According to PricewaterhouseCoopers, 79 per cent of companies fell victim to cyber-incidents in 2015 globally, and Symantec identified 54 new zero-day vulnerabilities, or more than one per week.

Numbers like these position cybercrime as an escalating threat, and the upcoming meeting of the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) (Subcommittee SC) 27 in Abu Dhabi presents an opportunity for local firms to offer a voice in securing our digital economy in the region.

For the first time since the working group was founded in 1990, a nation in the Middle East will host the international discussion on IT security standards, and ultimately shift the nexus of discussions on the delivery of resiliency in digital networks.

Historically, the same hubs that gave us some of our most popular technologies have had the job of remedying their exploitation. For instance, the World Economic Forum's index of nations most prepared to battle cyberattacks is filled with the usual suspects, with the US, Canada and Australia topping the list.

This first meeting of ISO/IEC JTC SC 27 in a less well-established region from the perspective of active cyber security defence suggests that emerging markets will play an expanding role in cyber resiliency and security in the future.

Under the auspices of Emirates Authority for Standardisation & Metrology (ESMA) and the UAE's National Electronic Security Authority (NESA), 350 international experts in IT security will meet to set information security standards with global implications.

Together, in the presence of 52 voting members and 18 observing members of the ISO, they will deliberate over technical specifications, identity management, biometrics and conformance assessments required to meet the challenges confronting governments, businesses and consumers in a digital age.

Data security vulnerabilities threaten economies of all sizes. Inadequate governance, unethical or uninformed computer users, insufficient legislation, in addition to poor technical standards chip away at internet and IT security.

The ISO/IEC's decision to convene the meeting in the UAE is a significant vote of confidence in the country's proactive stance on the management of its cyber environment, not least as Dubai aspires to emerge as the 'smartest city' in the world by 2017.

In 2015, the International Telecommunication Union (ITU) ranked the UAE among the top-10 most dynamic countries in ICT development, and the first in ICT use and government efficiency. Government agencies, such as ESMA and NESA, have led the charge in implementing best practices in security and reinforcing IT infrastructure.

The UAE is also leading internet security in a region that has proven vulnerable to cyberattack. Businesses in the Middle East report a higher frequency of incidents and a greater volume of losses per attack than any other region in the world. The ISO/IEC JTC SC 27 in Abu Dhabi (October22-27) represents an opportunity for firms in the UAE, and indeed the region, to gain international recognition for what is being accomplished in the field. At the same time, participants from the UAE will network with their peers and exchange information from markets around the world.

Despite the significant strides made by the government, businesses also have a role to play in mitigating attack. Cyber incidents cost the Gulf region $1 billion (Dh3.67 billion) in 2015 according to organisers of the UAE Security Forum.

Now Lebanon
Russia preparing to spy on Syria internet, activists warn
Friday, 21 October 2016
Byline: Albin Szakola

Beirut - An activist group dedicated to ensuring safer online communication for Syrians has warned that maintenance work being conducted on an undersea cable providing internet to the country is part of a Russian espionage effort.
SalamaTech Project issued a statement Wednesday that Syrian Telecom's announcement of repairs on the fiber-optic cable off Syria's Mediterranean coast "confirms" that a Russian deep sea exploration vessel spotted sailing in the area "is either already spying on this internet cable or will be in the future."

The organization cited an unnamed security expert as saying that the Russian ship will likely route the maritime cable through the Russian naval base in Tartous, allowing Moscow "to eavesdrop on internet communications between Syria and the rest of the World Wide Web."

Questions have been raised over the presence of the Russian oceanographic research vessel Yantar near an undersea fiber- optic cable providing internet to Syria.

In a separate statement, SalamaTech advised all Syrians to "take the highest degree of caution when using the internet" and avoid using it entirely when not using a Virtual Private Network (VPN) to encrypt their connection and prevent authorities from spying on them.

It also called on internet users to avoid the use of Skype and instead use Signal, an encrypted online messaging program.

SalamaTech's statements come after Syrian Telecom informed the public that maintenance work began October 19 on a "major international cable" providing approximately "60% of the internet capacity in Syria," as well as service to other countries in the region.

The government-owned company added that the maintenance work--which it described as "unexpected, urgent and swift"-- will last until October 28, causing "low level Internet quality."

Late last week, the Russian vessel Yantar was spotted off the northern coast of Lebanon sailing north toward Syria, raising fears it could cut the undersea fiber-optic cable providing internet to the war-torn country, according to a report in the Daily Beast.

The report noted that the Yantar is equipped with remote submarines that are "capable of severing the cables miles under the ocean's surface that carry global Internet communications."

Wall Street Journal
U.S. Ads Aim to Dispel Terrorism's Lure
Friday, 21 October 2016
Byline: Felicia Schwartz

Washington - The Obama administration, which has struggled for years to combat the social-media lure of Islamic State, is experimenting with new ways to put its online antiextremism messages in front of would-be terrorist fighters overseas.
The revamped effort uses targeted ads on Facebook linked to videos to reach the young men and women who have given digital hints that they could be thinking of traveling to Syria or Iraq to join extremist movements.

The campaign -- being run by the Global Engagement Center, a multiagency initiative housed at the State Department -- is seen by U.S. officials as one of the most promising new initiatives aimed at dissuading would-be fighters. But many officials acknowledge that such efforts are tricky since the target audience can be suspicious of the U.S. government's involvement and that their effectiveness is impossible to know.

"This isn't easy work," said Michael Lumpkin, who earlier this year left his post as assistant secretary of defense for special operations to run the Global Engagement Center.

But early results have been encouraging. The center spent $15,000 on a pilot four-week Facebook ad campaign that targeted 13-to- 34-year-old unmarried men and women in Morocco, Tunisia and Saudi Arabia who expressed an interest in Iraq, Syria or Islamic State-related topics, as indicated by their Facebook activity. Facebook didn't individually identify the people.

The campaign, which ended Oct. 1, reached 6.9 million people and generated 781,000 visits to external sites.

The most successful part of the pilot used a native video ad, which blends in with a site's editorial look and feel. The ad ran on Facebook for a week and reached 2.4 million people who watched for a total of more than 1,050,913 minutes, or two years' worth of streaming.

The ad, about two minutes long, used a cartoon portraying a man exchanging online messages with an Islamic State recruiter. The recruiter encourages him to go to Syria to fight. The man asks questions: Is it true that Islamic State kills Muslims and takes women as slaves? The faceless recruiter offers defenses to each question, urging the man to "trust us."

Ultimately, the man concludes that joining Islamic State wouldn't meet his expectations and decides against it.

The campaign marked the first time the U.S. government had turned to targeted ads to try to disrupt Islamic State recruitment. With the pilot complete, officials are moving to a broader, $50,000 campaign in 12 countries, including Egypt, Indonesia and France.

A pilot earlier this year by Google placed ads alongside results of searches for keywords and phrases entered by users with an apparent interest in Islamic State. The ads linked to Arabic- and English-language YouTube channels with videos intended to dissuade would-be fighters by featuring Islamic State defectors and other themes.

More than 300,000 people were drawn to the YouTube channels over two months, according to Google.

U.S. officials acknowledge they can't directly measure how many people they have persuaded not to join terrorist groups. But an analytics team led by two former National Security Agency scientists is assessing the campaigns' effectiveness. For example, they are examining how long people engage with the content and whether they fill out surveys when prompted.

CNN.com
Did Hillary Clinton reveal classified intel at debate?
Friday, 21 October 2016
Byline: Jamie Crawford

Washington - The Twitterverse was aflame in the hours after Wednesday night's debate with questions about whether or not Hillary Clinton divulged classified information about the country's nuclear arsenal. "There's about four minutes between the order being given and the people responsible for launching nuclear weapons to do so," Clinton said, explaining the quick decision-making required of a commander in chief and questioning Donald Trump's fitness for the job.

"And that's why 10 people who have had that awesome responsibility have come out and, in an unprecedented way, said they would not trust Donald Trump with the nuclear codes or to have his finger on the nuclear button," she continued.

But questions soon began to emerge about whether Clinton was too specific in her description of nuclear launch times and had perhaps revealed something she learned in a classified setting.

A Clinton campaign aide said the information didn't come from a classified briefing, pointing to multiple instances when similar information has been disclosed in public or through open source material.

In the July 2001 report "Minuteman Weapon System History and Description," authors from Hill Air Force Base in Utah discuss the amount of time needed. The "process of presidential authentication with the Pentagon war room and the formatting of a launch order by the war room prior to its dissemination to the Minuteman firing crews would add another 1 minute or so, for a grand total of 4-5 minutes."

And Joseph Cirincione, president of the Ploughshares Fund, which specializes in nuclear issues, tweeted out public references to the same assertions regarding timing.

But even if the information is publicly available, those with clearances cannot reveal anything they learn in a classified setting.

Asked about the sensitivity of this specific information, US Strategic Command, which oversees the US nuclear arsenal, declined to weigh in on the specifics.

"We do not disclose operational timelines, but we do work to provide the President as much decision space as possible," Capt. Brook DeWalt, chief spokesperson for Strategic Command, told CNN in a statement.

Defense Secretary Ash Carter, who appeared at news conference with his South Korean counterpart Thursday, demurred on a similar question about whether such information was classified, saying that the question was "cast in terms of the ongoing presidential campaign."

Reuters
U.S. vote authorities warned to be alert to Russian hacks faking fraud - officials
Friday, 21 October 2016
Byline: David Rohde, Mark Hosenball

Washington - U.S. intelligence and law enforcement officials are warning that hackers with ties to Russia's intelligence services could try to undermine the credibility of the presidential election by posting documents online purporting to show evidence of voter fraud. The officials, who spoke on condition of anonymity, said however, that the U.S. election system is so large, diffuse and antiquated that hackers would not be able to change the outcome of the Nov. 8 election. But hackers could post documents, some of which might be falsified, that are designed to create public perceptions of widespread voter fraud, the officials said. They said that they did not have specific evidence of such a plan, but state and local election authorities had been warned to be vigilant for hacking attempts. On Oct. 7, the U.S. government formally accused Russia for the first time of a campaign of cyber attacks against Democratic Party organizations to interfere with the election process.
U.S. officials familiar with hacking directed against American voting systems said evidence indicates that suspected Russian government-backed hackers have so far tried to attack voter registration databases operated by more than 20 states. Tracing the attacks can be difficult but breaches of only two such databases have been confirmed, they said. The officials said there is no evidence that any hackers have succeeded in accessing equipment or databases used to record votes. Many states use systems that would be difficult to hack or defraud, including paper ballots which initially are tallied by machines. U.S. elections are run by state and local officials, not the federal government. On Nov. 8, votes will be cast in hundreds of thousands of polling stations in 9,000 different jurisdictions, according to the National Association of Secretaries of State.

The U.S. officials declined to comment on Republican candidate Donald Trump's contention that the election is being "rigged." Trump said in the third and final presidential debate with Democratic candidate Hillary Clinton on Wednesday night that he would not say until the election results were known whether or not he would accept the outcome. Trump and his campaign officials have repeatedly said that the potential for voter fraud remains high but they have not provided any evidence.

On Thursday, Trump said he would accept the results of the election "if I win." He said he reserved the "right to contest or file a legal challenge in the case of a questionable result." Clinton supporters said Trump is unwittingly aiding an effort by Russian President Vladimir Putin to undercut the credibility of the vote. Washington and Moscow are at odds over several issues, from Russian involvement in the Ukraine conflict, the war in Syria and cyber attacks. "Trump does not even know he is being manipulated," said Michael Morell, a former deputy CIA director who has endorsed Clinton. "Trump is an unwitting agent of Putin."

Washington Post
Government alleges former NSA contractor stole 'astonishing quantity' of classified data over 20 years
Friday, 21 October 2016
Byline: Ellen Nakashima

Washington - Federal prosecutors in Baltimore on Thursday said they will charge a former National Security Agency contractor with violating the Espionage Act, alleging that he made off with "an astonishing quantity" of classified digital and other data over 20 years in what is thought to be the largest theft of classified government material ever.
In a 12-page memo, U.S. Attorney Rod Rosenstein and two other prosecutors laid out a much more far-reaching case against Harold T. Martin III than was previously outlined. They say he took at least 50 terabytes of data and "six full banker's boxes worth of documents," with many lying open in his home office or kept on his car's back seat and in the trunk. Other material was stored in a shed on his property.

Though he lacks a valid U.S. passport, the government said Martin could still flee to a foreign government that might wish to help him. Prosecutors said he has communicated with unnamed people in Russian and in June downloaded information on Russian and other languages.

The prosecutors also said Martin had an "arsenal" of weapons in his home and car, including an assault-rifle-style tactical weapon and a pistol-grip shotgun with a flash suppressor.

In a complaint unsealed earlier this month, the government charged him with felony theft of government property and the unauthorized removal and retention of classified materials, a misdemeanor. The prosecutors said that when an indictment is filed, they expect charges to include "violations of the Espionage Act," offenses that carry a prison term of up to 10 years for each count.

One terabyte is the equivalent of 500 hours' worth of movies.

Martin, who will appear at a detention hearing in U.S. District Court in Baltimore on Friday, also took personal information about government employees as well as dozens of computers, thumb drives and other digital storage devices, the government memo said.

The government has not alleged that Martin passed any material to a foreign government, but contends that if he is released on bail he could do so.

Prosecutors will argue Friday that Martin, 51, of Glen Burnie, Md., presents "a high risk of flight, a risk to the nation and to the physical safety of others," and that he should not be released from jail.

"The case against the defendant thus far is overwhelming, and the investigation is ongoing," said Rosenstein, Assistant U.S. Attorney Zachary Myers and trial attorney David Aaron. "The defendant

knows, and, if no longer detained, may have access to a substantial amount of highly classified information, which he has flagrantly mishandled and could easily disseminate to others."

Continued detention without bail is necessary, prosecutors said, because of "the grave and severe danger that pretrial release of the defendant would pose to the national security of the United States."

Martin's attorneys argued in a memo filed Thursday that their client is not a flight risk and should be released under court-approved conditions pending trial. "The government concocts fantastical scenarios in which Mr. Martin -- who, by the government's own admission, does not possess a valid passport -- would attempt to flee the country," wrote public defenders James Wyda and Deborah L. Boardman.

Martin's wife and home are in Maryland, they said. He has served in the U.S. Navy. "There is no evidence he intended to betray his country," they said. "The government simply does not meet its burden of showing that no conditions of release would reasonably assure Mr. Martin's future appearance in court."

The government also alleged that Martin took a top-secret document detailing "specific operational plans against a known enemy of the United States." Prosecutors did not name the enemy. The document, prosecutors said, contained a warning, in capital letters, that said: "This conop [concept of operations] contains information concerning extremely sensitive U.S. planning and operations that will be discussed and disseminated only on an absolute need to know basis."

Martin was not involved in the operation, the government said, and had no need to have the document or know its specifics.

Another document found in his car contained handwritten notes describing NSA's classified computer systems and detailed descriptions of classified technical operations, the prosecutors said.

In an interview before his arrest, Martin denied having taken classified material and only admitted to it when confronted with specific documents, prosecutors said. He had access to classified data beginning in 1996, when he was with the Navy Reserve, and that access continued through his employment with seven private government contractors.

The government alleged that Martin was able to defeat "myriad, expensive controls placed" on classified information.

They said the devices seized show he made extensive use of sophisticated encryption. He also used a sophisticated software tool that runs without being installed on a computer and provides anonymous Internet access, "leaving no digital footprint on the machine," they said.

In August, a cache of highly sensitive NSA hacking tools mysteriously appeared online. Although investigators have not found conclusive evidence that he was responsible for that, he is the prime

suspect, said U.S. officials, who spoke on the condition of anonymity because the investigation is ongoing. That is the event that set off the search that turned up Martin, the officials said.

In July, according to the prosecutors' memo, he watched a video about how law enforcement authorities catch computer users who wish to remain anonymous on the Internet. "He has a demonstrated ability to conceal his online communications and his access to the Internet," the prosecutors said.

To support their argument that Martin poses a danger to the community, they noted that in late July, he went to Connecticut to buy a "Detective Special" police-package Chevrolet Caprice. While searching his house, the FBI also recovered 10 firearms, only two of which were registered, the government said. Prosecutors said a loaded handgun was found in a case on the floorboard of the Caprice, in violation of Maryland law.

Martin's wife, Deborah Vinson, was "very upset" to learn about his arsenal, prosecutors said, and asked the FBI to take custody of the firearms because she was afraid that he would kill himself if he "thought it was all over."

If Martin had taken the classified material "for his own edification, as he has claimed, there would be no reason to keep some of it in his car, and arm himself as though he were trafficking in dangerous contraband," prosecutors said.

Radio Free Europe
Digital Trail Betrays Identity Of Russian 'Hacker' Detained In Prague
Thursday, 20 October 2016
Byline: Dmitry Treshchanin, Nick Shchetko

Prague - An investigation by RFE/RL's Current Time TV has determined that the Russian national accused by American officials of hacking U.S. targets and arrested earlier this month in the Czech capital is 29-year-old Moscow resident Yevgeny Nikulin.
Czech authorities this week said the suspect was detained in downtown Prague on October 5 in response to an Interpol warrant requested by the United States and now faces a Czech extradition hearing.

Czech police and local media have identified him only as "Yevgeniy N," and the Russian and U.S. governments revealed only that he was a Russian citizen.

Current Time's investigation uncovered Nikulin's Instagram account under the handle "i.tak.soidet," displaying a taste for luxury cars and jewelry and a digital trail that led through Belarus and Poland to the Czech Republic in the weeks before the Prague arrest.

The Instagram account went private shortly after Current Time's Russian-language report was published on October 20. Soon after that, Russian Foreign Ministry spokeswoman Maria Zakharova confirmed Nikulin's identity for journalists in Moscow.

"The Russian Foreign Ministry and the Russian Embassy in Prague are actively working with the Czech authorities to prevent the extradition of a Russian citizen to the United States," she added.

The Instagram account contained numerous photographs that included a gold Rolex watch, a distinctive bracelet and sneakers, and a luxury Mercedes AMG GLE63 automobile that all match items shown in a video of the arrest released by Czech police.

A social-media friend of Nikulin's who asked not to be identified told Current Time that Nikulin was "an idiot" for traveling abroad and that "he knew about Interpol."

The last post to the i.tak.soidet Instagram account appeared on October 11, six days after Nikulin's arrest. It is a simple text message that says, "I will return soon, what's all the fuss?" and was tagged "Prague Old Town."

One of the Instagram road photos from the days before the detention shows Nikulin's Mercedes apparently in Poland, and has a comment from a user asking, "What about Interpol?"

Current Time was also able to learn the license-plate number of Nikulin's Mercedes, which appears to match the blurred number shown in the video released by the Czech police.

It is unclear exactly what role Nikulin is suspected of playing in the alleged U.S. website hacks or even which websites were involved. A spokesperson from the U.S. Embassy in Prague confirmed that a Russian had been detained who was "suspected of hacking U.S. targets."

Hours after news emerged of the arrest, the professional networking service LinkedIn issued a statement suggesting the development was connected to a 2012 breach of its members' information. In May, LinkedIn acknowledged that intrusion compromised more than 100 million of its users' passwords.

The social-media friend who spoke with Current Time described Nikulin as "a young genius" who "now will be working for the government in the United States." The i.tak.soidet Instagram account, however, does not hint at any specific expertise in computers.

The i.tak.soidet account is popular, with nearly 44,000 followers and most of his posts garnering hundreds, or even thousands, of "likes."

'A Successful Entrepreneur'

In a 2015 interview with the Russian car website AvtoRambler, Nikulin describes his experience of owning Lamborghini cars. He is described as "a very busy young man."

"Yevgeny is already a successful entrepreneur whose business interests include a construction firm, an automobile service garage, and a company that sells luxury watches. As you can see from our interview," the article states, "the Huracan is not his first Lamborghini."

He boasts of owning a Bentley, a Continental GT, and a Mercedes-Benz G-Class.

No date has been set for Nikulin's extradition hearing, but Czech authorities said the man would remain in custody until that process.

The Russian Embassy in Prague told Current Time that Moscow will be seeking his return to Russia. Moscow, an embassy source said, rejects "the U.S. practice of forcing the entire world to enforce its extraterritorial jurisdiction."

Interpol had issued a so-called Red Notice for the alleged Russian hacker, a designation for "wanted international fugitives."

President Barack Obama's administration on October 7 explicitly pointed to Russia as the alleged director of recent cyberattacks and leaks seemingly aimed at disrupting the U.S. elections in November, citing e-mails and digital intrusions on a range of election-related institutions. A week later, Vice President Joe Biden said the United States was "sending a message" over Russia's apparent role in the digital attacks and Russian President Vladimir Putin would get it.

Putin's spokesman and other Russian officials have downplayed such allegations and suggested that they are "dirty tricks" and Americans should pay more attention to the information contained in the leaks.

ABC News
NSA Can Access More Phone Data Than Ever
Thursday, 20 October 2016
Byline: Lee Ferran

Washington - One of the reforms designed to rein in the surveillance authorities of the National Security Agency has perhaps inadvertently solved a technical problem for the spy outfit and granted it potential access to much more data than before, a former top official told ABC News.
Before the signing of the USA Freedom Act in June 2015, one of the NSA's most controversial programs was the mass collection of telephonic metadata from millions of Americans -- the information about calls, including the telephone numbers involved, the time and the duration but not the calls' content -- under a broad interpretation of the Patriot Act's Section 215. From this large "haystack," as officials have

called it, NSA analysts could get approval to run queries on specific numbers purportedly linked to international terrorism investigations.

The problem for the NSA was that the haystack was only about 30 percent as big as it should've been; the NSA database was missing a lot of data. As The Washington Post reported in 2014, the agency was not getting information from all wireless carriers and it also couldn't handle the deluge of data that was coming in.

On the technical side, Chris Inglis, who served as the NSA's deputy director until January 2014, recently told ABC News that when major telecommunications companies previously handed over customer records, the NSA "just didn't ingest all of it."

"[NSA officials] were trying to make sure they were doing it exactly right," he said, meaning making sure that the data was being pulled in according to existing privacy policies. The metadata also came in various forms from the different companies, so the NSA had to reformat much of it before loading it into a searchable database.

Both hurdles meant that the NSA couldn't keep up, and of all the metadata the agency wanted to be available for specific searches internally, only about a third of it actually was.

But then the USA Freedom Act was signed into law, and now Inglis said, all that is "somebody else's problem."

The USA Freedom Act ended the NSA's bulk collection of metadata but charged the telecommunications companies with keeping the data on hand. The NSA and other U.S. government agencies now must request information about specific phone numbers or other identifying elements from the telecommunications companies after going through the Foreign Intelligence Surveillance Act (FISA) court and arguing that there is a "reasonable, articulable suspicion" that the number is associated with international terrorism.

As a result, the NSA no longer has to worry about keeping up its own database and, according to Inglis, the percentage of available records has shot up from 30 percent to virtually 100. Rather than one internal, incomplete database, the NSA can now query any of several complete ones.

The new system "guarantees that the NSA can have access to all of it," Inglis said.

NSA general counsel Glenn Gerstell made a brief reference to the increased capacity in a post for the Lawfare blog in January after terrorist attacks at home and abroad.

"Largely overlooked in the debate that has ensued in the wake of recent attacks is the fact that under the new arrangement, our national security professionals will have access to a greater volume of call records subject to query in a way that is consistent with our regard for civil liberties," he wrote.

Mark Rumold, a senior staff attorney at the Electronic Frontier Foundation, told ABC News he doesn't have much of a problem with the NSA's wider access to telephone data, since now the agency has to go through a "legitimate" system with "procedural protections" before jumping into the databases.

"Their ability to obtain records has broadened, but by all accounts, they're collecting a far narrower pool of data than they were initially," he said, referring to returns on specific searches. "They can use a type of legal process with a broader spectrum of providers than earlier. To me, that isn't like a strike against it. That's almost something in favor of it, because we've gone through this public process, we've had this debate, and this is where we settled on the scope of the authority we were going to give them."

Rumold said he's still concerned about the NSA's ability to get information on phone numbers linked to a number in question -- up to two "hops" away -- but he said the USA Freedom Act "remains a step in the right direction."

The trade-off of the new system, according to Inglis, is in the efficiency of the searches. Whereas in the past the NSA could instantaneously run approved searches of its database, now the agency must approach each telecommunications company to ask about a number and then wait for a response.

In his January post Gerstell acknowledged concerns that the new approach could be "too cumbersome to be effective" and said the NSA will report to Congress on how the arrangement is working. A representative for the NSA declined to tell ABC News if any problems have been encountered so far, and Rumold noted there has been no public evidence of any issues.

Inglis said he isn't terribly concerned if the searches are a little slower. It's a small price to pay, he said, for what he called an "additional safeguard" that could increase the public's confidence in what the NSA is and how it operates.

Baltimore Sun
NSA chief: Cyber adds 'whole other dimension' to Russia's attempts to manipulate U.S. affairs
Thursday, 20 October 2016
Byline: Ian Duncan

Baltimore - The head of the NSA said Thursday that Russia's hack of Democratic Party emails is consistent with its history of trying to manipulate and influence affairs in other countries -- but the scope of such operations has changed dramatically.
"Cyber adds a whole other dimension to this because it now enables individuals, actors, groups, nation states to acquire data at massive scale and then divulge that," Adm. Michael S. Rogers told cyber professionals at the sixth annual Cyber Maryland Conference in Baltimore.

The job now for the National Security Agency and other parts of the government, Rogers said, is to make sure that Americans continue to have confidence in the electoral system.

"As we work our way through this particular issue, that's always at the forefront of our minds," he said.

Online conflict between Russia and the United States that typically takes place out of public view has burst into the national consciousness during the presidential election with the theft of emails from the Democratic National Committee and the campaign of Hillary Clinton and their release through the website WikiLeaks and other sites.

The intelligence community took the unusual step this month of publicly naming Russia's "senior-most officials" as the culprits.

The CIA is weighing options for a counterattack, NBC News reported last week. The NSA could help.

Clinton hammered the point during her debate Wednesday with Republican nominee Donald Trump. Trump said he would condemn any Russian interference with the election, but declined to blame Russia for the hacks.

Rogers was asked about comments by one of his predecessors, Michael Hayden, who said this week that collecting emails sent by political operatives was a legitimate intelligence operation.

Rogers responded with a question.

"We need to step back as a nation and think about the implications of that," he said. "Is that something we're comfortable with?"

Motherboard (Vice)
How hackers broke into John Podesta and Colin Powell's Gmail accounts
Thursday, 20 October 2016
Byline: Lorenzo Franceschi-Bicchierai

New York - On March 19 of this year, Hillary Clinton's campaign chairman John Podesta received an alarming email that appeared to come from Google.
The email, however, didn't come from the internet giant. It was actually an attempt to hack into his personal account. In fact, the message came from a group of hackers that security researchers, as well as the US government, believe are spies working for the Russian government. At the time, however, Podesta didn't know any of this, and he clicked on the malicious link contained in the email, giving hackers access to his account.

Months later, on October 9, WikiLeaks began publishing thousands of Podesta's hacked emails. Almost everyone immediately pointed the finger at Russia, who is suspected of being behind a long and sophisticated hacking campaign that has the apparent goal of influencing the upcoming US elections. But there was no public evidence proving the same group that targeted the Democratic National Committee was behind the hack on Podesta-- until now.

The data linking a group of Russian hackers--known as Fancy Bear, APT28, or Sofacy--to the hack on Podesta is also yet another piece in a growing heap of evidence pointing toward the Kremlin. And it also shows a clear thread between apparently separate and independent leaks that have appeared on a website called DC Leaks, such as that of Colin Powell's emails; and the Podesta leak, which was publicized on WikiLeaks.

All these hacks were done using the same tool: malicious short URLs hidden in fake Gmail messages. And those URLs, according to a security firm that's tracked them for a year, were created with Bitly account linked to a domain under the control of Fancy Bear.

THE TRAIL THAT LEADS TO FANCY BEAR

The phishing email that Podesta received on March 19 contained a URL, created with the popular Bitly shortening service, pointing to a longer URL that, to an untrained eye, looked like a Google link.

Inside that long URL, there's a 30-character string that looks like gibberish but is actually the encoded Gmail address of John Podesta. According to Bitly's own statistics, that link, which has never been published, was clicked two times in March.

That's the link that opened Podesta's account to the hackers, a source close to the investigation into the hack confirmed to Motherboard.

That link is only one of almost 9,000 links Fancy Bear used to target almost 4,000 individuals from October 2015 to May 2016. Each one of these URLs contained the email and name of the actual target. The hackers created them with with two Bitly accounts in their control, but forgot to set those accounts to private, according to SecureWorks, a security firm that's been tracking Fancy Bear for the last year.

SecureWorks was tracking known Fancy Bear command and control domains. One of these lead to a Bitly shortlink, which led to the Bitly account, which led to the thousands of Bitly URLs that were later connected to a variety of attacks, including on the Clinton campaign. With this privileged point of view, for example, the researchers saw Fancy Bear using 213 short links targeting 108 email addresses on the hillaryclinton.com domain, as the company explained in a somewhat overlooked report earlier this summer, and as BuzzFeed reported last week.

Using Bitly allowed "third parties to see their entire campaign including all their targets-- something you'd want to keep secret," Tom Finney, a researcher at SecureWorks, told Motherboard.

It was one of Fancy Bear's "gravest mistakes," as Thomas Rid, a professor at King's College who has closely studied the case, put it in a new piece published on Thursday in Esquire, as it gave researchers unprecedented visibility into the activities of Fancy Bear, linking different parts of its larger campaign together.

This is how researchers have been able to find the phishing link that tricked Colin Powell and got him hacked. This also allowed them to confirm other public reports of compromises, such as that of William Rinehart, a staffer with Clinton's presidential campaign. As The Smoking Gun reported in August, Rinehart received a malicious Google security alert on March 22, according to a screenshot Rinehart shared with the site. SecureWorks found a URL that had Rinehart's Gmail address encoded, which had the same date.

Similar malicious emails and short URLs have also been used recently against independent journalists from Bellingcat, a website that has investigated the incident of the shootdown of Malaysian Airlines Flight 17 (MH17) over Ukraine in 2014, finding evidence that Russian-backed rebels were behind it.

Other journalists in eastern Europe have also recently been targeted with phishing emails trying to break into their Gmail accounts.

These malicious emails, just like the ones used against Podesta, Powell, Rinehart and many others, looked like Google alerts, and contained the same type of encoded strings hiding the victims' names.

It's unclear why the hackers used the encoded strings, which effectively reveal their targets to anyone. Kyle Ehmke, a threat intelligence researcher at security firm ThreatConnect, argued that "the strings might help them keep track of or better organize their operations, tailor credential harvesting pages to specific victims, monitor the effectiveness of their operations, or diffuse their operations against various targets across several URLs to facilitate continuity should one of the URLs be discovered."

The use of popular link shortening services such as Bitly or Tinyurl might have a simpler explanation. According to Rid, the hackers probably wanted to make sure their phishing attempts went past their targets' spam filters.

THE SMOKING GUN?

None of this new data constitutes a smoking gun that can clearly frame Russia as the culprit behind the almost unprecedented hacking campaign that has hit the DNC and several other targets somewhat connected to the US presidential election.

Almost two weeks ago, the US government took the rare step of publicly pointing the finger at the Russian government, accusing it of directing the recent string of hacks and data breaches. The

intelligence community declined to explain how they reached their conclusion, and it's fair to assume they have data no one else can see.

This newly uncovered data paints an even clearer picture for the public, showing a credible link between the several leaking outlets chosen by the hackers, and, once again, pointing toward Fancy Bear, a notorious hacking group that's widely believed to be connected with the Russian government. While there are still naysayers, including presidential candidate and former reality TV star Donald Trump, for many, the debate over who hacked the DNC, and who's behind all this hacking, is pretty much closed.

"We are approaching the point in this case where there are only two reasons for why people say there's no good evidence," Rid told me. "The first reason is because they don't understand the evidence--because the don't have the necessary technical knowledge. The second reason is they don't want to understand the evidence."

Wired (UK)
Hackers are not as 'sophisticated as they think they are'
Thursday, 20 October 2016
Byline: Matthew Levy

London - The way we talk about cyberattacks has created a culture of fear around online security, said Ian Levy, technical director at the National Centre for Cyber Security. The newly-formed offshoot of GCHQ will be responsible for coordinating UK cybersecurity efforts and keeping the UK safe from online threats.
"The context in which you judge something also influences how you interpret it," he told the audience at WIRED Security in London. Media coverage of cyberattacks is crammed full of scary buzzwords. Cyberattacks - invariably represented by a lone hooded teenager in a dark room - are described as 'sophisticated' and 'unprecedented.'

Levy pins at least part of the blame for this language on the cybersecurity industry itself. "There is no other bit of public policy where the tone is set by a group of massively incentivised people," he said. Once they've got people sufficiently scared about cyber threats, security companies offer up what Levy describes as "magic amulets" - miracle defences which promise to defend against any and every attack.

Case in point: the Air Gap. Levy set up a website showcasing a magic amulet of his own creation. Like many cyber defences, his piece of hardware promised to defend against all known and unknown viruses, and stop zero day exploits. His product? An empty box with a blue blinking light on it. Levy had to take his website offline when he started getting sales enquiries by email.

The ex-GCHQ director takes exception with one cybersecurity phrase in particular: 'advanced persistent threats'. Levy prefers to use the phrase 'adequate pernicious toerags' - most cyberattackers, he said, just do the bare minimum to overcome cyber defences and don't pose much of a threat at all.

The government, too, deserves its share of the blame for public confusion over cybersecurity. "We have to change the advice we give and the way we talk about it," Levy said. Rather than telling people not to click on links within suspicious emails, the NCSC is working on making sure that UK citizens never get those emails in the first place.

Levy plans to introduce DMARC (which stands for domain- based message authentication, reporting and conformance) on to all 6,000 government domains. This would stop people receiving malicious mail from websites pretending to be associated with government agencies. Once they've done that, Levy said, "we're going to point and laugh at everyone that doesn't do the same."

If it works (and initial tests have already proven promising), the NCSC will recommend DMARC to the private sector too. "Let's publish what we've done, what effect it's had, and the cost," he said. "By default, let's protect people."

Le Monde
Surveillance hertzienne : le Conseil constitutionnel censure la loi renseignement
Friday, 21 October 2016
Byline: Jean-Baptiste Jacquin

Paris - La disposition contestée permettait de s'affranchir du code de procédure pénale, et de se dispenser de l'avis de la Commission nationale de contrôle des techniques de renseignement.
C'est un petit article de loi en vigueur depuis vingt-cinq ans que le Conseil constitutionnel a censuré dans une décision rendue vendredi 21octobre. Cet article permettait tout bonnement aux services de renseignement de procéder sans le moindre contrôle à la surveillance de communications par voie hertzienne. Les gardiens de la Constitution le déclarent contraire à l'article2 de la Déclaration des droits de l'homme et du citoyen de 1789 en portant «une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances». Ils le déclarent inconstitutionnel et demandent au législateur d'élaborer un nouveau texte d'ici le 31décembre 2017.

Au nom de «la défense des intérêts nationaux» , les pouvoirs publics pouvaient ainsi surveiller les déplacements de sous-marins étrangers ou les mouvements de troupes sur un théâtre d'opération, mais également des communications par téléphone mobile entre particuliers, des échanges par Wi-Fi ou Bluetooth. Rebaptisé article L.811-5 dans la loi renseignement de juillet2015, cet article permettait aux services de renseignement de s'affranchir des contrôles que cette loi imposait en précisant par exemple que la surveillance de particuliers ne peut être autorisée par le premier ministre qu'après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR).

«Un trou législatif béant»

C'est en invoquant cette disposition particulièrement floue que Bernard Squarcini, l'ancien patron de la Direction centrale du renseignement intérieur (DCRI), avait pris la liberté de procéder à des écoutes dans l'affaire des fadettes du Monde . Lors du débat sur la loi renseignement de 2015, quelques mois après les attentats contre Charlie Hebdo et l'Hyper Cacher, personne ne semblait s'être intéressé à cet article introduit par la loi de 1991 sur le secret des correspondances. Cette dernière avait elle-même été votée après le scandale des écoutes de l'Elysée où François Mitterrand avait fait écouter des personnalités, dont le journaliste du Monde Edwy Plenel.

Le Conseil constitutionnel s'était prononcé en juillet2015 sur la loi renseignement, en censurant d'ailleurs deux dispositions, mais n'avait validé que les articles qui lui avaient été soulignés dans les saisines du président de la République et du président du Sénat. Il ne s'était jamais saisi de ce sujet avant la question prioritaire de constitutionnalité déposée au printemps par des associations (La Quadrature du Net, French Data Network, la Fédération des fournisseurs d'accès à Internet associatifs et Igwan.net). Selon leur avocat, Patrice Spinosi, il a créé «un trou législatif béant» et ouvert «la voie à un espionnage de masse» , a-t-il expliqué à l'audience, le 11octobre.

L'article, très court, dit: «Les mesures prises par les pouvoirs publics pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne ne sont pas soumises aux dispositions du présent livre, ni à celles de la sous-section2 de la section3 du chapitreIer du titreIII du livreIer du code de procédure pénale.» Dans sa décision, le Conseil constitutionnel note que la disposition contestée permettait de fait de s'affranchir du code de procédure pénale qui encadre les écoutes ordonnées par un juge d'instruction.

Deux réserves transitoires

Balayant les observations du gouvernement et reprenant les arguments des associations, l'institution présidée par Laurent Fabius souligne que la rédaction du texte incriminé n'interdit pas des mesures de surveillance «utilisées à des fins plus larges que la seule mise en oeuvre de» la défense des intérêts nationaux. Surtout, écrit-elle, le recours à ces mesures n'est soumis «à aucune condition de fond ni de procédure» et leur mise en oeuvre n'est encadrée par «aucune garantie» . Aucune limite sur l'exploitation des données personnelles ni leur conservation n'était prévue...

Pour ne pas empêcher les services de renseignement de continuer à opérer des écoutes qui relèveraient réellement de la défense nationale, le Conseil n'abroge pas la loi mais encadre sérieusement son application. En attendant qu'un nouveau texte de loi soit voté, il impose deux «réserves transitoires». Les mesures de surveillance ne pourront pas s'appliquer aux écoutes soumises à autorisation par la loi renseignement, et la CNCTR devra être «régulièrement informée» des opérations mises en oeuvre. La nouvelle législature qui sortira des urnes en juin aura quelques mois pour faire le tri entre ce qui relève des surveillances susceptibles de porter atteinte à la vie privée et les autres.

New York Times

Private Security Group Says Russia Was Behind Hack of Clinton Campaign Chairman
Friday, 21 October 2016
Byline: Nicole Perlroth, Michael D. Shear

San Francisco - At the start of 2014, President Obama assigned his trusted counselor, John D. Podesta, to lead a review of the digital revolution, its potential and its perils. When Mr. Podesta presented his findings five months later, he called the internet's onslaught of big data "a historic driver of progress." But two short years later, as chairman of Hillary Clinton's presidential campaign, Mr. Podesta would also become one of the internet's most notable victims.
On Thursday, private security researchers said they had concluded that Mr. Podesta was hacked by Russia's foreign intelligence service, the GRU, after it tricked him into clicking on a fake Google login page last March, inadvertently handing over his digital credentials.

For months, the hackers mined Mr. Podesta's inbox for his most sensitive and potentially embarrassing correspondence, much of which has been posted on the WikiLeaks website. Additions to the collection on Thursday included three short email exchanges between Mr. Podesta and Mr. Obama himself in the days leading up to his election in 2008.

Mr. Podesta's emails were first published by WikiLeaks earlier this month. The release came just days after James R. Clapper Jr., the director of national intelligence, and the Department of Homeland Security publicly blamed Russian officials for cyberattacks on the Democratic National Committee, in what they described as an effort to influence the American presidential election.

To date, no government officials have offered evidence that the same Russian hackers behind the D.N.C. cyberattacks were also behind the hack of Mr. Podesta's emails, but an investigation by the private security researchers determined that they were the same.

Threat researchers at Dell SecureWorks, an Atlanta-based security firm, had been tracking the Russian intelligence group for more than a year. In June, they reported that they had uncovered a critical tool in the Russian spy campaign. SecureWorks researchers found that the Russian hackers were using a popular link shortening service, called Bitly, to shorten malicious links they used to send targets fake Google login pages to bait them into submitting their email credentials.

The hackers made a critical error by leaving some of their Bitly accounts public, making it possible for SecureWorks to trace 9,000 of their links to nearly 4,000 Gmail accounts targeted between October 2015 and May 2016 with fake Google login pages and security alerts designed to trick users into turning over their passwords.

Among the list of targets were more than 100 email addresses associated with Hillary Clinton's presidential campaign, including Mr. Podesta's. By June, 20 staff members for the campaign had clicked on the short links sent by Russian spies. In June, SecureWorks disclosed that among those whose email

accounts had been breached were staff members who advised Mrs. Clinton on policy and managed her travel, communications and campaign finances.

Two security researchers who have been tracking the GRU's spearphishing campaign confirmed Thursday that Mr. Podesta was among those who had inadvertently turned over his Google email password. The fact that Mr. Podesta was among those breached by the GRU was first disclosed Thursday by Esquire and VICE Motherload blog, which published the link Russian spies used against Mr. Podesta.

"The new public data confirming the Russians are behind the hack of John Podesta's email is a big deal," Jake Sullivan, Mrs. Clinton's senior policy adviser, said Thursday. "There is no longer any doubt that Putin is trying to help Donald Trump by weaponizing WikiLeaks."

The new release of Mr. Podesta's email exchange with Mr. Obama from 2008 made clear that Mr. Obama's team was confident he would win.

In one of the emails, Mr. Podesta wrote Mr. Obama a lengthy memo in the evening on Election Day recommending that he not accept an invitation from President George W. Bush to attend an emergency meeting of the Group of 20 leaders.

"Attendance alongside President Bush will create an extremely awkward situation," the memo said. "If you attempt to dissociate yourself from his positions, you will be subject to criticism for projecting a divided United States to the rest of the world. But if you adopt a more reserved posture, you will be associated not only with his policies, but also with his very tenuous global standing."

The White House did not respond to questions about the email.

London Daily Telegraph
GCHQ using cyber attacks on Isil to aid battle to take Mosul
Friday, 21 October 2016
Byline: Ben Farmer

London - GCHQ is using cyber warfare for the first time against Isil militants as part of the campaign to retake Mosul, the Defence Secretary has said.
The cyber attacks are understood to have targeted the communications of Islamic State of Iraq and the Levant to disrupt co-ordination in the Iraqi city.

Sir Michael Fallon told a conference organised by the Royal United Services Institute, a think tank on cyber warfare: "We are conducting military operations against Daesh [Isil] as part of the international coalition, and I can confirm that we are using offensive cyber for the first time in this campaign." He said £265 million is being pumped into "rooting out cyber vulnerabilities" in military and wider cyber-systems.

Esquire
How Russia Pulled Off the Biggest Election Hack in U.S. History
Friday, 21 October 2016
Byline: Thomas Rid

New York - On an April afternoon earlier this year, Russian president Vladimir Putin headlined a gathering of some four hundred journalists, bloggers, and media executives in St. Petersburg. Dressed in a sleek navy suit, Putin looked relaxed, even comfortable, as he took questions. About an hour into the forum, a young blogger in a navy zip sweater took the microphone and asked Putin what he thought of the "so- called Panama Papers."
The blogger was referring to a cache of more than eleven million computer files that had been stolen from Mossack Fonseca, a Panamanian law firm. The leak was the largest in history, involving 2.6 terabytes of data, enough to fill more than five hundred DVDs. On April 3, four days before the St. Petersburg forum, a group of international news outlets published the first in a series of stories based on the leak, which had taken them more than a year to investigate. The series revealed corruption on a massive scale: Mossack Fonseca's legal maneuverings had been used to hide billions of dollars. A central theme of the group's reporting was the matryoshka doll of secret shell companies and proxies, worth a reported $2 billion, that belonged to Putin's inner circle and were presumed to shelter some of the Russian president's vast personal wealth.

When Putin heard the blogger's question, his face lit up with a familiar smirk. He nodded slowly and confidently before reciting a litany of humiliations that the United States had inflicted on Russia. Putin reminded his audience about the sidelining of Russia during the 1998 war in Kosovo and what he saw as American meddling in Ukraine more recently. Returning to the Panama Papers, Putin cited WikiLeaks to insist that "officials and state agencies in the United States are behind all this." The Americans' aim, he said, was to weaken Russia from within: "to spread distrust for the ruling authorities and the bodies of power within society."

Though a narrow interpretation of Putin's accusation was defensible--as WikiLeaks had pointed out, one of the members of the Panama Papers consortium had received financial support from USAID, a federal agency--his swaggering assurance about America's activities has a more plausible explanation: Putin's own government had been preparing a vast, covert, and unprecedented campaign of political sabotage against the United States and its allies for more than a year.

The Russian campaign burst into public view only this past June, when The Washington Post reported that "Russian government hackers" had penetrated the servers of the Democratic National Committee. The hackers, hiding behind ominous aliases like Guccifer 2.0 and DC Leaks, claimed their first victim in July, in the person of Debbie Wasserman Schultz, the DNC chair, whose private emails were published by WikiLeaks in the days leading up to the Democratic convention. By August, the hackers had learned to use the language of Americans frustrated with Washington to create doubt about the integrity of the

electoral system: "As you see the U. S. presidential elections are becoming a farce," they wrote from Russia.

The attacks against political organizations and individuals absorbed much of the media's attention this year. But in many ways, the DNC hack was merely a prelude to what many security researchers see as a still more audacious feat: the hacking of America's most secretive intelligence agency, the NSA.

Russian spies did not, of course, wait until the summer of 2015 to start hacking the United States. This past fall, in fact, marked the twentieth anniversary of the world's first major campaign of state-on-state digital espionage. In 1996, five years after the end of the USSR, the Pentagon began to detect high-volume network breaches from Russia. The campaign was an intelligence- gathering operation: Whenever the intruders from Moscow found their way into a U. S. government computer, they binged, stealing copies of every file they could.

By 1998, when the FBI code-named the hacking campaign Moonlight Maze, the Russians were commandeering foreign computers and using them as staging hubs. At a time when a 56 kbps dial-up connection was more than sufficient to get the best of Pets.com and AltaVista, Russian operators extracted several gigabytes of data from a U. S. Navy computer in a single session. With the unwitting help of proxy machines--including a Navy supercomputer in Virginia Beach, a server at a London nonprofit, and a computer lab at a public library in Colorado--that accomplishment was repeated hundreds of times over. Eventually, the Russians stole the equivalent, as an Air Intelligence Agency estimate later had it, of "a stack of printed copier paper three times the height of the Washington Monument."

The Russians' tactics became more sophisticated over time; they even hacked satellites to cover their tracks. But while the American code names used to track the Russian effort changed--from Moonlight Maze to Storm Cloud to Makers Mark--the operation itself never really stopped. Over the next two decades, the FSB (successor to the KGB) and the GRU (Russia's premier military intelligence organization) went after political and military targets, while the NSA and the UK's GCHQ returned the favor.

This sort of espionage was business as usual, a continuation of long-standing practice. And during the cold war, both the USSR and the United States subtly, and sometimes covertly, interfered with foreign elections. What changed over the past year, however--what made the DNC hack feel new and terrifying--was Russia's seeming determination to combine the two. For the first time, Russia used a hacking operation, one that collected and released massive quantities of stolen information, to meddle in an American presidential election. The inspiration and template for this new attack was a poisonous cocktail of fact and fabrication that the Russians call kompromat, for "compromising material."

Kompromat had been deployed by the Soviet Union since at least the 1950s, but in 1999 the Kremlin gave the tactic a high-tech update. With parliamentary elections fast approaching, and with post-USSR corruption at a peak, the government of president Boris Yeltsin used anonymous websites to sling mud

at opposition candidates. One notorious kompromat repository was run specifically to slander the mayor of Moscow, a rising star in the opposition with his eyes on the presidency. In 2009, a senior British diplomat working in Russia was forced to resign after the appearance online of a four-minute video that showed him having sex with two blond women in a brothel.

One of the first American targets of kompromat was Victoria Nuland, who served as the top U. S. diplomat for Europe during Obama's second term. In February 2014, at the peak of the crisis in Ukraine, Nuland was surreptitiously recorded while speaking on the phone with the U. S. ambassador to Kiev. Frustrated with Europe's lackluster response to the Ukrainian crisis, Nuland said, "Fuck the EU." Shortly after, an aide to the Russian deputy prime minister tweeted a link to a recording of the intercepted phone call. The State Department called the leak "a new low in Russian tradecraft."

The Nuland leak prompted a minor diplomatic hiccup between the European Union and the United States. But the kompromat campaign of the past year appears to be aimed at much bigger game: the American electoral system. According to Reuters, the FBI first contacted the DNC in the fall of 2015, obliquely warning the Democrats to examine their network. It wasn't until May, however, that the DNC asked for help from a cybersecurity company called CrowdStrike, which had experience identifying digital espionage operations by nation-states. CrowdStrike immediately discovered two sophisticated groups of spies that were stealing documents from the Democrats by the thousands.

CrowdStrike was soon able to reconstruct the hacks and identify the hackers. One of the groups, known to the firm as Cozy Bear, had been rummaging around the DNC since the previous summer. The other, known as Fancy Bear, had broken in not long before Putin's appearance at the St. Petersburg forum. Surprisingly, given that security researchers had long suspected that both groups were directed by the Russian government, each of the attackers seemed unaware of what the other was doing.

Meanwhile a mysterious website named DC Leaks was registered on April 19. In early June, a Twitter account associated with the site started linking to the private conversations of Philip Breedlove, who had been, until a few weeks earlier, NATO's Supreme Allied Commander in Europe. DC Leaks was well designed, but nobody seems to have noticed it until early July.

On June 14, less than an hour after The Washington Post reported the breach at the DNC, CrowdStrike posted a report that detailed the methods used by the intruders. The firm also did something unusual: It named the Russian spy agencies it believed responsible for the hack. Fancy Bear, the firm said, worked in a way that suggested affiliation with the GRU. Cozy Bear was linked to the FSB.

The day after the Post story broke, a website appeared that claimed to belong to a hacker who identified himself as Guccifer 2.0. (Guccifer was the nickname of a Romanian hacker who, among other things, broke into the email account of George W. Bush's sister.) The operators, posing as Guccifer 2.0, dismissed CrowdStrike's attribution, insisting instead that the DNC had been "hacked by a lone hacker." As proof, Guccifer published eleven documents from the DNC, including an opposition- research file on Donald Trump and a list of major Democratic donors. In the weeks that followed, Guccifer offered

interviews and batches of documents to several journalists, but he wrote that "the main part of the papers, thousands of files and mails, I gave to WikiLeaks."

Ultimately, more than two thousand confidential files from the DNC found their way to the public. Throughout the campaign, Guccifer maintained that he was the only person behind the hacking and leaking. "This is my personal project and I'm proud of it," he--or they--wrote in late June. But several sloppy mistakes soon revealed who was really behind the operation. The unraveling happened more quickly than anybody could have anticipated.

As soon as Guccifer's files hit the open Internet, an army of investigators--including old-school hackers, former spooks, security consultants, and journalists--descended on the hastily leaked data. Informal, self-organized groups of sleuths discussed their discoveries over encrypted messaging apps such as Signal. Many of the self-appointed analysts had never met in person, and sometimes they didn't know one another's real names, but they were united in their curiosity and outrage. The result was an unprecedented open-source counterintelligence operation: Never in history was intelligence analysis done so fast, so publicly, and by so many.

Matt Tait, a former GCHQ operator who tweets from the handle @pwnallthethings, was particularly prolific. Hours after the first Guccifer 2.0 dump, on the evening of June 15, Tait found something curious. One of the first leaked files had been modified on a computer using Russian-language settings by a user named "Feliks Dzerzhinsky." Dzerzhinsky was the founder of the Cheka, the Soviet secret police--a figure whose mythic renown was signaled by a fifteen-ton bronze statue that once stood in front of KGB headquarters. Tait tweeted an image of the document's metadata settings, which, he suggested, revealed a failure of operational security.

A second mistake had to do with the computer that had been used to control the hacking operation. Researchers found that the malicious software, or malware, used to break into the DNC was controlled by a machine that had been involved in a 2015 hack of the German parliament. German intelligence later traced the Bundestag breach to the Russian GRU, aka Fancy Bear.

There were other errors, too, including a Russian smile emoji--")))"--and emails to journalists that explicitly associated Guccifer 2.0 with DC Leaks, as the cybersecurity firm ThreatConnect pointed out. But the hackers' gravest mistake involved the emails they'd used to initiate their attack. As part of a so-called spear- phishing campaign, Fancy Bear had emailed thousands of targets around the world. The emails were designed to trick their victims into clicking a link that would install malware or send them to a fake but familiar-looking login site to harvest their passwords. The malicious links were hidden behind short URLs of the sort often used on Twitter.

To manage so many short URLs, Fancy Bear had created an automated system that used a popular link-shortening service called Bitly. The spear-phishing emails worked well--one in seven victims revealed their passwords--but the hackers forgot to set two of their Bitly accounts to "private." As a result, a cybersecurity company called SecureWorks was able to glean information about Fancy Bear's targets.

Between October 2015 and May 2016, the hacking group used nine thousand links to attack about four thousand Gmail accounts, including targets in Ukraine, the Baltics, the United States, China, and Iran. Fancy Bear tried to gain access to defense ministries, embassies, and military attachés. The largest group of targets, some 40 percent, were current and former military personnel. Among the group's recent breaches were the German parliament, the Italian military, the Saudi foreign ministry, the email accounts of Philip Breedlove, Colin Powell, and John Podesta--Hillary Clinton's campaign chairman--and, of course, the DNC.

The rapid public reconstruction of the DNC break-in appears to have caught the hackers off guard. Researchers surmised that the Russian spies had not expected to be identified so quickly, a theory that would explain, among other things, the peculiar animus Guccifer seemed to have for CrowdStrike. According to this hypothesis, the tradecraft blunders that Tait and others had identified were the result of a hasty effort by the GRU to cover its tracks.

As if to regroup after the initial rush of activity, Guccifer and DC Leaks went quiet at the end of June. But the 2016 presidential campaign, already the most bizarre in living memory, had a further surprise in store, one that worked in favor of the Russians. At a time when only 32 percent of Americans say that they trust the media to report the news fairly and accurately, the hackers were about to learn that getting called out publicly didn't really matter: Their kompromat operations would still work just fine.

On July 22, three days before the Democratic National Convention in Philadelphia, WikiLeaks published the largest trove of files to date, which included nearly twenty thousand hacked emails. Press coverage of the release quickly centered on emails that suggested a bias among some DNC staffers in favor of Hillary Clinton. The leaked emails lent credence to a suspicion held by some Democrats that the party establishment had never intended to give Bernie Sanders, Clinton's opponent in the primaries, a fair shake. Protesters in Philadelphia held up signs that read election fraud and dnc leaks shame. One day before the convention, the Russian kompromat campaign took its first trophy: Debbie Wasserman Schultz, the DNC chair, resigned from the organization.

The episode shocked the Democratic establishment, not least because of what it augured for the future. As Clinton's lead in the polls widened after the convention, commentators began to speculate that a damaging leak late in the campaign might be the only chance for Donald Trump to win the election. Fears of a Russia-sponsored October surprise grew as it became clearer that the subversion effort was improving. When files appeared, they were now scrubbed of the sort of distinguishing metadata that had allowed analysts to trace the leak back to Russian intelligence.

The operators behind Guccifer and DC Leaks also appear to have recognized that American journalists were desperate for scoops, no matter their source. The Russians began to act like a PR agency, providing access to reporters at Politico, The Intercept, and BuzzFeed. Journalists were eager to help. On August 27, when part of the DC Leaks website was down for some reason, Twitter suspended the @DCLeaks account. The Daily Caller, a conservative news website, posted a story about the events, drawing an

outcry from Trump supporters. Lou Dobbs, the Fox Business anchor, sneered that "leftist fascism" was throttling the last best hope for a Trump victory. Twitter soon reinstated @DCLeaks.

The most effective outlet by far, however, was WikiLeaks. Russian intelligence likely began feeding hacked documents to Julian Assange's "whistleblower" site in June 2015, after breaching Saudi Arabia's foreign ministry. A group called WikiSaudiLeaks, probably a Guccifer-like front for Fancy Bear, claimed that "WikiLeaks have been given access to some part of these documents." The so-called Saudi Cables showed princes buying influence and monitoring dissidents. They became a major news story, proving that the old methods worked even better in the twenty-first century.

A leak released at the end of this past summer showed how frictionlessly the kompromat campaign was able to operate in the fact-free atmosphere of the 2016 American presidential campaign. In late September, DC Leaks published hundreds of emails from the account of a twenty-two-year-old freelancer for the Clinton campaign. Lachlan Markay, a reporter for The Washington Free Beacon, found an audio clip buried deep in the cache. In the recording, which was made at a fundraiser in Virginia, Hillary Clinton could be heard describing Sanders supporters as "children of the Great Recession" who "are living in their parents' basement." The comments were clumsy but, in context, hardly damning; Clinton was describing the appeal of Sanders's "political revolution" for young voters. ("We want people to be idealistic," she said.) Nevertheless, within a few days, Donald Trump was telling a roaring crowd in Pennsylvania, "Clinton thinks Bernie supporters are hopeless and ignorant basement dwellers."

In mid-August, when Guccifer and DC Leaks were making near-daily news, a third mysterious social-media account popped up out of nowhere. A group calling itself the Shadow Brokers announced that it had published "cyberweapons" that belonged to the NSA on file-sharing sites such as Github. The group said that it would soon hold an auction to sell off a second cache of tools. After a security researcher posted a link to a repository of the supposed NSA software, analysts flocked to the dump. Security researchers quickly discovered that the tools, a collection of malware designed to steal data from their targets, were the real thing. Crucially, The Intercept, a media outlet with access to the NSA files leaked by Edward Snowden, found a sixteen-character string ("ace02468bdf13579") in the Shadow Brokers' tools that was referenced in a top-secret, and previously unpublished, NSA manual. The connection proved the provenance of the Shadow Brokers' find.

Robbing the NSA, of course, is not easy. The agency's elite hacking unit, called Tailored Access Operations, has an internal network known as the "high side" that is physically segregated from the Internet (the "low side"). Data diodes, devices that allow data to flow one way only, like water from a faucet, make it nearly impossible to hack high-side computers from the low side. When TAO hackers want to attack an adversary, they move their tools from the high side to a server on the low side, navigate through a series of addresses that make their tracks difficult to trace, and install malware on their target. To steal the NSA's malware, the Shadow Brokers had to compromise a low-side machine that the TAO was using to hack its targets. The Shadow Brokers likely got lucky: Some analysts believe that an NSA operator mistakenly uploaded a whole set of tools to a staging computer the hackers were already watching. The alternative theory: an old-fashioned mole passed on the tools.

After going to all that trouble, why publish the results? A possible answer is suggested by a surprising discovery made by the U. S. intelligence community around the time Putin was addressing the journalists in St. Petersburg. American investigators had long known that the Russians were doing more than spear-phishing, but sometime around April they learned that the intruders were using commercial cloud services to "exfiltrate" data out of American corporations and political targets. Cozy Bear, the hacking group believed to be affiliated with the FSB, used some two hundred Microsoft OneDrive accounts to send data from its victims back to Moscow.

Using cloud services such as OneDrive was a clever but risky move-- it was a little like taking the bus to make off with stolen goods from a burglary. Though the widespread use of the services by legitimate users offered a degree of cover for the hackers, data provided by Microsoft also helped America's elite digital spies identify the DNC intruders "with confidence" as Russian. It is even possible that the U. S. government has been able to identify the names and personal details of individual operators. The Russians knew they'd been caught. On July 30, an FSB press release announced that twenty government and defense organizations had been hit by high-powered spying tools.

Some intelligence analysts believe that the Shadow Brokers' publication of the NSA spy kit was a message from one group of professionals to another. "You see us?" the Russians seemed to be saying, perhaps in reference to ongoing U. S. efforts to investigate the DNC breach. "Fine, but we see you, too." Similarly, the announcement of an auction--all but certainly phony--was probably intended as a warning that the hackers were prepared to publish a key that would unlock an encrypted container holding a second batch of stolen tools. Like a severed ear in an envelope, the announcement told the Americans: Don't mess with us.

Meanwhile, the kompromat campaign proceeded apace. August and September each saw six data dumps, including files from the Democratic Congressional Campaign Committee, which had also been hacked. In October, as the presidential election drew near, Guccifer published a massive cache, more than twenty-one hundred files. Three days later, WikiLeaks began publishing thousands of emails stolen from John Podesta's account.

On the day WikiLeaks published the first batch of Podesta's emails, the U. S. government took the unprecedented step of announcing that it was "confident" Russia's "seniormost officials" had authorized the DNC hacks. So far U. S. investigators have not said publicly who was responsible for the Podesta hack, but the data harvested by SecureWorks makes it clear that Fancy Bear broke into the Clinton chairman's account as early as late March. The CIA briefed Trump about the origin of the kompromat, but he continued to cite the material, telling a Pennsylvania crowd, "I love WikiLeaks!"

On October 12, Putin appeared at another forum, this time with more than five hundred guests in Moscow. Sitting comfortably in front of a giant banner that said russia calling! he answered an audience question about the hacks. "Everyone is talking about who did it," Putin said. "Is it so important?" The former KGB officer, proving his full command of U. S. political intrigue, suggested that the Democrats

had "supported one intraparty candidate at the expense of the other." Any talk of the hacks being in Russia's interest, he said, was "hysteria" intended to distract Americans from what the hackers discovered: "the manipulation of public opinion." When the audience applauded, a smirk returned to Putin's face. "I think I answered your question," he said.

Wired (UK)
Can governments really keep us safe from terrorism without invading our privacy?
Thursday, 20 October 2016
Byline: Ruby Lott-Lavigna

London - GCHQ has many negative connotations attached to it - including illegally collecting data from the UK public - but David Omand, former head of GCHQ and now professor at Kings, is hoping for a change in the way goverments deal with our private information.
Referring to new legislation that is currently going through parliament - the 'Investigatory Powers Law' - he explained how regulation is being implemented to create transparency in the way the UK government deals with cybersecurity. "What is going on, as we speak, is a phase change in the relationship between the secret state and parliament," explained Omand. "One way of looking at this is that the secret activity of the state is now being fully bought under the modern rule of law."

In 2013, when the NSA scandal went public, the way governments mine data from its citizens became of public concern. No longer were the intelligence departments free to take what they wanted without public repercussion and outrage. "It kicked off a moral panic around Europe. It lead to investigations and endless court cases against the government."

However, in 2015 and 2016, when terrorists hit Paris, Orlando, Nice and other major cities around the world, intelligence agencies cited the attacks as the reason behind their rigorous stealing of data.

Omand explained how we'd reached this state of cyberthreat. "There were urgent demands for intelligence on those who mean us harm, but that coincided with the fact that we have been placing our personal intelligence in the digital world."

So where does the line stand with mining data for security reasons? Is there a balance to be reached between privacy and security? According to Omand, "2017 is the year of reconciliation, in which we recognise as a mature democracy, it is possible to have sufficient security and sufficient privacy."

"The key to that is rule of law. Courts have to have comprehensible, black letter law."

The Investigatory Powers Law is a new bill to, hopefully, provide transparency and regulation and judicial oversight. Various elements like communication data and meta-data, internet connection records, single and bulk interception and equipment interference or hacking will be regulated under this new law.

In light of this, Omand hopes that along with the new National Cyber Security Centre, that will be reporting to GCHQ ("their email address starts 'opendoor'" Omand boasted) a balance will be reached.

However, many are still skeptical. "I hope I've convinced you of this paradigm shift. It's a big change."

Omand currently serves as a Commissioner for the Global Commission on Internet Governance, and was the director of GCHQ from 1996 to 1997

He was appointed in 2002 the first UK Security and Intelligence Coordinator, having previously been Permanent Secretary of the Home Office 1997 to 2001 and before that the Director of GCHQ, the UK's intelligence and cyber-security organisation.

Globe and Mail
RCMP's counterterrorism centre in Ottawa serves as intersection of information
Monday, 24 October 2016
Byline: Colin Freeze

Ottawa - The Mounties have created a permanent place for counterterrorism detectives to work shoulder-to-shoulder - and database to database - with federal border guards, immigration officials and spy-agency analysts.
The RCMP's national-security joint-operations centre (NSJOC) in Ottawa is a "real-time and rapid information-sharing" crossroads where federal agents can efficiently swap files, according to recently released records. However, critics fear it will go places no watchdog can follow.

The counterterrorism centre was largely unknown until RCMP Commissioner Bob Paulson made a brief reference to it in Parliament earlier this year. The Globe and Mail has acquired the centre's terms of reference under Access to Information laws.

The centre brings federal agents of all stripes together in an RCMP facility in Ottawa where they can talk to each other and exchange information as part of the fight against terrorism. It formally came into existence in October, 2014, the same month two men inspired by the Islamic State killed two Canadian Forces soldiers.

The next spring, executives at the Communications Security Establishment, the Canadian Security Intelligence Service, the Canada Border Services Agency and Citizenship and Immigration Canada signed the centre's terms of reference, under which they agree to embed at least one staff member with the RCMP at all times.

The federal agencies constantly collect data, but under different mandates than that of the Mounties. Federal agents typically shield their files from each other unless they have a compelling reason to share. In some cases, warrants are needed for information handovers.

Yet federal agents want to knock down institutional walls in times of crisis, and the RCMP-led centre seeks to keep the bureaucratic barriers to information sharing low.

"The NSJOC's members are colocated at the RCMP's National Operations Centre in Ottawa to facilitate real-time and rapid information sharing ... [where] members have access to the databases and information holdings of their respective agencies," the terms of reference say.

The document says criminal charges are just one approach to fighting terrorism. Pooling knowledge among federal agents makes other interventions possible - such as revoking suspects' passports, adding people to no-fly lists, or even warning the family and friends of radicalized young people "of the risks associated with violent extremist activity."

Nothing in the terms of reference suggests the agencies got new powers to share information.

"NSJOC members are required to adhere to the respective operational policies and procedures of their agencies," the document says. However, the Conservative government's 2015 Bill C-51, which was created at the same time as the centre, allows federal departments to move information relevant to "activity that undermines the security of Canada" to federalsecurity agencies. The Privacy Commissioner of Canada has called this law highly invasive.

Federal watchdog agencies have complained for years that they cannot track what information agencies share in the name of national-security. Even as federalsecurity agencies increasingly swap files, none of their review bodies are legally empowered to see what is happening as it happens, or within more than one agency.

"A body like this makes the case for why we need more robust realtime oversight," says Carmen Cheung, a professor at the University of Toronto's Munk School of Global Affairs, who was shown a copy of the terms of reference. "It looks like they are all co- located in essentially one room, and that room has direct access to all the databases of all the respective agencies, which is amazing."

A decade ago, a judicial inquiry recommended Canada create a watchdog to track all security agencies at once, but the concept never got off the ground. The finding followed a Canadian counterterrorism investigation in which federal agents swapped information carelessly and several Canadians were wrongly jailed as presumed terrorists in Middle East prisons.

Today, federal- security agencies are under renewed pressure to amass and share records. Recent disclosures indicate CSIS, the domestic spy agency, has been "ingesting bulk data sets " in hopes of predicting patterns of terrorism, and its foreign-focused counterpart, CSE, is mapping out "contact chains" of global communications to discern where threats lie.

It's not clear how police would use such deductions. The records about the RCMP-led centre say that sharing information, early and often, can minimize the risk that federal police and spies trip over each other, and head off future problems.

Globe and Mail
Terrorism investigations tax RCMP's ability to fight Canada's organized crime
Saturday, 22 October 2016
Byline: Colin Freeze

Ottawa - The number of RCMP wiretaps on organized-crime groups is plummeting sharply as the force shifts its detectives to the fight against terrorism, according to statistics analyzed by The Globe and Mail.

In its federal policing role, the RCMP essentially has two major business lines - chasing mobsters and chasing terrorists. The priority the Mounties give to each of the two files has always been an issue, but the balance clearly shifted after the attack on Parliament Hill two years ago.

The RCMP has moved hundreds of officers from organized-crime probes to terrorism investigations in a bid to track suspected sympathizers of the Islamic State. This may come at a cost to other important RCMP missions, such as stopping human trafficking, getting guns off the street and curbing trade in illicit drugs such as fentanyl.

Related: Guilty pleas end risk of revealing RCMP surveillance technology (www.theglobeandmail.com)

Related: Surveillance device used in prison sets off police probe (www.theglobeandmail.com)

Related: RCMP fight to keep lid on high-tech investigation tool (www.theglobeandmail.com)

A spokeswoman for the police force does not dispute that a significant shift has taken place.

"The decrease in RCMP wiretap applications for serious and organized-crime investigations in the past year can partially be attributed to the shifting of a number of federal-policing resources to national-security criminal investigations," Corporal Annie Delisle said in an e-mailed response to Globe questions.

Her e-mail added that the RCMP "prioritizes its investigations based on threat and risk to public safety and remains committed to fighting organized crime."

Public Safety Canada, the bureaucracy that oversees the Mounties, is legally obliged to release an annual electronic-surveillance report.

In a typical year, the Mounties and their partner agencies usually seek approval for more than 100 wiretap applications from federal Crown attorneys, before bringing these bids to criminal-court judges for final approval.

The Public Safety Canada annual report for 2015, released this month, shows that 67 such applications were made.

This number does not necessarily mean police surveillance is declining. Police can pack scores of suspects and potential charges into a single wiretap application.

The Public Safety Canada report says the overall number of people being wiretapped by police is not changing much from year to year.

Yet the focus of police investigations is clearly shifting.

In 2011, police sought wiretaps in hopes of laying charges for 82 Criminal Code offences that explicitly had to do with organized-crime. Only six such charges were contemplated in 2015.

Half of all wiretap applications still involve drug cases, yet the number of drug charges being pursued has plummeted.

In 2011, federal police were seeking wiretap warrants involving only three terrorism charges. In 2014, police were hoping to lay 97 terrorism charges. In 2015, that number was 68.

The Public Safety Canada electronic surveillance report is preliminary and the 2015 numbers may increase because police do not have to disclose data about all their investigations right away. Not every wiretap warrant of leads to an arrest or criminal charge.

The pivot point was Oct. 22, 2014. That was the day Michael Zehaf-Bibeau stormed Parliament Hill's Centre Block with a rifle, after killing a Canadian Forces soldier. Two days before, a man ran over a Canadian Forces soldier in Quebec.

Both attackers were supporters of the Islamic State terrorism group and were shot dead by police. At the time, Parliament had just voted to send Canadian Forces warplanes overseas to bomb Islamic State fighters.

Two years later, the RCMP is still focused on terrorism.

"We continue to transfer people out of other areas into counter- terrorism investigations," RCMP Commissioner Bob Paulson told a Parliamentary committee earlier this month. "We've taken our investigative resources from areas of organized crime and financial integrity work," he added.

The RCMP says another reason for the declining number of wiretap applications is that suspects are now using encryption software to shield their digital communications from surveillance.

"Traditional criminality, like terrorism, like organized crime, like child exploitation, like fraud, is being advanced, supported and accelerated by the availability of these commercial encryption programs," Mr. Paulson says.

Public Safety Minister Ralph Goodale is canvassing Canadians on whether police need new powers.

Not so long ago, the RCMP was boasting of its surveillance prowess. In 2014, detectives held a press conference announcing they had curbed a Montreal gang war, arresting more than 30 mobsters after decoding more than a million secure messages.

Court records in the case revealed the RCMP used so-called "Stingray" machines that track suspects by indiscriminately catching smartphone signals in a given area. Police had also sought BlackBerry's help to store the suspects' secured communications so authorities could crack them later.

Such modern surveillance methods go largely unmentioned in Public Safety Canada's annual reports, which are a creature of 1970s-era laws that focus only on conventional police wiretapping powers.

Toronto Star
Liberals should keep promise on access law: Editorial
Sunday, 23 October 2016

Editorial: Access to information laws have become an essential feature of modern democracy. They allow citizens to watch over their governments and hold them to account. So it's deeply disturbing that Canada's access law, designed for a pre-digital world, and largely unchanged for three decades, is so profoundly broken.
Justin Trudeau's Liberals came to power promising to fix the problem, quickly setting up an all-party committee to review the law. The committee published its recommendations in June and the government vowed to reform the legislation later this year, or early in 2017. A long-overdue change seemed within view.

But last week Treasury Board President Scott Brison quietly backed off those timelines, indicating the government would implement initial changes later this year, but conduct a fuller review of the act starting in 2018. A concerned Information Commissioner Suzanne Legault told CBC News that she now doubts the legislation will be amended before the next election.

That's a shame. In recent years, loopholes in the law have too often been used to keep politically inconvenient information secret. Federal officials have invoked so-called cabinet confidentiality with alarming frequency. In 2013-14, it was used a record 3,100 times - a 49-per-cent uptick over the previous year. As the information commissioner has argued, the law meant to ensure openness has metastasized into an effective shield against disclosure.

Many recommendations have been made over the years on how to improve the act, but three simple, widely supported changes in particular would do a great deal to foster more openness.

First, the loophole should be shrunk. Cabinet confidentiality is meant to protect the frank and open exchange among cabinet ministers. But it should not be used to prevent Canadians from having the facts and background information that informed their government's decisions.

Second, when an access request has been rejected on grounds of cabinet secrecy, the information commissioner should have the power to investigate that refusal. Currently, the commissioner isn't allowed to see the documents involved.

Finally, Ottawa should invest the commissioner with the authority to issue "binding orders" that would force government disclosures required by the act. Under the current system, she can overturn a government decision only by taking Ottawa to court.

The first two are long-standing recommendations of transparency advocates and the information commissioner, endorsed by the all-party parliamentary committee. The third was a Liberal campaign promise. Canadians should not be made to wait until after the next election to see them realized.

The trouble is that while democracy loves openness, governments quite often do not. Canada no doubt needs a modern access law that ensures transparency and a watchdog capable of enforcing it. The Liberals understood this in opposition. In government, the temptation to carry on in the dark will be strong, but promises were made, and democratic principle, not political expediency, should light the way.

Ottawa Citizen
Older government systems showing age , revealing the price of email delay
Monday, 24 October 2016
Byline: James Bagnall

Ottawa - A sign of the times. A government official recently sent the following email:
"Treasury Board has been experiencing significant email issues since October 6, 2016," the note to other federal departments read. "We recommend that you contact employees by phone until further notice. We will update you when the issues are resolved."

Taken on its own, this was not a big deal. A few hundred Treasury Board employees went without email service off and on for a couple of weeks. The workers also lost email history and calendar appointments, which were being restored over the weekend using backups.

"Shared Services Canada has been working 24 hours a day to resolve the initial and any subsequent email issues," noted Stephanie Richardson, a spokesperson for Shared Services, the federal department responsible for computer services, including email and data centres.

But there was an unsettling message in this latest email glitch because it involved existing infrastructure. Most of the headlines involving government email over the past two years have focused on problems with the new system ordered from Bell Canada in 2013 but with delivery nowhere in sight. Now the reasonably reliable older systems are showing their age and may require additional investment.

Until the Bell system is up and running, most of the government's 600,000-plus email boxes must be hosted in aging data centres, most of them located in the National Capital Region. This means

government email service is increasingly vulnerable to breakdowns in data centres generally or the parts specific to the delivery of email.

It's not clear yet what triggered the Treasury Board email issues. "The root cause of the incident is still under investigation," Richardson explained in an email.

The email breakdown followed routine maintenance at one of the government's older data centres. When power was restored, email servers failed. Richardson confirmed that a "corrupted database" was involved.

Regardless, this is not good news for Shared Services, the five- year-old computer services agency.

Early in its mandate, Shared Services launched a $400-million project to consolidate 63 email systems across government into one. Bell Canada and CGI were to have completed the switch to canada.ca email addresses by March 31, 2015 but the contractors have been wrestling with a revised design, faulty hardware and other technical difficulties. While hardware issues, according to Shared Services, have been fixed, an overall solution has proved elusive.

Shared Services a year ago halted the migration of the new system to federal employees until Bell could resolve the difficulties. Not quite 70,000 government email boxes - less than 15 per cent of the total - currently use the new addresses.

In the meantime, of course the volume of data being sent on email is significantly higher each year, putting further strain on the legacy infrastructure.

The Conservative government estimated the new system designed by Bell would save taxpayers $50 million annually by taking advantage of economies of scale. Those savings have not been realized.

To date, most of the cost of the delay has been borne by Bell, which under its contract will not be paid until it delivers the goods. Bell declined comment for this article.

Richardson noted in her email: "There are outstanding contracted, functional issues that need to be resolved before new migrations can resume." Shared Services did not elaborate or provide a revised deadline.

While Bell is on the hook for fixing the new email system, Shared Services bears responsibility for keeping the older email systems running - and may soon have to invest significant sums.

Shared Services faces a similar issue with another of its responsibilities involving the consolidation of more than 500 data centres into a handful of modern ones. Because Shared Services was late to begin the streamlining process, it is diverting significant sums into keeping legacy data centres running even as it's investing in new data centres in Barrie and Borden.

The Liberals early this year said they would kick in an extra $384 million over two years to keep aging electronic infrastructure going. It's not known what percentage of this amount, if any, was earmarked specifically for email service - or if the Liberals anticipated continuing long delays in the new email system.

This much is clear: attempting simultaneously to modernize large computer networks and keep the old ones running appears to be a hugely difficult job in government.

Federal workers may have to get used to using the telephone in the months ahead.

National Post
Countering the Kremlin narrative
Monday, 24 October 2016
Byline: Matthew Fisher

Column: As the Kremlin gins up its cyberwarfare capabilities by using hackers to interfere with western elections, Canada is being asked to assist a European project to counter an older, but equally sinister information warfare campaign by President Vladimir Putin to influence ethnic Russians and others in what Russians call the Near Abroad.
Jerzy Pomianowski, who leads the European Endowment for Democracy (EED), was in Ottawa Thursday to discuss with Foreign Minister Stephane Dion whether Canada would consider funding a project designed to provide Balts, Moldovans, Belarussians and other eastern Europeans with access to Russian-language TV programming not produced in Moscow.

While Russia Today - the state-controlled English-language international all-news network - and other Russian media projects in Europe and the Middle East are used to spread highly biased ideas, this was "a secondary issue compared to the damage that has been done by the Kremlin narrative within the Russian language media space" in countries with significant ethnic Russian minorities and where local populations often speak Russian well, Pomianowski said after meeting Dion.

What the former Polish deputy foreign minister was referring to is immediately obvious to travellers to places such as Latvia and Lithuania.

Russians there readily tell visitors that the only news sources they pay attention to emanate from Russia. Reports are often extremely untruthful - and sometimes incendiary - especially surrounding events such as Moscow's annexation of Crimea, the shooting-down of a Malaysian Airliner over Ukraine by a Russian missile system or the alleged mistreatment of Russian minorities in the former Soviet republics.

There is a perverse echo in Armenian, Kyrgyz and Azeri-language media, too, because much of their content is lifted directly from reports originally provided in Russian and produced in Moscow. That is aside from the immense amount of time and money that Russian invests in Internet trolls operating mostly in English and German who criticize or ridicule people in social media who have criticized the Kremlin.

"We observe this. It is quite a common practice," Pomianowski said. "But it comes into a market that offers many other options so it is much less effective than it is in the Russian language media space."

As part of a propaganda strategy developed over 15 years, the Putin government first captures the hearts and minds of native Russian speakers with high quality entertainment and nostalgic films and songs that glorify the Soviet era, said Pomianowski, who became politically active during the heady days of Poland's Solidarity Movement more than 25 years ago.

"This content is designed to appeal to their emotions and feelings," he said. "It is used as a tool to keep them glued to the screen and then brainwashed through false debates and lies that are spread through the news programs."

The EED is affiliated with the EU and based in Belgium. Its intent is not to create counter-propaganda but to encourage open debate and alternative narratives and to assist independent Russian-speaking voices outside Russia.

Estonia has already created a state TV channel broadcasting in Russian to its Russian minority. A centre in Prague has been established where Russian- language journalism is being produced, including some investigative journalism. It is a hub where Russian-language media from outside Russia can also exchange news reports.

Seed money is being sought from abroad, including Canada, to allow independent producers to create high-quality dramas or infotainment for Russian minorities and others who speak Russian and live in the Near Abroad.

"The amount of funds being mobilized is not dramatically impressive," Pomianowski said. "What we are talking about is 10 million or 15 million euros a year" - roughly $15 million to $21 million.

Canada is already providing the EED with a $5-million grant to support the development of grassroots democratic values in Ukraine. As regards the EED's new initiative to create Russian-language programming, "there is a big hope that Canada will join these efforts" because of what Pomianowski called the country's "commitment to core democratic values" and because "sooner or later problems become global. Even Canada, on the far side of the ocean, is not that far away."

Since Putin took power in 2000 his government has developed a direct and indirect stranglehold over most media that recalls the power that the Politburo once had. He has achieved this by closing news

agencies and radio and television stations or by organizing new owners for media companies who immediately purge the staff.

"In the West, we pretend that we are discovering this strategy," Pomianowski said. "But everything was clear and well analyzed five or six years ago. We were just in a different mood. The U.S. was resetting relations with Russia so it was not in fashion to talk about such trends.

"That is the weakness in our part of the story. We see things when they hit our eyes with great strength rather than acting when they are visible but not yet at full speed."

National Post
How not to launch a cyber-attack
Monday, 24 October 2016
Byline: Eric Jardine

OpEd: The Obama administration seems to have a penchant for broadcasting its plans to the world before putting them into action. But telling your opponents what your next move will be is a bad idea. Whether in football, the board game Risk or the real world, a strategy should surprise them and keep them off balance. If your adversaries know you are coming, they can react faster, deploy pre-emptive countermeasures and ultimately blunt the impact of whatever it is you plan on doing.
Since the Democratic National Committee's email servers were hacked in the lead-up to the Democratic convention and allegations began swirling about Russian President Vladimir Putin's attempts to disrupt the American election through cyber- attacks on American soil, the Obama administration has been vocal about how it plans to deal with the situation.

We now know that the U.S. has proposed a proportional counterattack: Central Intelligence Agency Sources reportedly noted that the administration had asked the intelligence agency to prepare a "clandestine" cyberattack that aims to "embarrass" the Russians. Vice- President Joe Biden said on Meet the Press that the U.S. is intent on "sending a message" to Putin.

Of course, while the U.S. seems to have lost its strategic advantage here, its actual tactics may still be in the works behind closed doors, assuming it hasn't already initiated some kind of retaliation. But there's no question that it has blown the element of surprise.

Everything we have been hearing suggests that the Americans will try to embarrass Putin by responding with a hack of their own. Needless to say, the obvious next step for the Russians would be to go into information- control mode. If there are embarrassing emails on servers under Russian control, rest assured they have been expunged or stowed carefully away.

The popular idea that everything stays on the Internet forever is not quite true. For your average person, what you say, type or send online is pretty well permanent, but if you are a Russian oligarch, or

even Putin himself, keeping your most embarrassing content away from prying eyes is more than possible.

As the events surrounding Hillary Clinton's deleted emails makes clear, if you control the server, you control the content of that server (although the recipient of the email could still have a record, of course). The trouble is that Russia often does control the servers, as it has a data localization law on the books that requires data generated by Russian citizens be stored within Russia's borders.

Thus, the Americans would have to gather the data before the Russians have had a chance to delete it. But since the administration has already shown its hand, that scenario seems less likely. Of course, the U.S. could try to show how Putin and other oligarchs are exporting money and otherwise engaging in corrupt practices, as was recently suggested by retired Adm. James Stavridis. Since a lot of the proof would be stored outside of Russia, the option seems initially plausible, but comes with its own set of problems.

First, to embarrass members of the Russian government in this way would require that the U.S. hack - or, ideally, secure lawful access to - third-party servers, to gain access to the necessary data. Furthermore, for U.S. intelligence agencies to access Russia's computers, it is helpful if they are connected to the outside world. But, even back in October 2015, Russia was reportedly testing ways to sever the link between the Russian portion of the Internet and the rest of the network.

As Nikolay Nikiforov, the Russian communications minister, said, "Our task is to do what is needed so that the Russian Internet will carry on working independently of the opinion of colleagues, whatever sanctions policy decisions they decide to take." In other words, the U.S. might be able to disrupt Russia at the margins (and I have no doubt the U.S. has the skills and the technology to do so), but the Russians also have a last-ditch kill switch that could be used to keep the Russian networks running, and free from any foreign countermeasures. What's more, they can just blame the disruption on the U.S. and win points domestically.

In the end, the cat is out of the bag. Russia now knows that it is likely facing an imminent cyber-attack, and the U.S. cannot back down, waver or change course.

Eric Jardine is a fellow at the Centre for International Governance Innovation and assistant professor of political science at Virginia Polytechnic Institute and State University, in Blacksburg, Va. He recently co-authored the report, Look Who's Watching: Surveillance, Treachery and Trust Online.

The National (UAE)
Warning for UAE companies after huge cyber attack
Monday, 24 October 2016
Byline: Lucy Barnard

Abu Dhabi - Companies in the UAE are being warned that the sort of massive cyber attack which blocked some of the world's most popular websites over the weekend could be used to target regional businesses and governments.
On Friday, millions of web users in the United States and Europe were left unable to view popular websites including Twitter, PayPal, Amazon, Netflix and even The New York Times and Wall Street Journal, after hackers took over hundreds of thousands of common internet-enabled devices such as webcams and used them to bombard the sites with spam data.

FBI officials are still investigating the source of the attacks but days ahead of the US election, controversial website WikiLeaks claimed its supporters were responsible.

"[Julian] Assange is still alive and WikiLeaks is still publishing. We ask supporters to stop taking down the US internet. You proved your point," it tweeted early on Saturday morning.

The attacks differed from other recent cyber attacks because they centred around New Hampshire-based internet infrastructure company Dyn, which acts as a switchboard for online traffic - an area of the internet not typically targeted by cyber criminals.

According to Dyn, the company was hit by a series of at least three massive distributed denial-of-service (DDoS) attacks where millions of IP addresses flooded the targets with junk traffic, making it one of the largest ever cyber attacks.

Security experts said that the attack used a new powerful control software called Mirai to forcibly network together thousands of web-enabled CCTV cameras around the world and turn them into what is known as a "botnet".

Since the start of this month when the Mirai code was published on a hackers' forum, experts have warned that criminal organisations and pressure groups will find it easier to launch this sort of attack.

"These sorts of DDoS attacks are extremely worrying and on a company level there isn't a whole lot that you can do about them," said Mohammad Amin Hasbini, a senior security researcher at internet security firm Kaspersky Lab, which advises businesses on cyber defences.

"The big problem is that we don't know who is responsible for these attacks; we don't know if they are financially motivated, politically motivated or if they are just doing it for fun. WikiLeaks claims its supporters were responsible but who are they? This attack is perhaps 15 times bigger than any that we have experienced so far in the UAE, but DDoS attacks do happen every day in the UAE and, as technology improves, the problem is getting worse."

The disruptions come at a time of unprecedented fears about the cyber threat in the Middle East and around the world.

Between 2011 and 2013, 46 major financial institutions in the US were targeted through DDoS attacks, preventing hundreds of thousands of customers from accessing their accounts and costing the businesses millions of dollars to upgrade their systems. In March this year the FBI charged seven Iranian computer experts with carrying out the attack. And in 2013 two members of "hacktivist" group Anonymous were convicted of carrying out DDoS attacks against online payment websites including PayPal.

"The risks for this sort of attack are growing daily. There are now more devices than there are humans on the planet, and these days it is getting easier and easier for anyone with a grudge against a company or a government to buy a botnet army to launch attacks," said Eric Eifert, the senior vice president for managed security services at cybersecurity firm DarkMatter.

He warned that terror organisations such as ISIL had the capacity to use cyber technology to take over drones being used against them and convert them into improvised explosive devices.

"In the UAE especially we are seeing a lot of new devices being used as consumers look to control all sorts of things including lighting, cooling, even their fridges from their smartphones," Mr Eifert added. "Anything with an IP address can be infected by malware and these devices often have generic passwords which hackers can easily guess. It is important that manufacturers don't let this happen in future."

According to figures from Kaspersky Security, an average of 17.4 per cent of users in the Middle East encountered cyber threats originating from the internet in the third quarter of 2016.

The countries with the highest percentage of users affected by these threats were Qatar (24.4 per cent), the UAE (22.8 per cent), Kuwait (20.1 per cent), Saudi Arabia (17.9 per cent) and Egypt (17.1 per cent).

At the same time, an average of 47 per cent of users in the region encountered malware that spread in local networks, via USBs and storage disks.

Earlier this month the first US secretary of homeland security Tom Ridge, told a cyber security conference that as a global hub, the UAE is a prime target for cyber attacks.

"Any enterprise that is as successful, vibrant and connected like Dubai [is a target]," Mr Ridge said. "It's a centre for financial transactions and trade historically. That's what makes the government's decision to make it a smart city timely and relevant and increases the pressure on [it] to do it right because it becomes an iconic player in the region and the world. The higher the profile, the more sophisticated the attacks."

Wired (US)
Inside the Cyberattack That Shocked the U.S. Government

Monday, 24 October 2016
Byline: Brendan I. Koerner

New York - The US OFFICE of Personnel Management doesn't radiate much glamour. As the human resources department for the federal government, the agency oversees the legal minutiae of how federal employees are hired and promoted and manages benefits and pensions for millions of current and retired civil servants. The core of its own workforce, numbering well over 5,000, is headquartered in a hulking Washington, DC, building, the interior of which has all the charm of an East German hospital circa 1963. It's the sort of place where paper forms still get filled out in triplicate.
The routine nature of OPM's business made the revelations of April 15, 2015, as perplexing as they were disturbing. On that morning, a security engineer named Brendan Saulsbury set out to decrypt a portion of the Secure Sockets Layer (SSL) traffic that flows across the agency's digital network. Hackers have become adept at using SSL encryption to cloak their exploits, much as online vendors use it to shield credit card numbers in transit. Since the previous December, OPM's cybersecurity staff had been peeling back SSL's camouflage to get a clearer view of the data sloshing in and out of the agency's systems.

Soon after his shift started, Saulsbury noticed that his decryption efforts had exposed an odd bit of outbound traffic: a beacon-like signal pinging to a site called -opm-security.org. But the agency owned no such domain. The OPM-related name suggested it had been created to deceive. When Saulsbury and his colleagues used a security program called Cylance V to dig a little deeper, they located the signal's source: a file called mcutil.dll, a standard component of software sold by security giant McAfee. But that didn't make sense; OPM doesn't use McAfee products. Saulsbury and the other engineers soon realized that mcutil.dll was hiding a piece of malware designed to give a hacker access to the agency's servers.

The Office of Personnel Management repels 10 million attempted digital intrusions per month--mostly the kinds of port scans and phishing attacks that plague every large-scale Internet presence--so it wasn't too abnormal to discover that something had gotten lucky and slipped through the agency's defenses. In March 2014, for example, OPM had detected a breach in which blueprints for its network's architecture were siphoned away. But in this case, the engineers noticed two unusually frightening details. First, opmsecurity.org had been registered on April 25, 2014, which meant the malware had probably been on OPM's network for almost a year. Even worse, the domain's owner was listed as "Steve Rogers"--the scrawny patriot who, according to Marvel Comics lore, used a vial of Super-Soldier Serum to transform himself into Captain America, a member of the Avengers.

Registering sites in Avengers-themed names is a trademark of a shadowy hacker group believed to have orchestrated some of the most devastating attacks in recent memory. Among them was the infiltration of health insurer Anthem, which resulted in the theft of personal data belonging to nearly 80 million Americans. And though diplomatic sensitivities make US officials reluctant to point fingers, a wealth of evidence ranging from IP addresses to telltale email accounts indicates that these hackers are tied to China, whose military allegedly has a 100,000-strong cyber-espionage division. (In 2014 a federal grand jury in Pennsylvania indicted five people from one of that division's crews, known as Unit 61398, for

stealing trade secrets from companies such as Westinghouse and US Steel; all the defendants remain at large.)

Once Captain America's name popped up, there could be little doubt that the Office of Personnel Management had been hit by an advanced persistent threat (APT)--security-speak for a well-financed, often state- sponsored team of hackers. APTs like China's Unit 61398 have no interest in run-of-the-mill criminal activities such as selling pilfered Social Security numbers on the black market; they exist solely to accumulate sensitive data that will advance their bosses' political, economic, and military objectives. "Everyone can always say, 'Oh, yeah, the Pentagon is always going to be a target, the NSA is always going to be a target,'" says Michael Daniel, the cybersecurity coordinator at the White House, who was apprised of the crisis early on. "But now you had the Office of Personnel Management as a target?"

To figure out why the hackers had trained their sights on OPM, investigators would have to determine what, if anything, had been stolen from the agency's network over the preceding year. But first they had to hunt down and eliminate the malware on its network, an archaic monstrosity that consisted of as many as 15,000 individual machines.

Curtis Mejeur was a victim of dreadful timing. A wry and diminutive former marine who had served in Fallujah, where he mapped insurgent strongholds as part of an intelligence unit dubbed the Hobbits, Mejeur started work as one of OPM's senior IT strategists on April 1, 2015. He was still getting acclimated to his new job when, on the morning of April 16, he was handed the most daunting assignment of his career: Lead the effort to snuff out the attack on the agency's network.

Based on the little he'd already heard about the malware's power and lineage, Mejeur was certain his investigation would uncover plenty of nasty surprises. But he wouldn't have to deal with them alone; early that morning, a team of engineers from the US Computer Emergency Readiness Team, the Department of Homeland Security unit that handles digital calamities, marched into OPM's headquarters. The engineers set up a command post in a windowless storage room in the sub-basement, just down the hall from where Saulsbury had discovered the hack less than 24 hours earlier.

Since they couldn't trust OPM's compromised network, the visitors improvised their own by lugging in workstations and servers that they could seal behind a customized firewall. Soon enough, the subbasement was filled with the incessant clatter of keyboards, occasionally punctuated by the hiss of a Red Bull being popped open. The dozen-plus engineers rarely uttered more than a few words to one another, which is how they prefer to operate.

One of the US-CERT team's first moves was to analyze the malware that Saulsbury had found attached to mcutil.dll. The program turned out to be one they knew well: a variant of PlugX, a remote-access tool commonly deployed by Chinese--speaking hacking units. The tool has also shown up on computers used by foes of China's government, including activists in Hong Kong and Tibet. The malware's code is always slightly tweaked between attacks so firewalls can't recognize it.

The hunt to find each occurrence of PlugX continued around the clock and dragged into the weekend. A sleeping cot was squeezed into the command post, where temperatures became stifling when the building's air conditioners shut off as usual on Saturdays and Sundays.

The hunt turned up not just malware but also the first inklings of the breach's severity. A technician from the security software company Cylance, who was supporting the effort, spotted encrypted .rar files that the attackers had neglected to delete. He knew that .rar files are used to store compressed data and are often employed by hackers to shrink files for efficient exfiltration. In an email to Cylance CEO Stuart McClure on Sunday, April 19, the technician was blunt in his assessment of OPM's situation: "They are fucked btw," he wrote.

By Tuesday the 21st, having churned through a string of nearly sleepless days and nights, the investigators felt satisfied that they'd done their due diligence. Their scans had identified over 2,000 individual pieces of malware that were unrelated to the attack in question (everything from routine adware to dormant viruses). The PlugX variant they were seeking to annihilate was present on fewer than 10 OPM machines; unfortunately, some of those machines were pivotal to the entire network. "The big one was what we call the jumpbox," Mejeur says. "That's the administrative server that's used to log in to all the other servers. And it's got malware on it. That is an 'Oh feces' moment."

By controlling the jumpbox, the attackers had gained access to every nook and cranny of OPM's digital terrain. The investigators wondered whether the APT had pulled off that impressive feat with the aid of the system blueprints stolen in the breach discovered in March 2014. If that were the case, then the hackers had devoted months to laying the groundwork for this attack.

At first, the investigators left each piece of malware in place, electing only to throttle its ability to send outbound traffic; if the attackers tried to download any data, they would find themselves confined to dial-up speeds. But on April 21, Mejeur and the US-CERT team began to discuss whether it was time to boot the attackers, who would thus learn that they'd been caught. "If I miss one remote-access tool, they'll come back in through that variant, they'll reestablish access, and then they'll go dormant for six months to a year at least," says a US-CERT incident responder who participated in the OPM investigation and who agreed to speak on the condition he remain anonymous. "And then a year later, they've now put malware in a lot of different places, and you don't know what's happening because you think you already mitigated the threat."

The debate continued until the evening of Friday, April 24, when an opportunity presented itself: As part of a grid modernization program in Washington, OPM's building was scheduled to have its power cut for several hours. The team decided that, even though it would mostly be just a psychological triumph, they would dump the malware just minutes before the blackout. If the attackers were monitoring the network, they wouldn't realize their access had been cut until everything finished booting up at least 12 hours later.

By the time power was restored on the 25th, the hackers no longer had the means to roam OPM's network--or at least that's what everyone hoped. The investigators could finally turn toward piecing together what the attackers had hauled away.

There is a common misperception that the surest way to frustrate hackers is to encrypt data. But advanced persistent threats are skilled at routing around such measures. The first item groups like these usually swipe is the master list of credentials--the usernames and passwords of everyone authorized to access the network. The group's foot soldiers will then spend weeks or months testing those credentials in search of one that offers maximum system privileges; the ideal is one that belongs to a domain administrator who can decrypt data at will. To minimize their odds of tripping any alarms, the attackers will try each credential only once; then they'll wait hours to try the next. Since these hackers are likely salaried employees, investing that much time in an attack is just part of the job.

There is a straightforward way to foil this approach: multifactor authentication, which requires anyone logging in to a network to be in physical possession of a chip-enhanced ID card that correlates with their username and password. OPM has such an authentication scheme, but it wasn't fully implemented until January 2015-- too late to prevent the PlugX attack. The beacon that connected to opm-security.org helped the attackers keep their foothold in the network.

When hackers utilize genuine credentials, life becomes difficult for those who specialize in post--attack forensics. Investigators must determine when authorized credential holders weren't using their accounts at times when the records state otherwise. And the only way to accomplish that is through face-to-face interviews: For nearly a month, Mejeur and the US- CERT engineers grilled hundreds of OPM employees in groups of six. Since human memories are so faulty, the investigators counted themselves fortunate when an employee was able to recall that they had been on vacation while their credential was in use for a particular week; the team could then analyze that account's activity during that span, confident that a hacker was responsible for it all.

As the investigators laboriously sifted through interview transcripts and network logs, they created a rough timeline of the attack. The earliest incursion they could identify had been made with an OPM credential issued to a contractor from KeyPoint Government Solutions. There was no way to know how the hackers had obtained that credential, but the investigators knew that KeyPoint had announced a breach of its own in December 2014. There was a good chance that the hackers had first targeted KeyPoint in order to harvest the single credential necessary to compromise OPM.

Once established on the agency's network, they used trial and error to find the credentials necessary to seed the jumpbox with their PlugX variant. Then, during the long Fourth of July weekend in 2014, when staffing was sure to be light, the hackers began to run a series of commands meant to prepare data for exfiltration. Bundles of records were copied, moved onto drives from which they could be snatched, and chopped up into .zip or .rar files to avoid causing suspicious traffic spikes. The records that the attackers targeted were some of the most sensitive imaginable.

The hackers had first pillaged a massive trove of background-check data. As part of its human resources mission, OPM processes over 2 million background investigations per year, involving everyone from contractors to federal judges. OPM's digital archives contain roughly 18 million copies of Standard Form 86, a 127-page questionnaire for federal security clearance that includes probing questions about an applicant's personal finances, past substance abuse, and psychiatric care. The agency also warehouses the data that is gathered on applicants for some of the government's most secretive jobs. That data can include everything from lie detector results to notes about whether an applicant engages in risky sexual behavior.

The hackers next delved into the complete personnel files of 4.2 million employees, past and present. Then, just weeks before OPM booted them out, they grabbed approximately 5.6 million digital images of government employee fingerprints.

When OPM went public with news of the hack in early June, speculating about the attackers' plans for the data became a popular Beltway pastime: Some of the theories involved a Chinese plot to recruit agents and, more outlandishly, a scheme to graft finger-prints onto Chinese spies so they could foil biometric sensors. But concrete evidence of the hackers' long-term intentions remains virtually nonexistent, which may be the scariest part of all.

"We haven't seen a single indication of this data being used anywhere," says Arun Vishwanath, a cybersecurity researcher at the State University of New York at Buffalo. "Yeah, we know the data is gone, but where did it go? What's the purpose of all of this? No one has the answer to any of that."

The Congressional hearings that take place in the wake of national calamities often have a vicious edge, and the one looking into the OPM hack was no exception. The agency's director, Katherine Archuleta, turned in a clumsy performance before the House Oversight Committee: She failed to offer a clear idea of how many people had been affected by the attack, and she seemed to duck personal responsibility by repeatedly mentioning how difficult it is to secure OPM's aging "legacy systems." The committee's members reacted with predictable scorn.

"I wish that you were as strenuous and hardworking at keeping information out of the hands of hackers as you are keeping information out of the hands of Congress and federal employees," chided representative Stephen Lynch (D-Massachusetts).

Damning details about OPM's porous security emerged at the hearing. The agency's own assistant inspector general for audits testified about what he characterized as a "long history of systemic failures to properly manage its IT infrastructure."

The tone of the hearings struck some observers as overly brutal. The OPM brain trust received no credit for implementing the SSL decryption program that had led to the attack's discovery, nor for acting fast to quell the threat. "They could easily have just buried all this stuff and no one would ever have known,"

says Stuart McClure, the Cylance CEO. "But they were highly pro-active--they just wanted to do what was right."

But political dramas of this sort seldom end in acts of mercy: Archuleta resigned under pressure, and her CIO, Donna Seymour, opted for retirement days before she was to endure another round of grilling by the House committee. The two executives' departures struck fear into their peers across the federal bureaucracy. "It was easy for people to see themselves in OPM and ask the question 'What do we have that people might care about that we hadn't thought about before?'" says Michael Daniel, the White House cyber-security coordinator who previously spent over a decade overseeing the intelligence community's budget while at the Office of Management and Budget.

These newly frightened agency heads made for a receptive audience during the Cybersecurity Sprint, a White House initiative that aimed to improve security throughout the government in a mere 30 days. Held in June 2015, the Sprint was the idea of Tony Scott, who had become the third-ever US federal CIO just five months earlier. "Don't waste a good crisis," says Scott, a bearlike and avuncular veteran of Microsoft and Disney. He pressed agencies to spend the Sprint focusing on what he terms "basic hygiene"--that is, making simple upgrades that can drastically reduce an organization's susceptibility to attack. These include measures such as keeping current with the latest software patches, reducing the number of network users with administrative privileges, and, above all, broadening the adoption of multifactor authentication. According to Scott, the federal government's use of smartcards for multifactor authentication increased by more than 70 percent during the Sprint.

As the Sprint neared its end in July, Scott and Daniel began to work on a longer-term response to the OPM fiasco--a set of policy goals that they hoped would revolutionize the federal government's approach to cybersecurity. The document they eventually produced, with substantial input from the likes of the Pentagon and the National Institute of Standards and Technology, became known as the Cybersecurity National Action Plan. First publicly announced by President Obama in February 2016, it calls for billions to be set aside for several critical projects, such as upgrading outmoded systems.

CNAP also stresses the need for better cooperation between the private and public sectors--something that might have made the OPM hack far less severe. In February 2015, in its published analysis of the Anthem hack, the security firm Threat-Connect wrote about its discovery of a suspicious domain registered to "Tony Stark"--the alter ego of Iron Man. That domain was named opm-learning.org. Had anyone at OPM been made aware of ThreatConnect's finding that month, the agency's security staff might have started to look for malware right away. But the tip never reached the sub-basement at OPM headquarters.

But the plan pays too little attention to a fundamental flaw in our approach to security: We're overly focused on prevention at the expense of mitigation. One reason these attackers can do so much damage is that the average time between a malware infection and discovery of the attack is more than 200 days, a gap that has barely narrowed in recent years.

"We can't operate with the mindset that everything has to be about keeping them out," says Rich Barger, ThreatConnect's chief intelligence officer. "We have to operate knowing that they're going to get inside sometimes. The question is, how do we limit their effectiveness and conduct secure business operations knowing they're watching?" Accomplishing that means building networks that are designed to limit a hacker's ability to maneuver and creating better ways to detect anomalous behavior by allegedly authorized users.

A cybersecurity overhaul of this magnitude will, of course, require an abundance of talent. And that means much depends on how well government recruiters can convince the best engineers that being locked in a high-stakes competition with supervillain- -esque adversaries is more exciting than working in Silicon Valley. Perhaps it will be an easy sell. After all, improving a commercial antivirus program, no matter how highly paid a gig, simply doesn't have the romantic appeal of battling Unit 61398 for world supremacy.

Agence France-Presse
Moscow confirms ministry website attack after US hacker claim
Monday, 24 October 2016
Byline: Staff report

Moscow - Russia's foreign ministry on Sunday said an old version of its website had been attacked after a US hacker claimed he broke in and posted a mocking message.
Foreign ministry spokeswoman Maria Zakharova wrote on Facebook that the hacker targeted "an old site that has not been used for a long time," adding that "specialists are working out what happened."

The attack came after Washington earlier this week formally accused the Russian government of trying to "interfere" in the 2016 White House race by hacking, charges the Kremlin has repeatedly dismissed.

"If they establish there was hacking by Americans, even of a resource that wasn't working, this is far from pleasant," Zakharova wrote.

She said that this could be an indication that a "cyber machine of destruction has started acting" after US Vice President Joe Biden told NBC television that President Vladimir Putin would get a "message" from Washington in response to the hacking blamed on Russia.

Alternatively, the latest hack simply shows that the "US elections have wound up people to such a state that they start smashing everything," Zakharova wrote.

The foreign ministry's main website was apparently working normally on Sunday afternoon.

On Saturday, a hacker who calls himself the Jester tweeted: "I'm Jester & I approve this message via the Russian Foreign Affairs Website."

The hacker, who has previously attacked WikiLeaks website, posted a link to a page which had content replaced with a message and an image of a jester.

"Comrades! We interrupt regular scheduled Russian Foreign Affairs Website programming to bring you the following important message," he wrote.

- 'This is America' -

"Knock it off. You may be able to push around nations around you, but this is America. Nobody is impressed," he added.

CNN reported that the jester's attack overnight Moscow time included the piercing sound used for civil alert messages about extreme weather.

The hacker said he was writing on the ministry site to complain after waves of distributed denial of service (DDoS) attacks pounded Twitter, Netflix and other major websites on Friday, accusing Russia of being behind this.

"Now, you can do the usual, shrug, smirk and say 'there's no evidence' that points to Russia being behind any of this stuff, and you can get the Russian Ambassador to US to post some mildly amusing quips over Twitter."

"But let's get real, I know it's you, even if by-proxy, and you know it's you," the hacker wrote.

On Sunday, after the Zakharova's Facebook message, Jester tweeted, "#OutPropagandered - Getting Russia to admit they got 'dinged'. Priceless. They've already started tweaking the story," with a link to a somewhat dismissive article on the pro-Putin Russia Today website.

The mass DDoS attack on Friday could have been meant as a message from a foreign power, cyber security analysts told AFP at the time.

The onslaught commanded the attention of top US security agencies, including the Department of Homeland Security.

"DHS and the FBI are aware and are investigating all potential causes" of the outages, a spokeswoman said.

New York Times
A New Era of Internet Attacks Powered by Everyday Devices
Sunday, 23 October 2016

Byline: David E. Sanger & Nicole Perlroth

Washington - When surveillance cameras first began popping up in the 1970s and '80s, they were welcomed as a crime-fighting tool, then as a way to monitor traffic congestion, factory floors and even baby cribs. Later, they were adopted for darker purposes, as authoritarian governments like China's used them to prevent challenges to power by keeping tabs on protesters and dissidents.
But now those cameras -- and many other devices that today are connected to the internet -- have been commandeered for an entirely different purpose: as a weapon of mass disruption. The internet slowdown that swept the East Coast on Friday, in a nation already jittery about the possibility that hackers could interfere with election systems, offered a glimpse of a whole new era of vulnerabilities confronting a highly connected society.

The attack on the infrastructure of the internet, which made it all but impossible at times to check Twitter feeds or headlines, was a remarkable reminder about how billions of ordinary web-connected devices - - many of them highly insecure -- can be turned to vicious unintended purposes. And the threats will continue long after Election Day for a nation that increasingly keeps its data in the cloud and its head in the sand.

Remnants of the attack continued to slow some sites on Saturday, though the biggest troubles had abated. Still, to the tech community, Friday's events were as inevitable as an earthquake along the San Andreas fault. A new kind of malicious software exploits a long-known vulnerability in those cameras and other cheap devices that are now joining up to the "internet of things."

The advantage of putting every device on the internet is obvious. It means your refrigerator can order you milk when you are running low, and the printer on your home network can tell a retailer that you need more ink. Security cameras can alert your cellphone when someone is walking up the driveway, whether it is a delivery worker or a burglar. When Google and the Detroit automakers get their driverless cars on the road, the internet of things will become your chauffeur.

But hundreds of thousands, and maybe millions, of those security cameras and other devices have been infected with a fairly simple program that guessed at their factory-set passwords -- often "admin" or "12345" or even, yes, "password" -- and, once inside, turned them into an army of simple robots. Each one was commanded, at a coordinated time, to bombard a small company in Manchester, N.H., called Dyn DNS with messages that overloaded its circuits.

Few have heard of Dyn, but it essentially acts as one of the internet's giant switchboards. Bring it to a halt, and the problems spread instantly. It did not take long to reduce Twitter, Reddit and Airbnb -- as well as the news feeds of The New York Times -- to a crawl.

The culprit is unclear, and it may take days or weeks to find out. In the end, though, the answer probably does not mean much anyway.

The vulnerability the country woke up to on Friday morning can be easily exploited by a nation-state such as Russia, which the administration has blamed for hacking into the Democratic National Committee and the accounts of Hillary Clinton's campaign officials. It could also be exploited by a criminal group, which was the focus of much of the guesswork about Friday's attack, or even by teenagers. The opportunities for copycats are endless.

The starkest warning came in mid-September from Bruce Schneier, an internet security expert, who posted a brief essay titled "Someone Is Learning How to Take Down the Internet." The technique was hardly news: Entities like the North Korean government and extortionists have long used "distributed denial-of-service" attacks to direct a flood of data at sites they do not like.

"If the attacker has a bigger fire hose of data than the defender has," he wrote, "the attacker wins."

But in recent times, hackers have been exploring the vulnerabilities of the companies that make up the backbone of the internet -- just as states recently saw examinations of the systems that hold their voter registration rolls. Attacks on the companies escalated, Mr. Schneier wrote, "as if the attack were looking for the exact point of failure." Think of the mighty Maginot Line, tested again and again by the German Army in 1940, until it found the weak point and rolled into Paris.

The difference with the internet is that it is not clear in the United States who is supposed to be protecting it. The network does not belong to the government -- or really to anyone. Instead, every organization is responsible for defending its own little piece. Banks, retailers and social media hubs are supposed to invest in protecting their websites, but that does not help much if the connections between them are severed.

The Department of Homeland Security is supposed to provide the baseline of internet defense for the United States, but it is constantly playing catch-up. In recent weeks, it deployed teams to the states to help them find and patch vulnerabilities in their voter registration systems and their networks for reporting results.

The F.B.I. investigates breaches, but that takes time -- and, in the meantime, people want to bank online and stream television shows. On Nov. 8, Americans will have to look up where they are supposed to vote, and, in a few cases, they will cast their vote on the internet. Yet the voting system is not considered part of the nation's "critical infrastructure."

The head of the National Security Agency, Adm. Michael Rogers, said recently that experts were looking at the problem the wrong way. "We are over-focused on places and things," he said in a talk at Harvard. "We need to focus on the data," and how it flows -- or doesn't flow.

That is where the "internet of things" comes in. Most of the devices have been hooked up to the web over the last few years with little concern for security. Cheap parts, some coming from Chinese suppliers, have weak or no password protections, and it is not obvious how to change those passwords.

And the problem is quickly expanding: Cisco estimates that the number of such devices could reach 50 billion by 2020, from 15 billion today. Intel puts the number at about 200 billion devices in the same time frame. (Assuming the global population is around 7.7 billion people in 2020, that would be about six to 26 devices per person.)

Security researchers have been warning of this problem for years, but that caution has largely been written off as hype or fear-mongering. Then Brian Krebs, who runs a popular site on internet security, was struck by a significant attack a few weeks ago. The company protecting him, Akamai, gave up. The malware behind the attack, called Mirai, had a built-in dictionary of common passwords and used them to hijack devices to become attackers.

Chester Wisniewski, a principal computer research scientist at Sophos, a security company, said that attacks like the one on Dyn "might be the beginning of a new era of internet attacks conducted via 'smart' things."

"There are tens of millions more insecure 'smart' things that could cause incredible disruptions, if harnessed," Mr. Wisniewski added in an email.

It is possible, investigators say, that the attack on Dyn was conducted by a criminal group that wanted to extort the company. Or it could have been done by "hacktivists." Or a foreign power that wanted to remind the United States of its vulnerability. The answer may not come by Election Day, but the next wave of attacks very well could.

David E. Sanger reported from Washington, and Nicole Perlroth from San Francisco.

New York Times
Russian Suspected of Hacking U.S. Tech Companies Is Indicted
Sunday, 23 October 2016
Byline: Nicole Perlroth

San Francisco - A Russian man accused of breaking into computer systems at three internet companies in 2012 has been indicted by a federal grand jury in Oakland, Calif.
Yevgeniy Aleksandrovich Nikulin, 29, was arrested this month while vacationing with his girlfriend in the Czech Republic on charges that he hacked into computer networks at LinkedIn, Dropbox and Formspring, damaged computers and conspired to traffic in stolen information.

The arrest of Mr. Nikulin provided a look at the shadowy world of Russian hackers, who appear to operate with relative impunity even as they are accused of escalating attacks on computer networks in the United States. They are accused of attacking a long list of targets, including retailers, banks, energy companies, and more recently, the Democratic National Committee.

Hackers have been able to operate in Russia with little concern about getting arrested, security experts and law enforcement executives say, so long as they do not attack targets inside Russian borders. But they risk arrest when they leave the country.

In 2014, for example, a hacker was arrested in Guam and extradited to the United States for accessing cash register systems at American retailers between 2009 and 2011. A federal jury convicted that hacker, Roman Valerevich Seleznev, of 38 counts of hacking-related charges in August. He is awaiting sentencing.

The grand jury indictment, which was unsealed on Friday, accuses Mr. Nikulin of hacking into the computer networks of the three companies, damaging the computers of LinkedIn and Formspring employees, and using their credentials for further intrusions.

He is also accused of conspiring with unnamed co- conspirators to traffic in user credentials stolen from Formspring, a social networking site. He faces three counts of computer intrusion, two counts of causing damage to a protected computer, two counts of aggravated identity theft, one count of trafficking, and one count of conspiracy.

Mr. Nikulin could face more than 30 years of prison and more than $1 million in fines.

The charges were announced on Friday by Brian J. Stretch, a lawyer at the Justice Department, and John F. Bennett, a special agent in charge with the Federal Bureau of Investigation.

Mr. Nikulin, who goes by the online aliases Chinabig01, Dex.007, Valeriy.krutov3 and itBlackHat, was captured in a raid at a hotel in central Prague on Oct. 5. The arrest came 12 hours after authorities there learned he was in the country with his girlfriend and driving a luxury car, according to local police.

He did not resist arrest, but had medical problems and was briefly hospitalized, the police said in a statement. The raid was conducted in collaboration with the F.B.I. after Interpol issued an arrest warrant for him.

Mr. Nikulin's arrest came two days before the Obama administration formally accused the Russian government of stealing and disclosing emails from the Democratic National Committee and other institutions and prominent individuals.

Federal officials, including Vice President Joseph R. Biden Jr., have said that the United States would respond to the Russian attacks in kind.

After the Czech police arrested Mr. Nikulin, the Russian Embassy in Prague called for his release.

Aleksei Kolmakov, spokesman for the embassy in Prague, was quoted by the state-run Russian news agency Tass as saying, "We insist that the detained Russian citizen should be transferred to Russia."

A judge in Prague ordered Mr. Nikulin to remain in custody and a court to examine whether to extradite him to the United States.

Waterloo Region Record
Waterloo startup focuses on security for the quantum age
Saturday, 22 October 2016
Byline: Terry Pender

Waterloo - A small startup in Waterloo is working on a problem that touches everyone using the Internet for buying, selling and banking -- securing sensitive data against attacks from quantum computers.
Isara Corp. , based in the Quantum Valley Investments building, went public about a month ago with the first in a suite of planned software products that it says will protect data in existing computers from hackers using quantum computers. The startup's sole focus is quantum-safe cryptography.

It is not only e-commerce that is threatened by the next generation of computers, but also sensitive government communications, says Scott Totzke, Isara's chief executive officer.

There is now a consensus among some of the biggest players in technology, including Google, Amazon and Microsoft, that quantum computers will be a commercial reality by 2026. Using the properties of subatomic particles to process and store information, they will be able to quickly break current methods of encryption.

Everything from credit card numbers, bank accounts, personal records, health files, tax records, corporate data and top-secret messages exchanged by spy agencies are all vulnerable to hackers using quantum computers, Totzke says.

That means any data that is currently stored -- and must remain secret beyond 2026 -- is already vulnerable, and steps should be taken now to protect it from quantum hackers.

"We have an existing threat even though this technology looks like it is a decade out," he says.

In a process called "harvest and decrypt," foreign governments collect encrypted information now and stash it in data centres, waiting for the day when quantum computers can break it all open, Totzke says.

Multinational banks and insurance companies with global infrastructure will need four to five years to plan for and deploy quantum- resistant software that protects their data, he says.

"Which means as an industry we've only got five years to get a solution in place, get technology that is tested and accepted and start upgrading all of our critical infrastructure so it will be quantum safe," Totzke says.

Cars and other products that are connected to the Internet and receive software updates over wireless connections and other devices that are part of the Internet of Things must also be safe from quantum hackers, he says.

"If we aren't considering how to mitigate the threat of a quantum computer-enabled adversary, we may not be able to trust software updates that we get to the cars," he says. "We could get rogue software updates that interfere with critical navigation systems or critical operational systems like steering and brakes and acceleration."

The issue goes beyond financial services and government secrets, Totzke says.

"It really becomes everything that is connected where you have to authenticate a user or a system or we have to protect a secret."

Something known as public key cryptography protects private information on the Internet. Most of the Internet connections people trust today are secured by something called RSA -- an algorithm whose name is an acronym for the three founders of the widely used encryption method.

Isara says the remaining 20 per cent of Internet connections are protected by something called elliptic curve cryptography, which was developed by Certicom, a University of Waterloo spinoff that was acquired by BlackBerry in 2009. The technology is the basis for BlackBerry's vaunted security software that has never been hacked.

Totzke was formerly a senior vice-president at BlackBerry, responsible for the security of the company's products. His group helped to make security the biggest competitive advantage for BlackBerry. After 13 years at BlackBerry, he left in June 2014, looking for a change. He linked up with Mike Brown, another veteran of the BlackBerry security team, and founded Isara.

Brown has a master's degree in math from the University of Waterloo and spent a lot of time at the university's Centre for Applied Cryptographic Research. Most of the research going on at Isara is pure, advanced mathematics.

"When you connect with your phone to Amazon or TD or something like that, fundamentally there is mathematics," Brown says.

"Up to today we have trusted and relied upon that math because nothing can break it. Well, a quantum computer does," he says. "So the problem now is: 'What's the new math that we replace it with?' That's what Isara is focused on, studying that, implementing that and providing those products to customers."

In 18 months, the startup went from Totzke and Brown working together to 21 employees. It has produced the first in a small library of quantum-safe algorithms that will enable cryptography upgrades for traditional computers, sensors, Internet servers, routers and networks.

Isara is earning revenue, fully funded and hiring. Its lead investor is Quantum Valley Investments.

Even with 21 employees, Isara is the largest group of people focused on the problem of quantum safe cryptography, says Mike Pecen, the company's chief technology officer.

Implementing quantum-safe cryptography is presenting interesting challenges to the Isara team that includes four PhDs.

The challenges include: How do you make quantum-safe cryptography scale? How do you get a quantum safe algorithm to work on a sensor for the Internet of Things that has limited memory, limited computing power and limited battery power?

"Or how do you make it work, say in Amazon's web service cloud? These are very different problems that take different approaches," Totzke says. "And fortunately we have this great team here that is able to address those concerns in our design and implementation."

Pecen, formerly a senior-vice president and head of the advanced technology division at BlackBerry, sits on the board of the Institute for Quantum Computing at UW and he reports to the board of the European Telecommunications Standards Institute -- the most influential organization in the world for setting technical benchmarks for smartphones and other wireless telecommunications devices.

Last year, he founded the institute's working group for quantum safe cryptography. He serves as the group's chair. Companies and governments that want to take part pay an annual fee. That money pays for the engineers and research that informs the standards.

"It is in the formative stages," Pecen says of the group's work. "That being said, the European Commission is in my group, the French government is in my group, the government of the United Kingdom is in my group."

Quantum computers use the properties of subatomic particles -- atoms, ions, photons and electrons -- for processing information. Instead of the bits and bytes of traditional computers, they use qubits.

Pecen says quantum computers already exist, mostly in university-based research labs, but the machines are small, ranging in size from one qubit to 12 qubits. The Institute for Quantum Computing at UW has what is believed to be the largest quantum computer, with 12 qubits, he says.

"Little, baby quantum computers can solve some amazingly difficult problems faster than a super computer today," Pecen says.

He says no one knows how many qubits are needed before a quantum computer easily cracks the current methods of encryption. But the threat is real, because someone may have a breakthrough. Or someone may figure out a way to co-ordinate the power of several, small quantum computers with a conventional computer, he says.

With the threat increasing, some government agencies have started talking about quantum safe cryptography. Last year, the National Security Agency (NSA) in the United States said it would transition its computers to quantum-resistant algorithms "in the not too distant future."

The NSA's Canadian counterpart is the Ottawa-based Communications Security Establishment. Last month, Greta Bossenmaier, head of the agency, said cryptologists there are racing to find ways to protect information from quantum hackers.

Isara is part the quantum technology ecosystem supported and funded by Mike Lazaridis, co-founder of Research In Motion, now BlackBerry.

Lazaridis and Fregin founded Quantum Valley Investments in 2013. It has invested in several startups that are working out of its building on Westmount Road North. So far, only two have come out of stealth mode -- Cognitive Systems and Isara.

Isara has ties to the Institute for Quantum Computing and the Perimeter Institute for Theoretical Physics. Lazaridis founded the Perimeter Institute in 2000 and has donated $170 million to it. He also donated $100 million to the Institute for Quantum Computing.

Earlier this year, the Canadian government gave the institute $76 million to help advance its research. At that time, the institute said it expected to have a 100 qubit quantum computer within five years.

"We are here ultimately because it is an exciting problem. This is a fascinating area to be in, looking at the quantum age," Brown says. "So how do we go from desktop computing, to mobile computing to quantum computing and all those changes it will make to industry?"

New York Times
A WikiLeaks Lesson for Mrs. Clinton
Saturday, 22 October 2016

Editorial: The consensus by United States intelligence agencies is that the WikiLeaks dump of emails from the account of John Podesta, Hillary Clinton's campaign chairman, was the result of a hack by Russia in an effort to influence the presidential election. The leaks are continuing, so it's impossible to

say whether anything truly damaging to Mrs. Clinton will emerge. Some of the purloined exchanges consist of routine and often boring campaign planning, while others seem embarrassing or cynical, as when Clinton aides debate accepting campaign cash from foreign government lobbyists, and one writes: "Take the money!!"
None of the emails, at least so far, seem particularly harmful to Mrs. Clinton, although some suggest that her closest aides have the same concerns that weigh on many Americans -- that she can be thin-skinned and secretive.

As Neera Tanden, one of Mrs. Clinton's closest advisers, put it in the emails, "She always sees herself bending to 'their' will when she hands over information."

This is partly because of the endless investigations the Clintons' political enemies have pursued over the years. But that sort of scrutiny will surely intensify if she becomes president. Mrs. Clinton will only stir up her Republican critics by appearing secretive; she has a much better chance of shutting them down, as she did in her Benghazi hearing, with a dogged determination to show she has nothing to hide.

Fuller disclosure would clearly have helped her when it came to her lucrative speeches to Wall Street, a matter that has dogged her throughout this campaign. While she has released a full list of her speeches and fees, Mrs. Clinton has consistently refused to release the transcripts. From the snippets seen in the emails, one wonders why.

One speech has been politically problematic -- a 2013 presentation to Brazil's Banco Itaú in which she said, "My dream is a hemispheric common market, with open trade and open borders, some time in the future." Mr. Trump pounced on this as evidence that Mrs. Clinton favored unfettered immigration -- which seemed misleading given her long support for strong border security.

Over all, the excerpts from WikiLeaks suggest that Mrs. Clinton's speeches were what one would expect for audiences interested in global investment: talk about incentivizing growth and spurring entrepreneurship.

Imagine if months ago, Mrs. Clinton had done her own giant information release, including hundreds of pages of speeches to Goldman Sachs and Citi, to Salesforce.com, the United Fresh Produce Association and the Cardiovascular Research Foundation. Journalists and the public could have waded through them, discussed them, written about them -- and by now, everyone would have long since moved on.

Daily Telegraph (Australia)
Cybercrime costs us £11bn
Saturday, 22 October 2016

London - A terror plot targeting the London Underground has been uncovered after police found what they believe to be a bomb on a Tube train.

A 19-year-old man was Tasered and arrested by counter-terrorism officers yesterday following the discovery of the device aboard a train outside the O2 centre in south London on Thursday.

Last night it emerged that security officials had already contacted the Ministry of Defence to warn military personnel and that the threat level for transport in the capital had been raised to "severe".

The MoD told troops before the arrest: "It remains possible that the perpetrator may attempt to place further devices."

British Transport Police confirmed it had increased security and would be stepping up patrols.

The incident and subsequent arrest came 11 years after the 7/7 bombings when the London Underground was targeted in a terror attack that killed 52 passengers.

Details of the suspected plot emerged in a memo sent to serving military personnel that forwarded a warning from the security agency that gives terrorism alerts.

It said the Joint Terrorism Analysis Centre "has raised the threat level for transport in London to severe: an attack is highly likely".

It said: "This increase is in response to the discovery of a suspected viable improvised explosive device (IED) on a London Underground train yesterday.

"It is unknown who placed the device and what their motivation was. Therefore it remains possible that the perpetrator may attempt to place further devices. The threat level will continue to be reviewed as further information is received."

It is understood the threat level for transport outside London remains unchanged at "moderate".

The Home Office last night declined to say why the military had been contacted and other bodies including Transport for London and Network Rail also refused to comment.

The teenage suspect was arrested outside London Metropolitan University on Holloway Road, north London, about 10 miles from where the device was found in North Greenwich.

Witnesses described the young man being dragged to the ground by plainclothed masked officers carrying machineguns.

One onlooker said police appeared to be waiting for the suspect.

The man, described as Asian in appearance with black hair, was Tasered in the back.

A shop worker who did not want to be named said: "He was just walking down the street. He was definitely Asian and he definitely had black hair and I think he was in his twenties.

"Officers came from behind him and Tasered him. They jumped on him. He was on the floor. They checked him. They put him in a car and took him away. I saw the whole thing from where I work."

Specialist forensic officers will examine the suspect package over the weekend.

Scotland Yard said the arrest came "following the discovery of a suspicious item on a Tube in north Greenwich".

Financial Times
Chinese hackers targeted US aircraft carrier
Saturday, 22 October 2016
Byline: Jeevan Vasagar and Geoff Dyer

Washington - Chinese hackers targeted foreign government personnel who visited a US aircraft carrier the day before a contentious international court ruling on the South China Sea, according to a US cyber security company.
The China-based group created an infected document impersonating an official message addressed to officials visiting the USS Ronald Reagan, a nuclear-powered aircraft carrier which conducted patrols of the South China Sea in July.

The suspect document is dated July 11, the day before a tribunal in The Hague ruled against China's expansive claims in the region. The targets of the attack were delegates from a foreign government due to visit the aircraft carrier that day.

The document contained Enfal malware, which can be used to copy information from an infected computer or download further computer viruses.

According to FireEye, a US cyber security business, the China-based group that designed the suspicious document is the source of previous attempts to compromise US and Vietnamese national defence computer networks.

The likely goal of the "spear-phishing" attack -- a attack in the form of an email that appears to be from someone known to the recipient -- was to gather information on military manoeuvres and command and control systems, as well as policy issues, the company said.

There is no direct evidence to link the attempt with the Chinese government, and no indication the attack was successful.

According to FireEye's iSight unit, which identified the attack, the command and control system used for the infected file shared an IP address with a domain previously used by the China-based group.

This system was first identified in June, while the suspect document surfaced in September, FireEye says.

FireEye says the file -- which contains details of an itinerary for a visit to the aircraft carrier on July 11 this year -- is likely to have been distributed through targeted email messages.

Tensions over the South China Sea have fuelled high levels of cyber espionage in the region, according to a FireEye expert.

"Many governments and militaries in Southeast Asia lack cyber security controls that can effectively match these elevated threats," said Bryce Boland, the group's Asia-Pacific chief technology officer.

"For example, personal webmail and unmanaged devices aren't unusual, and many organisations lack the technology to detect unique attacks which haven't been seen before."

The USS Ronald Reagan and its escort ships conducted 53 days of operations in the western Pacific, including the South China Sea, this year.

The South China Sea patrols were intended "to maintain the seas open for all to use", according to a US Navy statement at the time.

Commander Clay Doss, a spokesman for the US Pacific Fleet, said: "As a matter of policy and for reasons of operations security, we won't comment on alleged vulnerabilities in networks or our efforts to mitigate them. We have full confidence in the integrity of the Navy's networks on which we conduct critical operations."

A US Navy official said that there was no indication the USS Ronald Reagan's classified information systems had been compromised, nor that the ship's operations in the South China Sea had been affected. The official said unclassified information about logistics was often shared with contractors and foreign governments to support port visits for ships.

In July a Chinese businessman was sentenced to nearly four years in jail for his part in an alleged conspiracy to steal military technical data from the computer networks of US defence contractors.

US prosecutors claim this conspiracy involved Chinese military officers.

New York Times
Man Who Took Trove of N.S.A. Data Has Court Date

Saturday, 22 October 2016
Byline: Scott Shane

Baltimore - The intelligence contractor accused in the largest-ever breach of classified information was portrayed by his lawyer in court on Friday as a patriot and a dedicated worker who became compulsive about taking work home.
An unlocked garden shed, stuffed with more classified documents than the contractor, Harold T. Martin III, could ever read, might be a symptom of a mental disorder, the lawyer said.

Mr. Martin, a rotund man with glasses whose striped gray jail garb stood out in an ornate federal courtroom here, sat silently during his first public appearance as his lawyer, James Wyda, argued that he should be released while awaiting trial.

The prosecution, opposing the request, described Mr. Martin, 51, in starkly different terms: as a serial lawbreaker of staggering audacity. Over two decades as a contractor for the National Security Agency and other government units, it said, he took home masses of secrets in full knowledge that it was illegal to do so. And, the prosecution added, there is no way to be certain what he has done with the information, or whether he might be hiding more.

At the end of an hourlong detention hearing, Magistrate Judge A. David Copperthite sided with the government and decided that Mr. Martin would remain in jail. He noted that Mr. Martin had a history of binge drinking, and concluded that he posed a flight risk because he saw in him a divided personality.

"You have someone here who presents himself as two different people," Judge Copperthite said, agreeing with the defense that mental health might be an issue.

"He presents himself as the protector of the N.S.A.," the judge said, referring to an unsent letter the F.B.I. found in which Mr. Martin scolded his colleagues as "clowns" who were incapable of protecting the nation's secrets. "Yet he walks out with and keeps in an unlocked shed information that enemies of this country would love to exploit."

Likewise, the judge said, Mr. Martin's wife, Deborah Shaw, who sat in the front row, told investigators she had no idea that he owned what prosecutors called an "arsenal" of 10 firearms, including an assault-style rifle and a pistol-grip shotgun.

"For 20 years this has gone on," the judge said, referring to Mr. Martin's collecting of classified material. "His family was there, and I'm sure they had no idea what was going on."

Judge Copperthite said that because Mr. Martin is currently charged with relatively minor criminal offenses -- theft of government property and unauthorized retention of classified material -- the law permitted him to consider only whether the defendant posed a risk of flight, not whether he might be

dangerous. But he suggested that he agreed with the government that Mr. Martin would pose a danger -- not necessarily a threat of violence, but a threat that he might further damage national security.

Prosecutors said that in a raid on Mr. Martin's suburban Maryland home in August, the F.B.I. took boxes of papers and an estimated 50 terabytes of electronic files -- equivalent to 500 million pages -- from his home office, shed and car. Much of it, they said, is highly classified material that should never have left the secure premises of the N.S.A., the Office of the Director of National Intelligence and Pentagon offices where Mr. Martin worked.

The scale of the data Mr. Martin is accused of taking home is many times greater than either the hundreds of thousands of N.S.A. documents that Edward J. Snowden gave to journalists in 2013 or the military reports and diplomatic cables that Chelsea Manning gave to WikiLeaks in 2010.

But after seven weeks of frantic investigation, F.B.I. and N.S.A. officials have not been able to show that Mr. Martin gave any of his collection to anyone else. Notably, they have not been able to link him to the disclosure of highly classified N.S.A. hacking tools that an anonymous group called the Shadow Brokers offered for sale on the web in August.

Officials, however, say that investigators cannot be certain that he is not the source of the Shadow Brokers material or that he has not transferred other secrets elsewhere, in part because Mr. Martin's cyberskills would make it possible for him to erase his electronic tracks.

One of the prosecutors, Zachary A. Myers, suggested the continuing frustration of F.B.I. agents who look at Mr. Martin's record of "betrayal and deceit" and believe he is not being candid about his motives or his actions.

"Suffice it to say that the government does not at this point believe that the defendant has been fully cooperative," Mr. Myers said.

For example, Mr. Myers said, after many hours of searching Mr. Martin's property, F.B.I. agents thought, and Mr. Martin assured them, that they had found all his material. Then they discovered that more disks containing stolen data were still in his house, hidden behind a bookshelf.

"There's no guarantee that he's not storing other information somewhere else that he has not told us about," Mr. Myers said, noting that Mr. Martin had software that might make it possible to stash data in the electronic cloud and leave no trace for investigators to find.

Mr. Wyda, a federal public defender and Mr. Martin's lead lawyer, said his client wanted only the best for the N.S.A. and for his country. Indeed, he suggested, it was Mr. Martin's very dedication that became his undoing.

"Hal was always driven by his desire to be better," Mr. Wyda said of his client, whom he called "a voracious learner." He began to take work home to master it, the lawyer said, and "it became a compulsion."

"The mental health factor is the only explanation for this that makes sense," Mr. Wyda added.

The lawyer said Mr. Martin was "no Edward Snowden" -- he did not share Mr. Snowden's political conviction that the government was violating privacy. Nor, Mr. Wyda said, was he Aldrich Ames or Robert Hanssen, employees of the C.I.A. and F.B.I. who sold secrets to the Russians.

"This was the behavior of a compulsive hoarder," Mr. Wyda said, mentioning that Mr. Martin's mother had also had hoarding tendencies. Keeping top secret material in plain view in his home and car was not the conduct of a spy or a political activist, he said, just a man carried away with his drive to master his work.

Mr. Wyda said Mr. Martin was in poor financial shape and could not afford to flee even if he wanted to. He insisted that his client was telling agents everything he knew.

After the judge's decision that Mr. Martin would return to a suburban jail for the many months that are likely to elapse before a plea or a trial, Mr. Wyda said that Mr. Martin and his family were "very disappointed" and that they would seek a review of the decision next week. Ms. Shaw and Mr. Martin's brother, Michael Martin, a nurse anesthetist who lives in Florida, left the courtroom and walked off into the rain without speaking to journalists.

Daily Telegraph
GCHQ using cyber attacks on Isil to aid battle to take Mosul
Saturday, 22 October 2016
Byline: Ben Farmer

London - GCHQ is using cyber warfare for the first time against Isil militants as part of the campaign to retake Mosul, the Defence Secretary has said.
The cyber attacks are understood to have targeted the communications of Islamic State of Iraq and the Levant to disrupt co-ordination in the Iraqi city.

Sir Michael Fallon told a conference organised by the Royal United Services Institute, a think tank on cyber warfare: "We are conducting military operations against Daesh [Isil] as part of the international coalition, and I can confirm that we are using offensive cyber for the first time in this campaign." He said £265 million is being pumped into "rooting out cyber vulnerabilities" in military and wider cyber-systems.

Straits Times
Singapore using cyber diplomacy as weapon against cybercrimes
Monday, 24 October 2016
Byline: Lim Yan Liang

Singapore - What more can Singapore do in a digital world where dependence on technology trades security for greater efficiency and connectivity?
With more countries using technology as a component of military response, the first thing to do is to treat the threat as seriously as a conventional one.

To this end, Singapore has been deploying 'cyber diplomacy' - building alliances with other countries, both to swop expertise, such as the latest in attack methods, and to regularly exercise and test its defences.

Singapore's Cyber Security Agency (CSA) has signed bilateral cyber agreements with five countries: France, the UK, India, the Netherlands and the US.

The agreement with the US, signed in August, is the first cyber agreement between an Asean nation and the US. This opens the door to regular exchanges on cyber issues and effectively gives Singapore a voice when the larger countries try to shape global cyber norms, according to experts.

"While Singapore benefits from accessing knowledge about cyber threats and mitigation responses from the US, Washington will equally gain deeper insights into the cyber threats experienced by Singapore and potentially the South-east Asian region," said US Army Lieutenant-Colonel Harry Hung, a visiting fellow with the S. Rajaratnam School of International Studies.

This and other recent efforts by the government demonstrate a cyber security approach that looks to leverage on the island's reputation as a global hub and a valued intermediary.

At the launch on October 10 of Singapore's cyber security strategy, a comprehensive document, which maps the country's long-term approach to the issue, Prime Minister Lee Hsien Loong said the government is sparing no effort to build a sizeable workforce of industry professionals here.

The four prongs of the strategy involve strengthening cyber defence of the country's critical infrastructure, developing a vibrant cyber security ecosystem by educating businesses and individuals, creating jobs by developing cyber security talent and building international partnerships to better respond to cyber threats.

This means the republic wants to work closely with Asean countries to jointly secure the region's Internet space, an ambitious undertaking, given the uneven level of development across the 10 member states.

Singapore has put its money where its mouth is. At the first official gathering of Asean ministers in charge of cyber security, held a day after the launch of Singapore's strategy document, Minister in charge of Cyber Security Yaacob Ibrahim launched a $10 million fund to assist fellow Asean countries in building their cyber threat response capabilities.

Besides helping to train technical professionals in neighbouring countries, the funds will be used to train policymakers, prosecutors and other officials to help these countries formulate their cyber policies, said CSA Chief Executive David Koh.

This is long-term thinking. With Asean countries building their fibre networks and the region becoming more connected, cooperation is necessary, so that no Asean member becomes the "weak link" that makes the community vulnerable, said Yaacob.

"What we want to do is ensure that all Asean member states pay attention, so that they don't become that weakest link," he said.

The money will also go towards organising an annual Singapore International Cyber Week (SICW), the first edition of which closed on October 12, having drawn 5,000 attendees from almost 50 countries.

They included more than 100 experts in the field from governments, the private sector and academia, such as the US Department of State's Coordinator for Cyber Issues, the UK's Cyber ambassador and the director-general of China's Bureau of Cybersecurity Coordination and Administration.

Yaacob also hosted several bilateral meetings with key Asean cyber security principals on the sidelines of the SICW.

This is something Singapore has done well in the past. Identify a niche where there are few platforms for countries to meet and discuss an issue of growing importance, then become the pre-eminent forum for leaders to come together, in big groups and private sessions, to tackle thorny issues.

It is a model learnt from the Shangri-La Dialogue - an annual defence forum that attracts high-ranking military and political officials here from every country, and one of the world's top security gatherings.

Together with the annual Asean Cert Incident Drill, organised by CSA and into its 11th edition, the plan is for Singapore to "start the conversation" and to be useful to the region and the world as a hub for cyber security cooperation, said Koh.

"Our perspective is cyber security is a team sport: no one country can do it by itself, and that's why Singapore is partnering with the other Asean member states," he said.

And in the same way that regional forums have given the collection of small states that is Asean a bigger voice in global matters, Singapore is hoping to take the lead in shaping the ongoing global conversation on acceptable behaviour in cyberspace.

"The world is shaping cyber norms, and we agree that we must have norms in cyberspace," said Yaacob.

"But how those norms are applicable to our region is something that we have to understand ourselves before they're being imposed by others," Yaacob added.

However, in order to become a global heavyweight in cyber matters, Singapore has to keep its own house in order. This is where the remaining three prongs of the national cyber security strategy come in.

The strategy document lays out a plan to strengthen the republic's cyber defences, especially for critical infrastructure, such as utilities and emergency services, and includes a new law to be introduced next year that will compel such operators to secure their systems and report breaches to the government in a timely manner.

It spells out how the government will step up public education to teach the public safe Internet-use practices to keep their devices clean and to keep the man in the street aware of common online scams.

It also fleshes out how the government intends to develop a home-grown cyber security fraternity - through heavy investment in research and development, more scholarships for students looking to enter the sector and opportunities for mid-career professionals in related fields to cross over.

The issue of cyber security is particularly important, given Singapore's push to become the world's first Smart Nation, where a vast array of sensors provide the government with feedback used to shape policies and the day-to-day lives of Singaporeans.

Such sensors also need to be secure, giving further impetus to the push for strong cyber security. For, as Lee put it at the launch of the strategy document: "To be a Smart Nation, we must also be a safe nation."

Al Jazeera
Cyber warfare: The new international warfront
Monday, 24 October 2016
Byline: Creede Newton

Mesa, Arizona - To enter the Arizona Cyber Warfare range (AZCWR), a person must have a signed waiver, the consent from the strict private security firm that guards the facilities, and the fortitude to withstand the salty language and messy environment created by the hackers inside.

"This is the only place in the world where the good guys can learn to hack from good guys who really know how to hack," Brett Scott, one of the founders of the AZCWR, told Al Jazeera inside their hacking headquarters.

The organisation is housed inside a complex that began as a research facility for top-secret military technology in the 1980s. The group has three missions: to educate the public on the merits of hacking by offering free courses, to change the realm of cyber-security for both the public and private sectors to gather, and to handle the enemies of the United States.

Right now, the enemy at the top of that list is the Islamic State of Iraq and the Levant (ISIL, also known as ISIS), which controls a dwindling swath of land in Iraq and Syria.

AZCWR uses "bots", or computer programs that take advantage of thousands of computers across the planet, to lodge complaints against ISIL Twitter pages.

"Our net effect is taking down 1,000 accounts a day," Scott said. When asked how his cadre of hackers, none of whom speak Arabic, are able to find the accounts, Scott responded that the AZCWR is given tips from intelligence agencies across the globe.

"If a housewife in France who lived through an attack wants to do something but doesn't know how she can download our bot. Then we'll use her computer to kick [ISIL] out of our world - the internet."

The AZCWR has been open to the public for two years, though it has been in operation for longer. It currently teaches roughly 2,000 active users on its website and at the physical location in "ranges" whose difficulty levels go from "Beginner" to "Jedi" in reference to the sci-fi film series, Star Wars.

There is an assortment of tasks, from the aforementioned take-down of an ISIL account to attacking, with consent, the cyber security systems of businesses.

Also, when a foreign adversary is not "paying enough attention" to the AZCWR for the group to gather intel, the hackers will "poke the bear", Scott said.

Scott has worked for various government agencies, and his experience with has left a bad impression. "The US has a very backwards idea towards hackers. Russia, China, and even ... countries like Iran are offering them huge amounts of money, luxurious cars, and nice flats."

In the US, Scott explained, hackers still face witch-hunts and harsh penalties when the government should offer employment. AZCWR is there to force decision-makers to re-evaluate their stance on technologically-capable but legally questionable computer users. "World War III is already here, and it's happening on the internet," the hacker said.

While the assertion that WWIII is happening on the internet sounds hyperbolic, there are those in the US government who agree with the sentiment.

Representative Mac Thornberry, the Chairman of the US House Armed Services Committee (HASC) which is responsible for oversight and funding of the Department of Defense (DoD) and the Armed Forces, has stated repeatedly that US cyber capabilities need more attention.

At a June meeting with the DoD and US Cyber Command's Deputy Commander Lieutenant General James K McLaughlin on cyber attacks, Thornberry said that just as the military has "an air campaign [against ISIL], we want to have a cyber campaign".

Al Jazeera spoke to an HASC aid on condition of anonymity on the subject. The aid said that while work could be done to enhance US cyber capabilities, the nation is "at the same level as anyone else ... but we're also as vulnerable to attack as anyone else".

While The government wants a cyber campaign against ISIL and others who attack the state, they don't want to encourage "cyber militias" to mount attacks against enemies. This opens them to "hack backs", or retaliatory measures, the aid said.

Thornberry and the defence establishment are concerned by recent hack attacks on high-level politicians such as the revelation of emails from the Democratic National Committee and former Secretary of State Colin Powell.

These attacks have revealed embarrassing details from behind the scenes of the US political theatre that has undermined an already contentious election season, and Issues of cyber security, especially recruitment of hackers to work with the government, are still a "struggle", but public-private partnerships are something about which "we've been very supportive", the aid concluded.

While US agencies may be struggling with the hacking war abroad, digital rights group, Electronic Frontier Foundation (EFF), fears its citizens are losing the war at home.

Mark Rumold, a senior staff attorney at EFF who focuses on government secrecy and has successfully worked to make public tens of thousands of previously classified government documents, told Al Jazeera that recent court rulings on a controversial case are "troubling".

The FBI's investigation surrounding Playpen, a website on the "Dark Web" network, which can only be accessed through the Tor network, and displayed thousands of images of child pornography is one such case.

The Tor network runs a user's internet protocol (IP) address, which is a unique signature given to a device, through thousands of relays to pre-empt surveillance and facilitate anonymity.

However, the FBI hacked and reconfigured the site to collect true IP addresses for use in cases against those who visited the site. Due to the wide range of visitors to the site, courts all over the US have been obliged to weigh in on the legality of the practice.

In June, a federal court in the FBI's home district decided that the US Constitution's Fourth Amendment, which guarantees the right of the people "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures", does not apply to home computers.

In a post on EFF's website, Rumold wrote the decision "is the latest in, and perhaps the culmination of, a series of troubling decisions" surrounding the Playpen investigation.

"Every single thing they could have gotten wrong, they did," Rumold told Al Jazeera in an interview. "It's the equivalent of law enforcement coming into your house and taking things out without a warrant."

While this one decision doesn't mean the Fourth Amendment no longer applies in any such case, Rumold explains that judges often show deference to rulings made by other district judges.

In an increasingly surveilled society, this could have serious consequences. "There's no question that technology has made our lives far more transparent than ever before, and that law enforcement is taking advantage," Rumold continued.

While there are "plenty of laws" governing hacker activity, as well as law enforcement's use of technology, the ever-changing digital landscape leaves a "grey space" in which troubling decisions can be made, the digital rights advocate concluded.

Back at the AZCWR, Scott said that the EFF is right "nearly 100 percent of the time", and that his band of hackers "operate inside the law. It's not our job to determine what the limits are. It's our job to push them."

Times of Israel
South Korea may rent Israeli satellite to spy on North
Monday, 24 October 2016
Byline: Stuart Winer

Jerusalem - South Korea is reportedly considering using an Israeli spy satellite to peek at North Korea's military and nuclear facilities as it ramps up its defense capabilities in response to threats from Pyongyang.
A South Korean Ministry of National Defense official said last week the country was looking to foreign intelligence agencies to provide information on North Korean activities, as it will take several years for the country to develop its own surveillance satellites, the Yonhap News Agency reported.

Seoul has become increasingly concerned after North Korea conducted five nuclear tests in the last ten years, several recently, and a series of missile tests, including of intermediate-range ballistic missiles.

According to a report on the Ynet news website on Saturday, Israel's Ofek 11 spy satellite could be in position to provide information on North Korea.

Israel and South Korea lie on similar latitudes, between 30 and 40 degrees north of the equator. The orbit trajectory of Ofek 11, which was launched in September and experienced some initial technical difficulties, carries it over the Korean region where its sophisticated monitoring equipment could be directed at North Korean facilities.

"The military is expected to have its own surveillance satellites as early as 2023 that will allow Seoul to closely monitor military activities in North Korea," the South Korean official said.

"It is years behind the defense ministry's original schedule to deploy five surveillance satellites between 2021 and 2022 as part of the country's 'kill chain' strike system to deal with missile threats from the North," the official added.

South Korea currently relies on US satellites for information about North Korean nuclear and missile sites.

Aside from its spying capabilities, the Israel satellite would also offer images of sites from different angles than those provided by the US orbiters, boosting the intelligence value of the information, the report said.

South Korea was also looking to buy German-made KEPD-350K cruise missiles which have a range of 500 kilometers, putting the North Korean capital within striking distance.

In August 2014, a top defense official told Israel's Army Radio that South Korea is one of several countries interested in purchasing the Iron Dome missile defense system.

Yedidia Yaari, CEO of Iron Dome manufacturer Rafael Advanced Defense Systems Ltd., said that the system's high success rate had piqued foreign interest, Reuters reported at the time.

The short-range missile defense system, developed with American funding, had been highly effective in the 2014 round of violence between Israel and Hamas, intercepting hundreds of rockets headed toward major population centers in Israel.

Haaretz
Major Weekend Cyberattack Was a Preview for Israel's Future Wars
Monday, 24 October 2016

Byline: Amos Harel

Jerusalem - The hacking that brought down websites in the United States and Europe on Friday seems to be the most extensive, sophisticated and ambitious attack of its kind the West has ever experienced. Over the past two years there have been two major hackings of civilian infrastructures in Ukraine and Turkey that were attributed - without it ever having been categorically proven - to Russia, in the context of conflict between it and the two neighboring countries. Israel had a similar hacking experience, of much lesser magnitude, during the last war in the Gaza Strip, which it was able to counter without real damage.
As of Saturday, neither the American government, nor experts interviewed in the media, had directly accused anyone of the attack. It is clear that the attack represents major offensive capability and that it required a great deal of preparation. Ostensibly, the immediate suspect is Russia, which has been accused over the past two months of being behind the hacking of senior officials in the Democratic Party, leaks to the Wikileaks site and the indirect assistance given to the campaign of Republican presidential candidate Donald Trump.

Just last week, Vice President Joe Biden hinted that the United States would consider cyber- retaliation against Russia if it continued the attacks. Precisely in this context, Russia might consider such extensive hacking too risky a gamble - and Moscow is usually an expert at pushing the edge, rather than undertaking suicide attacks.

The actual damage was apparently not very extensive. No American firm collapsed or stopped functioning, although some sites were shut down for a few hours. Denial of service attacks are nothing new; they are the preferred way of hacking civilian infrastructures in terms of the hackers' cost effectiveness, because the defending side can't totally stop the attack in a way that completely blocks their access to the internet.

According to Israeli cybersecurity experts, the success of such an attack depends on the recruitment of a sufficiently large mass of attackers and targeting the "internet of things" - that is, internet-connected household devices, rather than computers. Most state security bodies know how to identify computer systems connected to countries that represent a major danger; they blacklist and identify them and are thus able to stop an attack. But security cameras and refrigerators are not on any blacklists - and so up until now attacks by such devices have not been anticipated.

Now that the attack has happened, the relevant industries might have to re-assess their vulnerability to hacking via devices connected to the web. That is true, for example, in the car industry, where most new vehicles come off the assembly line connected to the internet.

Such an attack could happen in Israel in the future. There are rival countries, or those with vested interests, that could act against Israel. The country's security and military computer systems are fairly well protected and their interface with civilian systems is limited in a way that makes them hard to

strike. Civilian infrastructures, especially those not belonging to the state, are still quite exposed despite considerable progress in recent years in the field of cyber-security.

In any case, the cyber-events of the past two days seem like a taste of the future. In the short term, it remains to be seen whether Russia, or hackers associated with it, will be tempted to disrupt the U.S. presidential elections on November 8. In the longer term, it is clear that cyberattacks will be an inseparable part of any future conflict between two countries with technological capabilities.

While attacks by bombs and missiles require a great deal of international involvement, leave clear fingerprints and often spark harsh criticism, hacking is a different sort of weapon. It can be used to perpetrate a more mild strike that cannot always be traced to the perpetrators. Hacking is convenient for sending threatening signals, for an attack that can serve as an alternative to a military face-off, or for an opening strike after which the bombs and missiles come. Since Israel and the United States are fostering such capabilities, they are also aware of the possibility that their opponents know how to use similar means against them.

Fars News Agency
Iraqis Launch Cyber Army to Support Mosul Liberation Operation
Monday, 24 October 2016

Tehran - Iraqis from different walks of life, specially the country's media persons, launched a campaign on the Internet in support of the ultimate defeat of the ISIL terrorist group by the country's military forces, specially Hashd al-Shaabi (volunteer) troops, in the city of Mosul in Nineveh province.
The main purpose of the campaign is said to be working in parallel with the Iraqi security forces and covering the victories of the Iraqi army and volunteer forces in the war against the ISIL.

Hundreds of Iraqi people, including reporters, media persons, web bloggers and other Iraqis have voluntarily joined this "cyber army".

Speaking to FNA, Iraqi journalist and blogger Ali Vajih said the cyber army has been set up with the aim of supporting Iraq's joint military forces.

Iraqi Prime Minister Haidar Al-Abadi announced last Monday that the country's armed forces and popular troops had started large-scale operation to take back the ISIL's self-proclaimed capital, Mosul.

Prime Minister Al-Abadi appeared on the state TV an hour after midnight to declare that his country's army, security and mobilized volunteer troops have started the long-awaited offensive to take back the country's second-largest city.

"The hour has come and the moment of great victory is near," Al- Abadi said in a speech on state TV, flanked by the armed forces' top commanders.

Al-Abadi vowed that the military troops will take maximum caution to save civilian lives and avoid collateral damage in the city that is believed to still be home to over a million people.

The premier asked the civilian population to raise white flags over their buildings and contact the government troops for any kind of helpful information that they might have about ISIL militants.

"We urge you, the heroic people of Mosul, to cooperate with our security forces to rescue you," the Prime Minister added.

Mosul in Nineveh province that is ISIL's last stronghold in Iraq was occupied by the terrorist cult on June 10, 2014 and its liberation marks an era of demise for ISIL in Iraq.

Mosul was the first city taken by the terrorist group and it was there that ISIL Leader Abu Bakr Al-Baghdadi declared his so-called caliphate on June 29, 2014.

ISIL could stretch control over 40 percent of Iraq after it took Mosul over two years ago, but now holds only 10 percent of the country after losing battles in such major cities as Beiji, Tikrit, Fallujah and Ramadi in the last one year.

Mosul is of paramount importance both to Iraq and the ISIL as it is in an oil-rich region close to the borders with Syria and Turkey, while it has been a regional trade hub for the last several centuries. In addition to smuggling crude stolen from the oil wells of Nineveh, ISIL also levied forceful taxes for various reasons from the over 1-million-strong population that is still believed to be living in the city. Loss of Mosul will inflict a major blow to the terrorist cult as it will lose a major source of its revenues.

Iraqi army troops and volunteer forces (Hashd al-Shaabi) had been deployed 15 kilometers from Mosul two days ago.

"The reconnaissance operation in Mosul ended; we are waiting for the operations to kick off," Hashd al-Shaabi announced in a statement last Saturday.

Iraq's military forces have been bringing in a large number of troops, weapons, ammunition, armored vehicles, personnel carriers, tanks and other types of military equipment in preparation for the operation for the last several weeks, but many military and state officials and popular forces' commanders were slamming the US for pressurizing Baghdad to delay the operation for the last several months, a view that was even supported by US presidential candidate Donald Trump.

In his second televised debate with Hillary Clinton, Trump asked why the US has been hindering the operation for such a long time to give ISIL commanders and top brass to escape to Syria.

ISIL has also been preparing for the operation for the last several weeks. The terrorist group has reportedly used thousands of prisoners to dig a complicated network of tunnels and trenches around the city and filled the wide trench dug around the city with oil to put it on fire as it expects the city to go under siege by Iraq's joint military troops. The terrorist group has opened multiple fronts to confront the government troops.

Meantime, many ISIL top commanders, including Al-Baghdadi himself and his deputies, as well as their family members have left the city for Raqqa, the terrorist cult's second self-proclaimed capital.

Al-Baghdadi and his top aides left the city last week, while local sources in Nineveh disclosed on Sunday that the families of the ISIL terrorists that had left Mosul just arrived in the town of Merkedeh in Syria's Hasaka province.

"The ISIL commanders, including al- Baghdadi, are escaping Mosul to Syria," Iraqi Kurdistan Democrat Party's media director Saeed Mamouziti said last week.

He said that al-Baghdadi has also ordered his followers to completely destroy Mosul if they are defeated in the war against Iraq's joint military forces.

Later Mamouziti said that the ISIL militants were fleeing the city since the long-awaited large-scale operation to free Mosul was expected to be launched in the following days.

Meantime, local sources revealed that "ISIL commanders' families, including over 25 foreign families, escorted by military convoys reached the town of Merkedeh" on Sunday.

Earlier on Sunday, local sources in Nineveh province disclosed that the ISIL has brought to a halt all activities of its security offices in the city of Mosul.

"The ISIL has recently issued a circular in Mosul city according to which all its offices will halt operation until further notice," a local source said.

The source noted that the ISIL has already evacuated its security offices in several districts of Mosul in recent days, while many ISIL members seem confused to see the rush in their commanders' actions.

The US has also been pressuring Baghdad to keep the Hashd Al-Shaabi away from the operation, but they are now deployed to the battlefield after Prime Minister al-Abadi, the commander-in-chief of Iraq's armed forces, personally approved their participation in the Mosul operation last week.

The Iraqi media had earlier reported that the Mosul operations would start from several directions, the most important of which are al-Qayyara axis located 60 kilometers to the South of Mosul and Sahl Nineveh some 20 kilometers to the East of the city.

Wall Street Journal
Web Attack Stemmed From Game Tactics --- Outage made use of code, hacking tools that have become increasingly powerful
Monday, 24 October 2016
Byline: Robert McMillan, Rory Jones

New York - The computerized attack that left more than 1,200 websites unreachable on Friday stemmed from efforts, years earlier, by players of online games to frustrate and slow their opponents, security experts say.
The massive denial-of-service attack was launched from thousands of internet-connected devices, including cameras, video recorders and routers. It overwhelmed computer servers at Dynamic Network Services Inc., also known as Dyn, which plays a crucial role in connecting users to websites. Popular sites including Twitter Inc. and Netflix Inc. were unreachable for parts of Friday.

On Saturday, Dyn said the attack had ended, though it continued to investigate the causes.

Several security experts say the computer instructions for the attack had been refined from code written by disaffected videogame players calling themselves Lizard Squad who launched attacks on Christmas Day 2014 against online-game services operated by Sony Corp. and Microsoft Corp.

Since then, the experts said, the code and hacking techniques have been passed around and made more powerful. Friday's attackers used it to seize control of devices connected to the internet, many with weak security, and assemble them into an online army, or "botnet." Both the code, and the botnet, used in Friday's attack are called "Mirai."

By 2020, the research firm Gartner projects there will be 20 billion internet-connected devices, up from six billion now, raising the specter of more such attacks.

"These guys just started off as 'booters'. . .just kick your enemy off the videogame you've been playing," said Gary Warner, director of research with the Center for Information Assurance and Joint Forensics Research at the University of Alabama at Birmingham. "As the gaming companies came after the booters, they created Lizard Squad to come after the gaming companies."

Mr. Warner and others say there is no single creator of Mirai. Rather, it is essentially an open- source project that has gradually been refined from tools built by Lizard Squad and others.

Allison Nixon, a researcher with internet-security firm Flashpoint, said the attackers have "refined really, really clever ways of hurting people over the internet."

Today, there is a vibrant underground marketplace of so-called booter or stresser services that allow anyone to attack a computer on the internet. One service, NetStress.org, sells packages for as little as $6.99 that let purchasers launch denial-of-service attacks for 30 days.

Law-enforcement agencies are trying to keep up. On Sept. 8, Israeli police arrested two 18-year-olds, Itay Huri and Yarden Bidani, on suspicion of operating a company called vDOS that sold denial-of- service attacks and earned the pair more than $600,000 over the past two years, according to lawyers for the two teenagers.

Messrs. Bidani and Huri became friends about four years ago after meeting on an internet-game website, the lawyers said. They began operating vDOS when they were about 14, the lawyers said.

VDOS marketed its product as a way for companies to check the security of their own websites by launching denial-of-service attacks against themselves, the lawyers said. Lawyers for Messrs. Bidani and Huri said it wasn't their clients' fault if customers used the product irresponsibly.

They were placed under house arrest on Sept. 9, but were released 10 days later after a judge deemed that the police had insufficient evidence to charge them, the lawyers said. Israel's police force referred questions to the Ministry of Justice, which declined to comment on the arrests.

In the U.S., the Federal Bureau of Investigation last month charged two 19-year-olds, Zachary Buchta of Fallston, Md., and Bradley Van Rooy of the Netherlands, with conspiring to damage computers in four attacks in 2015 as part of the Lizard Squad group.

An attorney for Mr. Buchta didn't respond to requests for comment. An attorney for Mr. Van Rooy couldn't be reached.

Washington Free Beacon
Russian Hacks Bring U.S. Vulnerabilities to the Forefront
Monday, 24 October 2016
Byline: Morgan Chalfant

Washington - The reliance of the United States' critical infrastructure on high technology renders it vulnerable to future cyber attacks by the Russians, making it difficult for the U.S. government to retaliate against Moscow for trying to interfere with the presidential election.
The U.S. intelligence community formally accused Russia earlier this month of hacking into American political organizations, including the Democratic National Committee, in order to influence the 2016 election.

But experts warn that the United States should be wary of starting a "tit-for- tat" cyber war with the Russians, given that the U.S. economy and other critical systems are more dependent on advanced technology and therefore more vulnerable to attack.

"Though we have overwhelming power in this policy area, we are also the most vulnerable nation in terms of the very advancement of the Internet as a part of our society and as a part of our economy," Claude Barfield, a scholar at the American Enterprise Institute with expertise in international trade and cyber security, told a small audience in Washington, D.C., on Friday.

"We are afraid in terms of retaliating against the Russians that we will not be able to have what is called 'escalation dominance,'" Barfield continued. "In other words, you start a tit-for-tat. If the Russians came back at us, and if we went back at them, our economy and society are more vulnerable than the Russians, and the Russians know that."

The issue came to the forefront at a panel discussion on Chinese cyber attacks hosted last week in the nation's capital by the Victims of Communism Memorial Foundation. Moscow and Beijing are both highly capable and advancing in the cyber realm and have hacked into systems used by American companies and organizations, including the government.

"Picture it this way," said Fred Kaplan, author of Dark Territory, a book that explores the history of cyber warfare. "We have much more powerful and agile rocks, but we also live in a house that's made of much more glass, so that even countries with smaller rocks can do more damage to us."

The critical infrastructure of the United States--including its banking and financial systems, transportation, and energy infrastructure--relies on high computer technology networks vulnerable to hacking, Kaplan noted.

"Our entire society is built on this, our economy, our military, everything," Kaplan explained. "One reason why our leaders are a little reluctant to get into the equivalent of a limited nuclear exchange with cyber weapons is that we are really more vulnerable than other countries which are not quite hooked up."

The Department of Homeland Security and the Office of the Director of National Intelligence said on Oct. 7 that the Russian government directed the DNC hack and other compromises of emails used by U.S. citizens and institutions. Representatives of the Russian government, meanwhile, have called the allegations groundless.

The White House has pledged to retaliate against Russia for the hacks with a "proportional response," though it remains unclear what such a response might look like.

"The president has talked before about the significant capabilities that the U.S. government has to both defend our systems in the United States but also carry out offensive operations in other countries," White House Press Secretary Josh Earnest told reporters on Oct. 11. "So there are a range of responses that are available to the president and he will consider a response that is proportional."

Both Russia and China have emerged as strong cyber powers that pose threats to the United States. Russian hackers are believed to be responsible for cyber attacks against the United States that infiltrated computer networks used by the White House, State Department, and Pentagon, as well as hacks of private U.S. entities in recent years.

Evidence also suggests that Russia targeted Ukraine's power grid in December 2015, a cyber attack that caused widespread outages.

"We see a lot of organized criminal behavior coming out of Russia in the cyber realm. But they also have nation- state capabilities. They are probably, next to the United States, the most powerful cyber offensive capability," Rep. Michael McCaul (R., Texas), chairman of the House Committee on Homeland Security, told the Washington Free Beacon in September before Russia was formally implicated in the DNC hacks.

"We see them shut down countries like Estonia, they shut down power in Ukraine. They have meddled in elections in the past. Without getting into all the details, attempts have been made by the Russians in that regard," he said.

China has regularly hacked U.S. companies, and Chinese hackers were responsible for the massive Office of Personnel Management data breach that exposed personal information of 22 million Americans in 2014.

Such attacks have persisted despite cyber pacts between these nations and the United States meant to curb hacking attempts.

The alleged Russian hacks resulted in thousands of embarrassing correspondences between DNC staffers being leaked by WikiLeaks days before the committee's convention in July. WikiLeaks, which has more recently been publishing hacked emails sent and received by John Podesta, Democratic nominee Hillary Clinton's campaign chairman, has denied having connections to Moscow.

Russia's cyber campaign has aggravated an already tumultuous election cycle and fueled speculation about whether the Kremlin is trying to aid Republican nominee Donald Trump, who has made positive statements about Russian President Vladimir Putin. Clinton has referred to the cyber attacks when undermining her opponent as a "puppet" of Russia.

The allegations also further heightened tensions between Washington and Moscow that have run high over the conflict in Syria and Russia's illegal annexation of Ukraine's Crimean Peninsula more than two years ago.

USA Today

Divisive election sparks 'massive rise' in hateful tweets ; Trump's inflammatory rhetoric fanning flames of anti-Semitism, racism on Twitter, observers say (Canada)
Monday, 24 October 2016
Byline: Jessica Guynn

Washington - On Sunday night, Hadas Gold, a Politico media writer, began receiving threats on Twitter. One image superimposed a yellow star of David on her shirt and a bloody bullet hole in her forehead. Another Photoshopped her face on a corpse in a concentration camp oven. The message: "Don't mess with our boy Trump, or you will be first in line for the camp."

Gold, whose grandmother fled Poland with her family weeks before Jews from their neighborhood were deported to concentration camps and whose grandfather lost about half of his extended family in the Holocaust, notified Twitter, which moved quickly to suspend the accounts.

Gold says these incidents have become increasingly common "the more we wrote about Trump, and the more we wrote about his rhetoric."

A report this week from The Anti-Defamation League documented the rise in anti-Semitic tweets targeting journalists who cover the Republican presidential candidate. From August 2015 to July 2016, the ADL found 2.6 million tweets with anti-Semitic language. Of those, nearly 20,000 tweets were directed at 50,000 journalists in the U.S., with more than two-thirds of the tweets sent by 1,600 Twitter accounts. Words that appear frequently in the profiles of these Twitter accounts: Trump, nationalist, conservative, white.

"The report is representative of the bigotry and hatred that we are seeing play out on a broader scale," said Oren Segal, director of ADL's Center on Extremism and an author of the report.

During this turbulent election season that has fanned the flames of racism, xenophobia, sexism and bigotry, hate speech that typically resides in the dark recesses of the Internet has bubbled into the mainstream and onto Twitter, a popular online hangout for journalists and politicians such as Trump, who has millions of followers there.

Because people don't have to use their real names on the service, they can attack people of color, women, Muslims and other groups with very little risk.

"This is only a fraction of what's happening online right now as a result of the legitimacy (that) various extremist ideologies have been given in this campaign season," said Ryan Lenz, editor of the Southern Poverty Law Center's Hatewatch blog. "We have seen a massive rise of hate speech."

Trump campaign spokeswoman Hope Hicks says the campaign has "no knowledge of this activity" and strongly condemns "any commentary that is anti-Semitic."

"We totally disavow hateful rhetoric online or otherwise," Hicks wrote in an emailed statement.

Conversations that take place on Twitter, famous for its 140- character limit, tap into the nation's pulse, be it the protests on the streets of Ferguson, Mo., the congressional sit-in over gun control or the launch of Beyonce's Lemonade album. But more and more, people venturing onto the service to catch up on news or with friends are confronted with hatred and bigotry spewed by the fringes of society, Segal says.

"When there is such a volume, we have to ask ourselves what can we do? What can the Internet service providers do? What can vast segments of society do? So that we hold people accountable and create safe spaces online the way we expect those spaces to be in the real world," he said.

For years, Twitter has faced sharp criticism for not aggressively enough policing abuse and harassment on its service. Twitter says its rules "prohibit inciting or engaging in the targeted abuse or harassment of others."

Yet, if anything, abuse has increased. In one of the highest- profile incidents, Leslie Jones, who starred in the remake of the Ghostbusters movie, temporarily left Twitter after being targeted by racist trolls who compared her to primates including Harambe, the gorilla shot dead in May at the Cincinnati zoo.

"Ok I have been called Apes," she wrote on Twitter at the time, "even got a pic with semen on my face. I'm tryin to figure out what human means. I'm out."

Trump's inflammatory rhetoric and policy positions such as banning Muslims from entering the U.S. "have really mainstreamed Islamophobia in our nation," said Ibrahim Hooper, communications director for the Council on American-Islamic Relations.

"He's given permission to all those who held anti-Muslim views or might have formed anti-Muslim views recently to go public with them quite proudly. Whereas before maybe they would have been reluctant to be so open about their bigotry, now you have a major American public figure saying that's perfectly OK. In fact, it's somehow patriotic," Hooper said.

Trump supporters have taken to Twitter and Facebook with hateful messages, saying in effect: "'Wait until Donald Trump gets into office and all of you will be gone. You will be in jail. Islam will be banned," he said.

Irfan Chaudhry, a criminology instructor at MacEwan University in Edmonton, Canada, who has researched racism on Twitter, says these disturbing attacks that tend to be spurred by election-season politics have been happening on Twitter for years, just never at this volume.

"During the last election, a lot of people were still trying to get a handle on what social media is," Chaudhry said. "Now they know what it is, and now we are able to utilize it in more data-driven and analytical ways that give us these insights we weren't aware of before."

Observers say the targeting of specific groups of people by hate speech, particularly Jewish journalists, has dramatically intensified during the Trump campaign.

The anti-Semitic hate speech is coordinated in a way it has not been against any other group, said Sophie Bjork-James, a post- doctoral fellow in the anthropology department at Vanderbilt University. "While various groups have been targeted with hate speech on Twitter during this election, I don't think anything compares to what Jewish journalists are going through," Bjork-James said. "Many white nationalists have been inspired by the Trump campaign to increase their involvement, and a central part of this ideology is anti-Semitism."

Washington Free Beacon
Military Warns Chinese Computer Gear Poses Cyber Spy Threat (Canada)
Monday, 24 October 2016
Byline: Bil Gertz

Washington - The Pentagon's Joint Staff recently warned against using equipment made by China's Lenovo computer manufacturer amid concerns about cyber spying against Pentagon networks, according to defense officials.
A recent internal report produced by the J-2 intelligence directorate stated that cyber security officials are concerned that Lenovo computers and handheld devices could introduce compromised hardware into the Defense Department supply chain, posing cyber espionage risks, said officials familiar with the report. The "supply chain" is how the Pentagon refers to its global network of suppliers that provide key components for weapons and other military systems.

The J-2 report was sent Sept. 28, and also contained a warning that Lenovo was seeking to purchase American information technology companies in a bid to gain access to classified Pentagon and military information networks.

The report warned that use of Lenovo products could facilitate cyber intelligence-gathering against both classified and unclassified--but still sensitive--U.S. military networks.

One official said Lenovo equipment in the past was detected "beaconing"--covertly communicating with remote users in the course of cyber intelligence-gathering.

"There is no way that that company or any Chinese company should be doing business in the United States after all the recent hacking incidents," the official said.

About 27 percent of Lenovo Group Ltd. is owned by the Chinese Academy of Science, a government research institute. In April, a Chinese Academy of Sciences space imagery expert, Zhou Zhixin, was named to a senior post in the Chinese military's new Strategic Support Force, a unit in charge of space, cyber, and electronic warfare.

China has been linked by the National Security Agency to large- scale cyber spying against both the Pentagon and American and foreign defense contractors.

Joint Staff spokesman Capt. Greg Hicks declined to comment on the J-2 report but said the military is wary of foreign nations' cyber spying.

"Although we are concerned any time another nation or individual attempts to initiate intelligence collection against the Department of Defense, we do not discuss internal assessments," Hicks said.

Lenovo spokesman Ray Gorman said he was unaware of the Joint Staff concerns.

On company efforts to acquire American information technology firms, Gorman said "we have stated many times that we continue to look worldwide for opportunities that make sense for our customers and shareholders, add value to our product portfolio, and help keep us on track for continued profitable growth." He declined to comment on specific acquisition talks.

A Pentagon spokesman said the Defense Department has not imposed a "blanket ban" on all Lenovo products and does not blacklist suppliers or individual products.

Pentagon policy for protecting mission critical functions in securing computer systems and networks "requires the department to perform supply chain risk management functions when acquiring products for use in its national security systems," the spokesman said, adding that the analysis is done on a case-by-case basis.

Rep. Robert Pittenger who has investigated Chinese cyber risks in the past, said he is concerned by the Joint Staff report.

"Chinese cyber security and supply chain concerns remain a significant problem for both the Defense Department and the remainder of the federal government," Pittenger (R., N.C.) told the Washington Free Beacon.

Pittenger said it is important for Congress to press Pentagon acquisition officials "to act swiftly on perceived cyber- threats and remove IT vendors from our supply chain if evidence exists suggesting a security vulnerability."

"I would be very disappointed to learn, however, if the Defense Department or the Air Force sought to obfuscate the facts regarding contracts with Lenovo when this issue was brought to my attention back in April," he added.

On Friday the chairman of the House Judiciary Committee wrote to the FBI warning that secrets stored on former secretary of state Hillary Clinton's private email server may have been compromised by a Clinton aide's use of a Lenovo computer.

Rep. Bob Goodlatte (R., Va.) stated in a letter to FBI Director James Comey that Heather Samuelson, former White House liaison to the State Department, used two Lenovo laptops to sort some of the thousands of classified emails from Clinton's server.

"Lenovo computers, and specifically the models used by Heather Samuelson for reviewing classified emails, have been shown by the Department of Homeland Security (DHS) to contain software, dating back to 2010, that permits remote hacking attacks," Goodlatte stated.

Disclosure of the Joint Staff warning comes after a similar warning from the Air Force Cyber Command in April.

An email notice stated that "per AF Cyber Command direction, Lenovo products are being removed from the Approved Products List and should not be purchased for DoD use."

"Lenovo products currently in use will be removed form the network," the email stated.

The Air Force later sought to play down the warning in the email and a spokesman told reporters the email was "coordinated" and should not have been sent.

Lenovo equipment has been a major cyber espionage worry since the company first purchased IBM's laptop computer business in 2005.

A congressional China commission report produced several years ago revealed that the Army Cyber Directorate in 2007 investigated a Lenovo-brand desktop computer that was engaged in "beaconing activity." The report said the beacon was a "self-initiating attempt to establish a connection to a suspicious foreign entity."

Rep. Mike Pompeo, a member of the House Permanent Select Committee on Intelligence, said the risks posed by Lenovo technology are serious.

"It is critical that the U.S. government, particularly the Pentagon, use the most secure technology available," Pompeo (R., Kan.) said.

"The threat from cyber attacks is real and demonstrated, as seen by China's hack of the Office of Personnel Management, which impacted millions of Americans," he added. "The U.S. must take all reasonable steps to ensure we are not an easy target for our enemies, competitors, or even partners."

Larry Wortzel, a former military intelligence official and member of the congressional U.S.- China Economic and Security Review Commission, said he helped alert security officials to a plan by the State Department to purchase 900 Lenovo computers in 2006. The computers would have been used to handle classified information and the State Department canceled the sale over cyber spying concerns.

"The Chinese government has a major stake in Lenovo," Wortzel said in an email.

"China remains one of the main threats to U.S. government and corporate information systems," Wortzel added. "One way to keep those systems safe is to ensure you are not getting system updates that may have a back door that can be opened by a Chinese intelligence service."

A National Security Agency document made public by renegade contractor Edward Snowden revealed that China has stolen sensitive military technology through cyber attacks, including radar designs, engine schematics, and other data through a program code-named Byzantine Hades. The program caused "serious damage to DoD interests," according to a briefing slide.

NSA detected more than 30,000 cyber attacks, including more than 500 significant intrusions into Pentagon systems. The attacks broke into at least 1,600 network computers and caused more than $100 million in damage.

Data stolen included Pacific Command aerial tanker refueling schedules, Transportation Command logistics information, and Navy nuclear submarine and anti-aircraft missile designs.

In 2014, Lenovo purchased IBM's BladeCenter line of computer servers for $2.1 billion. The sale prompted the Navy to replace the upgraded IBM servers within Aegis battle management systems deployed on guided missile destroyers and cruisers over concerns China could hack the Navy's most advanced warships through the server.

Specifically, the equipment being replaced is IBM's x86 BladeCenter HT server, a part of the Aegis Technical Insertion, or "TI," 12.

The upgrades, first reported last year by USNI News, involve TI-12 hardware upgrades, and the Advanced Capability Build, or "ACB," 12 software upgrades. The components make up the Aegis Baseline 9 combat system upgrade, which combines ballistic missile defense and anti-air warfare upgrades for the warships.

According to the Department of Homeland Security, Lenovo computers since September 2014 were loaded with adware called Superfish that could allow hackers to spoof encrypted security controls in

what are called "man-in-the-middle" cyber attacks. The attacks allow hackers to take over secure web browsers.

Lenovo purchased Motorola Mobility, the company's cell phone division in 2014, and has sought to buy the Canadian cell phone maker BlackBerry in the past.

Lenovo in the past has denied its products are engaged in cyber espionage. "Lenovo has been a trusted supplier of information technology in the U.S. since 2005 when it bought the IBM ThinkPad PC business," the company said in a statement. "Every single company selling technology to the U.S. government--including HP, Dell, Cisco, Apple, and Lenovo--use foreign components in their products. So it's critical that the U.S. continue to follow a standards- based process that allows for procurement of technology that is both cutting edge and totally secure."

U.S. intelligence agencies in August 2015 warned that Lenovo, along with another Chinese-government-linked firm, Huawei Technologies, had shipped some 80,000 computers to several nations in the Caribbean. The computers were found to contain spyware that can permit remote intrusions.

The cyber spying concerns are not limited to the Pentagon.

The Australian Financial Review newspaper reported in 2013 that all of the "Five Eyes" intelligence services--those in the United States, Britain, Australia, Canadian, and New Zealand--strictly prohibit the use of Lenovo computers over concerns about the potential for cyber espionage.

Yonhap English News
N.K. resumes encrypted numbers broadcast after 9-day break
Sunday, 23 October 2016

Seoul - North Korea's state radio station resumed broadcasting mysterious numbers Sunday after a nine-day break that could be some kind of coded message to its agents operating in South Korea.
An announcer at Radio Pyongyang, started reading a series of messages shortly after midnight (Seoul time), calling out a series of numbers.

The announcer said she is "giving review work in metal engineering to No. 21 expedition agents." The content was the same as those transmitted in the early hours of Oct. 9.

Since June 24, North Korea has sent out a total of 10 encrypted numbers broadcasts, with three being broadcast this month alone.

Broadcasts of mysterious numbers are a kind of book cipher that was often used by North Korea to give missions to spies operating in South Korea during the Cold War era. Spies could decode numbers to get orders by using a reference book, although many intelligence officials believe this form of sending

orders to be totally outdated. Many have said the broadcast may be some sort of deception strategy aimed at sparking confusion within South Korea.

Pyongyang had initially suspended such broadcasts in 2000, when the two Koreas held their first historic summit.

Tensions are already running high on the divided peninsula after North Korea carried out its fifth nuclear test on Sept. 9 and the unsuccessful launching of two Musudan intermediate-range ballistic missile in recent weeks.

Sunday Times (UK)
Hackers smell blood after co-opting 'internet of things'
Sunday, 23 October 2016
Byline: Mark Hookham

London - An army of copycat hackers could seize control of internetconnected home devices to carry out cyber-attacks, security experts have warned.
Web-connected "smart" gadgets including cameras, digital TV recorders, smart kettles and plugs are all vulnerable to being hacked by criminals and used remotely to mount cyber-attacks, according to James Lyne, head of security at Sophos, a security firm.

The warning follows one of the largest cyber-attacks involving home internet devices, which disrupted a number of popular websites on Friday, including Twitter, Spotify and Reddit. Airbnb, PayPal, Netflix, Yelp and some businesses hosted by Amazon were also affected.

The hack has raised questions about the security of the so-called internet of things -- networks of devices, ranging from central heating thermostats to fridges, baby monitors and home lighting, that connect online and can be controlled remotely by their owners from phones or tablets.

"Cyber-criminals have smelt the blood in the water and the sharks are circling," Lyne said. "We are going to be seeing a hell of a lot more of this in the next little while."

Security analysts believe the hackers responsible for last week's attack had used a malicious code to infect almost 500,000 devices, including digital video recorders and CCTV cameras.

Many of the devices involved were believed to be in the US, Brazil and Colombia and were made by Chinese manufacturers with easy-to-guess usernames and passwords.

The hackers used this so-called zombie or botnet army of hacked devices to launch a form of mass attack called a "distributed denial of service" (DDoS), in which a website is bombarded by messages sent by the hacked devices.

The target was a US company called Dyn that acts as a "switchboard" for internet traffic, helping direct users to some of the world's most popular websites.

The attack came hours after Doug Madory, a researcher at Dyn, presented a talk in Texas on cyber-criminals. Such DDoS attacks are favoured by cyber-attackers trying to make a political point.

A tweet from WikiLeaks, which has released thousands of emails hacked from the account of Hillary Clinton's campaign chairman, suggested that its supporters were behind the attack. "We ask supporters to stop taking down the US internet," the tweet said. "You proved your point."

Members of a shadowy collective called New World Hackers also claimed responsibility but US officials and cyber-security experts have yet to pinpoint the source.

The code -- or malware -- that infected the devices is known as "Mirai" and was last month used to launch a similar assault against the website of Brian Krebs, a US security blogger.

Krebs said: "Mirai scours the web for IoT [internet of things] devices protected by little more than factory-default usernames and passwords and then enlists the devices in attacks that hurl junk traffic at an online target until it can no longer accommodate legitimate visitors or users."

At the beginning of this month, the hacker responsible for Mirai released its source code online, in effect letting anyone build their own attack army. Earlier this month the government's newly formed National Cyber Security Centre (NCSC), part of the GCHQ spy agency, warned that "less technically capable" hackers were now able to use the code and "quickly start building" their own network of colonised devices.

In a blog posted before last week's attack, the NCSC highlighted how Mirai had been programmed to guess 68 different username and password combinations.

Lyne said there was a "morass" of "mid-tier cybercriminals" who were prepared to exploit the new malware to launch online fraud or steal data. "Any time source code like this is released it gives inspiration, ideas and ease of access to that larger community of cyber-criminals."

He said he had been shocked to discover how poorly protected internet-enabled household devices were from being hacked. He recently examined 12 web-connected CCTV cameras and found that they could all be hacked and accessed remotely.

Multimillionaire Russian hacker hits the skids as FBI pounces, page 22

The ghost in the machine

1 Hackers use a malware code to infect vulnerable internet-connected home devices

2 The code creates a 'zombie army' of hundreds of thousands of hacked devices such as digital TV recorders and CCTV cameras

3 The devices are then instructed to attack websites by bombarding them with thousands of junk messages that knock them offline

Tolo News
Taliban Using? Camera Drones In Helmand
Sunday, 23 October 2016
Byline: Faridullah Hussainkhail

Kabul - The Taliban has released a video of drone footage taken of the Nawa district in Helmand, which is under their control, the Helmand media office said in a statement.
According to the statement the Taliban have received the drones from outside intelligence agencies and are using these for operational purposes.?

In June 2016 the National Unity Government (NUG) banned the use of camera drones in Afghanistan due to security issues.

This move was however met with mixed reaction.

"With consideration of certain security issues and for the sake of national interests, the national security council has decided that drone cameras will no longer be allowed to be used in Afghanistan, the government of Afghanistan has major respect for media activities and because of this it has taken the decision," a spokesman to CEO Jawed Faisal said at the time.

But Afghan media companies and journalists slammed government's move to ban the use of camera drones during media coverage of events in the country, terming the move a violation of the mass media law.

They also said it is an attempt to restrict media activities.

Daesh militants have however used the hi-tech devices to film their own rocket attacks for propaganda videos in Iraq.

Times Colonist (Victoria)
Digital doors should be secure
Saturday, 22 October 2016

Editorial: In the legislative building and in other government offices, security officials go around after business hours to make sure everything is locked and secure. In the business of running the government, it would be unthinkable to leave doors ajar and filing cabinets open.
That same diligence has not always been applied to government-owned electronic devices that store and allow access to a wide array of sensitive information. As the provincial government rolls out its strategy concerning mobile devices, it should seek ways to keep up with technological change, rather than playing catch-up.

Two independent watchdogs released companion reports Tuesday saying there's a risk that government information could fall into the wrong hands because of slack security measures regarding tablets, smartphones and other mobile equipment.

Government safeguards have failed to keep pace with rapid advances in technology, say auditor general Carol Bellringer and acting information and privacy commissioner Drew McArthur.

The two watchdogs audited five ministries and the office of the chief information officer. These are some of their findings:

No central record is kept of mobile devices with access to government information. "You can't protect what you don't know about," said Bellringer.

The choice of installing anti-malware software or activating security features on phones is often left to employees, and it doesn't always happen.

Policies are often overlapping and confusing.

Employees sometimes took months to report a lost or stolen device.

Staff training did not cover mobile devices.

The watchdogs made several recommendations, and Technology Minister Amrik Virk said the government is already implementing measures to fix the problems identified by Bellringer and McArthur.

Those measures include maintaining detailed inventories of all mobile devices, ensuring additional security settings are applied before a device goes into service, enforcing a maximum inactivity-until-locked time, and installing and maintaining anti-malware software.

It would seem such measures would be a given, but smartphones and tablets have become so much part of life, it's easy to take them for granted, to overlook the power they have to find, store and disseminate information. We value how easy they are to use and how much they can do for us.

But those strengths are weaknesses, if the devices fall into the wrong hands. Complacency can be dangerous.

It's comforting know the government is taking the right steps, but it's a little disturbing that it is acting only now. It is common knowledge that bad things can happen when a tablet or smartphone is misplaced or stolen.

An individual's life can be seriously disrupted, as many people have learned, if someone gains access to personal data stored on or connected to a smartphone. If the device is used in government business, the potential for damage is exponentially greater.

For most people, not keeping pace with technological change can be inconvenient. For government, it is dangerous.

New York Times
New Weapons Used in Attack on the Internet
Saturday, 22 October 2016
Byline: Nicole Perlroth

San Francisco - Major websites were inaccessible to people across wide swaths of the United States on Friday after a company that manages crucial parts of the internet's infrastructure said it was under attack.
Users reported sporadic problems reaching several websites, including Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud and The New York Times.

The company, Dyn, whose servers monitor and reroute internet traffic, said it began experiencing what security experts called a distributed denial-of-service attack just after 7 a.m. Reports that many sites were inaccessible started on the East Coast, but spread westward in three waves as the day wore on and into the evening.

And in a troubling development, the attack appears to have relied on hundreds of thousands of internet-connected devices like cameras, baby monitors and home routers that have been infected -- without their owners' knowledge -- with software that allows hackers to command them to flood a target with overwhelming traffic.

A spokeswoman said the Federal Bureau of Investigation and the Department of Homeland Security were looking into the incident and all potential causes, including criminal activity and a nation-state attack.

Kyle York, Dyn's chief strategist, said his company and others that host the core parts of the internet's infrastructure were targets for a growing number of more powerful attacks.

"The number and types of attacks, the duration of attacks and the complexity of these attacks are all on the rise," Mr. York said.

Security researchers have long warned that the increasing number of devices being hooked up to the internet, the so-called Internet of Things, would present an enormous security issue. And the assault on Friday, security researchers say, is only a glimpse of how those devices can be used for online attacks.

Dyn, based in Manchester, N.H., said it had fended off the assault by 9:30 a.m. But by 11:52 a.m., Dyn said it was again under attack. After fending off the second wave of attacks, Dyn said at 5 p.m. that it was again facing a flood of traffic.

A global event is affecting an upstream DNS provider. GitHub services may be intermittently available at this time. -- GitHub Status (@githubstatus) October 21, 2016

A distributed denial-of-service attack, or DDoS, occurs when hackers flood the servers that run a target's site with internet traffic until it stumbles or collapses under the load. Such attacks are common, but there is evidence that they are becoming more powerful, more sophisticated and increasingly aimed at core internet infrastructure providers.

Going after companies like Dyn can cause far more damage than aiming at a single website.

Dyn is one of many outfits that host the Domain Name System, or DNS, which functions as a switchboard for the internet. The DNS translates user-friendly web addresses like fbi.gov into numerical addresses that allow computers to speak to one another. Without the DNS servers operated by internet service providers, the internet could not operate.

In this case, the attack was aimed at the Dyn infrastructure that supports internet connections. While the attack did not affect the websites themselves, it blocked or slowed users trying to gain access to those sites.

Anyone else having a whole lot of trouble with sites loading properly this morning? Paypal is down, Twitter was down, Netflix half loading. -- Emmy Caitlin (@emmycaitlin) October 21, 2016

Mr. York, the Dyn strategist, said in an interview during a lull in the attacks that the assaults on its servers were complex.

"This was not your everyday DDoS attack," Mr. York said. "The nature and source of the attack is still under investigation."

Later in the day, Dave Allen, the general counsel at Dyn, said tens of millions of internet addresses, or so- called I.P. addresses, were being used to send a fire hose of internet traffic at the company's servers. He confirmed that a large portion of that traffic was coming from internet-connected devices that had been co-opted by type of malware, called Mirai.

Dale Drew, chief security officer at Level 3, an internet service provider, found evidence that roughly 10 percent of all devices co-opted by Mirai were being used to attack Dyn's servers. Just one week ago, Level 3 found that 493,000 devices had been infected with Mirai malware, nearly double the number infected last month.

Mr. Allen added that Dyn was collaborating with law enforcement and other internet service providers to deal with the attacks.

In a recent report, Verisign, a registrar for many internet sites that has a unique perspective into this type of attack activity, reported a 75 percent increase in such attacks from April through June of this year, compared with the same period last year.

The attacks were not only more frequent, they were bigger and more sophisticated. The typical attack more than doubled in size. What is more, the attackers were simultaneously using different methods to attack the company's servers, making them harder to stop.

The most frequent targets were businesses that provide internet infrastructure services like Dyn.

"DNS has often been neglected in terms of its security and availability," Richard Meeus, vice president for technology at Nsfocus, a network security firm, wrote in an email. "It is treated as if it will always be there in the same way that water comes out of the tap."

Last month, Bruce Schneier, a security expert and blogger, wrote on the Lawfare blog that someone had been probing the defenses of companies that run crucial pieces of the internet.

"These probes take the form of precisely calibrated attacks designed to determine exactly how well the companies can defend themselves, and what would be required to take them down," Mr. Schneier wrote. "We don't know who is doing this, but it feels like a large nation-state. China and Russia would be my first guesses."

It is too early to determine who was behind Friday's attacks, but it is this type of attack that has election officials concerned. They are worried that an attack could keep citizens from submitting votes.

Thirty-one states and the District of Columbia allow internet voting for overseas military and civilians. Alaska allows any Alaskan citizen to do so. Barbara Simons, the co-author of the book "Broken Ballots: Will Your Vote Count?" and a member of the board of advisers to the Election Assistance Commission,

the federal body that oversees voting technology standards, said she had been losing sleep over just this prospect.

"A DDoS attack could certainly impact these votes and make a big difference in swing states," Dr. Simons said on Friday. "This is a strong argument for why we should not allow voters to send their voted ballots over the internet."

This month the director of national intelligence, James Clapper, and the Department of Homeland Security accused Russia of hacking the Democratic National Committee, apparently in an effort to affect the presidential election. There has been speculation about whether President Obama has ordered the National Security Agency to conduct a retaliatory attack and the potential backlash this might cause from Russia.

Gillian M. Christensen, deputy press secretary for the Department of Homeland Security, said the agency was investigating "all potential causes" of the attack.

Vice President Joseph R. Biden Jr. said on the NBC News program "Meet the Press" this month that the United States was prepared to respond to Russia's election attacks in kind. "We're sending a message," Mr. Biden said. "We have the capacity to do it."

But technology providers in the United States could suffer blowback. As Dyn fell under recurring attacks on Friday, Mr. York, the chief strategist, said such assaults were the reason so many companies are pushing at least parts of their infrastructure to cloud computing networks, to decentralize their systems and make them harder to attack.

"It's a total wild, wild west out there," Mr. York said.

Le Soleil
Le monde à la merci des hackers?
Saturday, 22 October 2016
Byline: Jean-François Cliché

Ottawa - Mine de rien, il y a pas mal de pirates informatiques qui ont ajouté de très, très gros trophées de chasse à leur collection récemment...
Les courriels de Hillary Clinton. Ceux du directeur de la CIA, John Brennan, l'an dernier. Cet été, un serveur du Comité national du Parti démocrate a été complètement éventé. Il y a deux semaines, ce fut au tour du directeur de campagne de Mme Clinton, John Podesta, de voir sa correspondance électronique atterrir sur le site WikiLeaks. Quand on pense aux secrets d'État que des gens si hauts placés peuvent échanger, la liste a quelque chose de totalement irréel.

Mais comment cela est-il possible? Comment l'entourage immédiat d'une potentielle présidente des États-Unis et le patron de l'espionnage américain peuvent-ils être à ce point vulnérables? Sont-ils mal conseillés, négligents, ou les pirates sont-ils tout simplement impossibles à arrêter?

Il y a sans doute un peu des deux, disent tous les experts auxquels Le Soleil a soumis la question. «La plus grande vulnérabilité de tout système d'information, c'est toujours le facteur humain, que ce soit accidentel ou volontaire», dit Marc-André Léger, qui enseigne la sécurité informatique à l'Université de Sherbrooke.

Ainsi, il a été démontré que Mme Clinton avait utilisé un compte personnel et un serveur privé et fort mal sécurisé à sa résidence lorsqu'elle était secrétaire d'État afin d'envoyer ses courriels, dont certains contenaient des documents sensibles. Les règles du gouvernement stipulent pourtant que seuls des serveurs gouvernementaux et dûment sécurisés peuvent être utilisés. Mais il a aussi été révélé en début d'année que beaucoup de hauts placés américains, tant dans le gouvernement Obama que dans l'administration républicaine précédente, ont des comportements semblables.

Mais il n'y a pas que des erreurs humaines dans ces histoires de piratage, poursuit M. Léger, «un ordinateur impossible à hacker, ça n'existe pas. [...] Tout ordinateur branché à Internet peut être piraté. C'est une question de mettre l'énergie et le temps qu'il faut pour entrer dans le système».

En conjuguant technique et faiblesse humaine, les «trous» potentiels qu'un pirate peut exploiter sont pratiquement innombrables, dit-il. Même aux plus hauts niveaux du pouvoir.

Comme de la magie

«C'est comme les tours d'un magicien : quand on les voit, c'est très impressionnant, puis quand on comprend le truc, on se dit : "Ah, c'était juste ça." C'est pareil quand on fait le post-mortem [d'une intrusion informatique] et qu'on regarde les brèches. C'est rarement très compliqué. Habituellement, c'est au contraire quelque chose de vraiment simple, et on se dit après coup : "Wow, c'était vraiment stupide"», explique Éric Parent, qui possède la boîte de sécurité informatique LogicNet et qui donne des cours dans ce domaine à l'École polytechnique de Montréal.

Les brèches peuvent être de toutes les sortes. «En théorie, c'est vrai que ça prend un mot de passe pour avoir accès à un serveur. Mais en pratique, ça dépend. Peut-être que le mot de passe de l'administrateur est très facile à deviner, on peut utiliser un outil qui va, par exemple, essayer tous les mots du dictionnaire et éventuellement le trouver», dit M. Léger.

Et s'il est vrai que beaucoup de machines bloquent l'accès à un ordinateur après trois essais ratés, un pirate organisé et déterminé peut avoir déjà pris le contrôle de milliers d'ordinateurs personnels et les faire essayer chacun trois clés différentes, signale Patrick Mathieu, consultant en sécurité informatique et organisateur du HackFest, gros congrès (et concours) sur le piratage qui a lieu à Québec chaque année.

«Écouter» le Wi-Fi

En outre, la multiplication des instruments Wi-Fi a ouvert de nouvelles portes pour les pirates parce qu'ils sont très faciles à «écouter», disent nos trois experts.

«Il y a des logiciels gratuits qui sont faits pour analyser ce qui se passe sur le réseau d'une entreprise et qui vont écouter tout ce qui se "dit" dans un réseau Wi-Fi. Mais bien sûr, ça peut être utilisé de façon malicieuse», dit M. Mathieu.

Souvent, dit-il, les réseaux sans fil offerts dans les cafés et les restaurants ne sont pas sécurisés - la connexion entre le routeur et chaque client n'est pas encryptée. N'importe qui peut donc «écouter» ce que font les clients de l'endroit sur Internet, pourvu d'être sur place (le Wi- Fi ne se rend pas loin). Si l'un d'eux se sert de ce réseau pour accéder à son courriel, son mot de passe peut alors être «entendu». Et comme peu de gens ont l'habitude d'utiliser plusieurs mots de passe différents...

On ne saura sans doute jamais comment tous ces courriels de proches de Mme Clinton ont été piratés, mais cela peut être aussi «nono» qu'un resto proche de bureaux du Parti démocrate dont le sans-fil est mal sécurisé...

Et quand les failles techniques sont trop étroites ou trop longues à exploiter, les pirates peuvent toujours se rabattre sur le «facteur humain», comme dit M. Léger, que le milieu du piratage appelle pudiquement l'«ingénierie sociale». «C'est un des moyens les plus utilisés, dit M. Mathieu. Ça peut être d'envoyer des e-mails qui incitent à cliquer sur un lien [un logiciel malicieux s'installe alors et «vole» les mots de passe] ou d'autre chose. Dans les tests en entreprise que je fais, quand on ne réussit pas à trouver une faille informatique dans un temps donné, il suffit souvent d'un coup de téléphone, et le tour est joué. Ça peut être aussi simple que ça. Ça ne marche pas à toutes les fois, mais j'ai vu des tests en entreprise où on obtenait des taux de réussite de 100 % [pour obtenir des informations permettant à un pirate informatique d'entrer dans le système] sur des dizaines de personnes. Des fois, c'est juste 50 %, mais ce n'est jamais zéro, malheureusement. L'humain est fait pour faire confiance. Tu dis que tu travailles au soutien informatique et si ton histoire fait du sens dans le contexte de cette entreprise-là, généralement, la personne va te donner son mot de passe.»

Et quand on multiplie tout cela par le nombre de personnes qu'il y a dans l'entourage d'un chef d'État, ceux des ministres et les hauts fonctionnaires, on arrive à la même conclusion que M. Parent : «C'est impossible d'éliminer tous ces risques-là.» La seule chose que l'on peut faire, dit-il avec M. Mathieu, c'est d'allonger suffisamment le travail des pirates pour qu'ils choisissent d'autres victimes...

La Presse
WikiLeaks est-il à la solde du Kremlin ?
Saturday, 22 October 2016

Byline: Marc Thibodeau

Analyse: À en croire l'entourage de la candidate démocrate à l'élection présidentielle américaine, l'affaire ne fait aucun doute: WikiLeaks tente, de concert avec le Kremlin, de déstabiliser la campagne de Hillary Clinton afin de favoriser l'élection de son rival républicain, Donald Trump.
Le porte-parole de l'ex-secrétaire d'État, Brian Fallon, s'en est pris directement à l'organisation de Julian Assange la semaine dernière en tweetant qu'elle se comportait en «outil de propagande du gouvernement russe» visant à favoriser la «marionnette» de Moscou.

«Le fait de distiller des mensonges n'améliore en rien votre crédibilité», a rétorqué en ligne un responsable non identifié du compte Twitter de WikiLeaks.

Au coeur du litige figure une série de courriels publiés par WikiLeaks au cours des derniers mois. Un premier lot témoignant de comportements hostiles de la direction du Parti démocrate envers le sénateur Bernie Sanders, qui était opposé à Mme Clinton, a d'abord été dévoilé en juillet à la veille de la convention de la formation.

Des courriels tirés du compte du directeur de campagne de la femme politique, John Podesta, ont ensuite été mis en ligne progressivement sur une période de dix jours dans la période précédant le troisième débat.

Dans un avis publié le 7 octobre, le département de la Sécurité intérieure des États-Unis s'est dit «raisonnablement certain» (confident) que la Russie était «directement responsable» des cyberattaques prenant pour cible le camp démocrate. Ses responsables ont ajouté que la divulgation de courriels piratés par l'entremise de WikiLeaks et d'autres sites comme DCLeaks.com était conforme aux «méthodes et motivations» de Moscou et visait à déstabiliser l'élection américaine.

Le communiqué ne disait cependant rien de la nature exacte des liens entre Moscou et WikiLeaks, contrairement à ce que pouvaient laisser entendre les interventions du camp démocrate à ce sujet.

Collaboration

Arun Vishwanath, spécialiste de cybersécurité rattaché à l'Université de Buffalo, note qu'il est possible, en étudiant la méthode utilisée par les hackers, de déterminer avec une assurance raisonnable la provenance des attaques ciblant le camp démocrate.

L'éventualité d'une action russe n'explique pas la nature de la collaboration entre WikiLeaks et Moscou, si collaboration il y a, relève le spécialiste, qui s'étonne malgré tout de la stratégie de diffusion des courriels suivie par l'organisation.

Il apparaît clairement, dit-il, que Julian Assange cherche actuellement à «faire de la politique» en ciblant un seul des camps dans la campagne présidentielle.

«Initialement, WikiLeaks se donnait pour mandat de surveiller les gouvernements. Là, ils surveillent le comportement d'un parti plutôt que d'un autre», relève l'analyste.

«Sont- ils utilisés à leur insu, ou agissent-ils en toute connaissance de cause? Je ne le sais pas. Ce qui est clair, c'est qu'ils sont devenus une courroie de transmission pour les informations piratées de toute nature», ajoute M. Vishwanath.

Neil Sroka, porte-parole de Democracy for America, organisation qui soutient la candidate démocrate, estime que WikiLeaks se comporte manifestement comme un «agent» de la campagne de Donald Trump, quelle que soit la nature de ses liens avec la Russie.

La diffusion des courriels à des moments-clés vise à susciter un maximum de «chaos», juge M. Sroka, qui fait peu de cas de la teneur des courriels diffusés. «Ce ne sont pas les Pentagon Papers [sur l'implication des États-Unis dans la guerre du Viêtnam] dont on parle ici», estime-t-il.

Pas de préférence?

WikiLeaks fait valoir de son côté qu'elle agit de manière désintéressée et ne cherche pas à favoriser un camp ou l'autre, encore moins à favoriser les visées de Moscou. Une éditrice, Sarah Harrison, a déclaré à Bloomberg que l'organisation n'hésiterait pas un instant à diffuser des documents nuisibles à Donald Trump si elle en avait.

Julian Assange, qui a déjà animé une émission sur Russia Today, chaîne contrôlée par Moscou, ne cache pas pour autant qu'il a maille à partir avec Hillary Clinton. L'ex-secrétaire d'État, a-t-il déclaré récemment, veut le faire incriminer relativement à une importante fuite de documents diplomatiques qui avait embarrassé les États-Unis il y a quelques années.

L'activiste lui reproche par ailleurs son côté «va-t-en-guerre». «Elle ne devrait pas pouvoir s'approcher d'un armurier, encore moins d'une armée. Et elle ne devrait certainement pas pouvoir devenir présidente des États-Unis», écrivait-il en février 2016.

Le directeur de Freedom of the Press Foundation, Trevor Timm, qui recueille notamment des dons pour WikiLeaks, relève dans une chronique parue la semaine dernière que les démocrates s'indignent des fuites les concernant en les qualifiant d'«illégales» tout en encourageant celles qui ciblent Donald Trump.

Le rôle éventuel de Moscou dans les fuites mérite d'être exploré par les médias, dit-il. Mais «concocter des théories conspirationnistes de collusion Poutine-Trump-WikiLeaks et faire de grands bonds logiques sans preuve directe [...] dessert le journalisme», prévient-il.

The Daily Beast
How Surveillance Cameras Have Become an Internet Superweapon
Sunday, 23 October 2016
Byline: Robert Graham

Analysis: On Friday, hackers crashed parts of the Internet, specifically services located on the East Coast of the United States. They used an old technique known for 20 years, a "DNS DDoS."
However, instead of launching the attack from virus-infected computers as has been the norm, hackers launched the attack from small, Internet-connected devices like security cameras. This is a worrisome development--such devices offer hackers a powerful new weapon.

The "Internet-of-Things" (IoT) revolution is sweeping the Internet, adding cars, pace makers, industrial robots, toasters, and security cameras to the Internet. If you own an appliance or device that uses electricity, you can find a similar device which connects to the Internet. Through a voice-activated device such as an Amazon Echo, you can command the coffee to start brewing, the car to start warming, and the lights to turn on in the morning--all before getting out of bed. According to research group Gartner, more than 6 billion of these devices will be on the Internet by the end of 2016.

This trend comes at the cost of cybersecurity. They are cheap devices that cut corners. While they are not prone to the same attacks as your home computers (such as phishing emails), they have other common problems (like backdoor passwords). These are passwords, like "support", that vendors put secretly in their devices for various reasons. While vendors think they are clever and secretive, hackers find these passwords effortlessly. They create lists of these well-known backdoors and trade them among themselves.

Luckily, the devices installed in your home are behind your firewall, so they are secure against most hacker attacks. A firewall is a common security device that allows outbound communication with the Internet, but blocks most inbound communication. Most of the devices that connect homes to the Internet contain a firewall. However, many more are placed directly on the Internet, where hackers can easily gain control of them.

That's why in the Friday's attacks, most of the devices were security cameras rather than baby monitors. Both devices do the same thing, record video, and often have the same internal hardware and software inside. However, baby monitors are usually installed in the home, behind firewalls, which hackers cannot directly access. Security cameras are installed in remote buildings, often with dedicated Internet connection just for the camera, with no firewall protection. However, some baby monitors were placed outside the firewall.

Most assume it would be too hard to find such devices on the Internet. For example, some remote village in Mongolia might have security cameras attached to a satellite uplink. What's the chance hackers can find that?

The answer is 100%. In much the same way that you need only somebody's phone number to call them, all you need is an Internet address to connect to a device. When you dial somebody's phone number, the fact they might be located in downtown Berlin or the middle of Mongolia is irrelevant. The same is true of an Internet address. There are fewer Internet addresses than phone numbers, only about 4 billion possible combinations. It's possible to try them all in the span of a few hours.

The following picture shows me running a tool called masscan, which probes every possible Internet address. As you can see, in about 6 hours, it will have scanned the entire Internet for all IoT devices of the sort that were used on Friday. It sends a probe to each and every address on the Internet, regardless where they are physically located. If you look carefully on your home firewall, you'll see that somebody with the Internet address 209.126.230.72 has tried to contact you today. That person was me. And this is true, even if you are living in the middle of Mongolia.

Mirai scans the Internet. When it finds targets, it attempts to login using many well-known backdoor

Once Mirai finds an infects a new device, it then contacts the hacker controlling these devise. It has now become a botnet under the hacker's control. One common command is to execute a DDoS attack. This stands for Distributed Denial of Service. It comes from thousands of devices, the source distributed across all these devices. The term "denial of service" is an old computer term meaning to either crash, slow down, or otherwise "deny" people the "service" of the targeted device.

The hacker (or hackers) behind Mirai have been building their botnet for a couple months. We've seen the scans on the Internet. And on Friday morning, they commanded the machines to target a victim, a major DNS provider. DNS is the phonebook of the Internet, translating between human names and the sequence of numbers that is an Internet address. When DNS crashes, the Internet technically runs, but anybody dependent on that DNS service can no longer find things. The victim of the attack, Dyn.com, was a particularly large DNS provider, and hence, the attack had a disproportionate effect on the Internet.

The scariest part of Friday's attack is that it takes no special skill. Anybody can use masscan or Shodan to find potentially vulnerable systems. Anybody can infect those systems with Mirai and remotely control them. Some have suggested that nation states are behind this attack - but so far we've seen nothing sophisticated, nothing requiring nation state resources. All this is within the abilities of a particularly nerdy teenager working out of her mother's basement.

When people open the box for the first time, they see an innocent looking device. They connect it to their network with that impression. But the Internet doesn't see them as devices. The Internet sees them as full computers, running the latest Windows or Linux software, with large amounts of memory and computer power, attached to fast Internet links. Hackers are now exploiting this disjuncture, taking control of devices, and using them to crash the Internet, and there is nothing you can do about it.

Le Monde
Le Conseil constitutionnel dit non à la surveillance de masse sans contrôle
Saturday, 22 October 2016
Byline: Jean-Baptiste Jacquin

Paris - C'est un petit article de loi en vigueur depuis vingt-cinq ans que le Conseil constitutionnel a censuré dans une décision rendue vendredi 21 octobre. Cet article permettait tout bonnement aux services de renseignement de procéder sans le moindre contrôle à la surveillance de communications par voie hertzienne. Les gardiens de la Constitution le déclarent contraire à l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 en portant « une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances . Ils le déclarent inconstitutionnel et demandent au législateur d'élaborer un nouveau texte d'ici au 31 décembre 2017.
Au nom de « la défense des intérêts nationaux » , les pouvoirs publics pouvaient ainsi surveiller les déplacements de sous-marins étrangers ou les mouvements de troupes sur un théâtre d'opération, mais également des communications par téléphone mobile entre particuliers, des échanges par Wi-Fi ou Bluetooth. Rebaptisé article L. 811-5 dans la loi renseignement de juillet 2015, cet article permettait aux services de renseignement de s'affranchir des contrôles que cette loi imposait, en précisant, par exemple, que la surveillance de particuliers ne peut être autorisée par le premier ministre qu'après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR).

« Un trou législatif béant »

C'est en invoquant cette disposition particulièrement floue que Bernard Squarcini, l'ancien patron de la Direction centrale du renseignement intérieur (DCRI), avait pris la liberté de procéder à des écoutes dans l'affaire des fadettes du Monde . Lors du débat sur la loi renseignement de 2015, quelques mois après les attentats contre Charlie Hebdo et l'Hyper Cacher, personne ne semblait s'être intéressé à cet article introduit par la loi de 1991 sur le secret des correspondances. Cette dernière avait elle-même été votée après le scandale des écoutes de l'Elysée où François Mitterrand avait fait écouter des personnalités, dont le journaliste du Monde Edwy Plenel.

Le Conseil constitutionnel s'était prononcé en juillet 2015 sur la loi renseignement, en censurant d'ailleurs deux dispositions, mais n'avait validé que les articles qui lui avaient été soulignés dans les saisines du président de la République et du président du Sénat. Il ne s'était jamais saisi de ce sujet avant la question prioritaire de constitutionnalité déposée au printemps par des associations (Quadrature du Net, French Data Network, la Fédération des fournisseurs d'accès à Internet associatifs et Igwan.net). Selon leur avocat, Patrice Spinosi, il a créé « un trou législatif béant » et « ouvre la voie à un espionnage de masse » , a-t-il expliqué à l'audience du 11 octobre

L'article, très court, dit : « Les mesures prises par les pouvoirs publics pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne ne sont pas soumises aux dispositions du présent livre, ni à celles de la sous-section 2 de la section 3 du chapitre Ier du titre III du livre Ier du code de procédure pénale. » Dans sa décision, le

Conseil constitutionnel note que la disposition contestée permettait de fait de s'affranchir du code de procédure pénale qui encadre les écoutes ordonnées par un juge d'instruction.

Balayant les observations du gouvernement et reprenant les arguments des associations, l'institution présidée par Laurent Fabius souligne que la rédaction du texte incriminé n'interdit pas des mesures de surveillance « utilisées à des fins plus larges que la seule mise en oeuvre de » la défense des intérêts nationaux. Surtout, écrit-elle, le recours à ces mesures n'est soumis « à aucune condition de fond ni de procédure » et leur mise en oeuvre n'est encadrée « d'aucune garantie » . Aucune limite sur l'exploitation des données personnelles ni leur conservation n'était prévue...

Pour ne pas empêcher les services de renseignement de continuer à opérer des écoutes qui relèveraient réellement de la défense nationale, le Conseil n'abroge pas la loi mais encadre sérieusement son application. En attendant qu'un nouveau texte de loi soit voté, il impose deux « réserves transitoires . Les mesures de surveillance ne pourront pas s'appliquer aux écoutes soumises à autorisation par la loi renseignement, et la CNCTR devra être « régulièrement informée » des opérations mises en oeuvre. La nouvelle législature qui sortira des urnes en juin aura quelques mois pour faire le tri entre ce qui relève des surveillances susceptibles de porter atteinte à la vie privée et les autres.

Yonhap News Agency
N.K. committed to staging cyberwarfare against S. Korea: source
Monday, 24 October 2016
Byline: Staff reporter

Seoul -North Korea is fully committed to staging cyberwarfare against South Korea by operating special teams that conduct hacking attacks and spread false information in a bid to fuel anti-Seoul propaganda, a source said Monday.
"North Korea has been engrossed in cyberwarfare operations with its reconnaissance bureau, the ruling party's department dealing with South Korea, and an operator of propaganda websites leading such campaigns," according to the source familiar with the reclusive country.

The special teams are tasked with filing pro-Pyongyang messages on South Korean websites and spreading lies through social media, he said.

The North's move comes as North Korean leader Kim Jong-un said in August 2013 that building cyberwarfare capabilities is a powerful tool in advancing the military's ability to stage strikes.

At a meeting with ideological workers held in February 2014, Kim called for measures to make the Internet a venue for North Korea's propaganda campaign, according to Pyongyang's state media.

Experts said that the North's propaganda websites are focusing on driving a wedge among South Koreans by highlighting sensitive issues such as a mass defection by North Korean restaurant workers in China and Seoul's latest decision to install an advanced U.S. missile defense system.

North Korea has claimed that a group of 13 North Korean restaurant staff had been tricked into defecting and were kidnapped by South Korea's spy agency. Seoul rejected it, saying that they came to Seoul of their own free will.

North Korea has been long accused of waging cyberwarfare, including a hacking attack on South Korea and even against U.S. companies.

In March 2013, North Korea carried out a massive cyberattack on South Korean financial firms and TV broadcasters, causing their networks to crash.

In late 2014, the U.S. accused Pyongyang of staging cyberattacks on Sony Pictures, which released "The Interview," a fictional movie about assassinating the North's current leader.

Korea Herald
'NK operates team for online propaganda in S. Korea'
Monday, 24 October 2016

Seoul -North Korea is assessed to be operating a team to conduct cyber "psychological warfare" in South Korea by spreading rumors favorable to Pyongyang, a government source said Monday.
According to the source, the North's cyber team on South Korea mainly focuses on hacking attacks to incapacitate Seoul's infrastructure and it also distributes fake information to manipulate public opinion here.

"North Korea's organizations on the South, including the General Bureau of Reconnaissance, have been identified as operating an 'online reply team' that spreads malicious tales and groundless rumors on the internet and social network services," an official told local media.

stock image(123rf)He said North Koreans are believed to also directly post pro-Pyongyang content on the internet.

A case of one such malicious rumor, according to the source, was a claim that the mass defection of China-based North Korean restaurant workers was a result of Seoul kidnapping them. These rumors also claimed that the workers have gone on a hunger strike in protest of the Seoul government.

North Korea is believed to be operating around 60 propaganda websites.

Pundits said these rumors are an inexpensive and effective way of spreading pro-North sentiment while undermining the South Korean government. Some call for extreme measures, such as a direct crackdown on the media and people.

Lee Sang-ho, a political science professor from Daejeon University, said the North is attempting to raise doubts on South Korean policymakers through these methods.

"By attacking the credibility of a country's leader and policymakers, nullifying their leadership and dividing public opinion, they can make people distrust each other. This is enough to threaten the very existence of that country," he said in his report titled &ldquo

China Daily
FM: Prevent internet use by terrorists
Monday, 24 October 2016
Byline: Wang Qingyun

Beijing - Countries should resolutely work together to prevent terrorists from taking advantage of the internet, a major tool responsible for the dramatic increase in terrorism, Foreign Minister Wang Yi said in Beijing on Friday.
Surveys show that most of those who carried out attacks in China had been "seduced and incited" by terrorist audio or video clips online, Wang said, adding that countries should focus more on this phenomenon.

Wang made the remarks during a symposium on countering terrorists' use of the internet that was hosted by the Foreign Ministry under the framework of the Global Counterterrorism Forum, a body of 29 countries and the European Union.

The symposium attracted about 180 participants, including officials representing forum members, plus scholars and representatives from internet companies. It was the ministry's second time hosting the symposium.

Wang said terrorist forces of the East Turkestan Islamic Movement have conducted a number of attacks both inside and outside China. According to a documentary by the Cyberspace Administration of China, the extremists released 73 terrorist audio and video clips in the first six months of 2014. In 2013, they released 109 - triple the previous year.

Terrorist organizations are abusing the development of information technology to spread violence and extremist thought, and this "has broken through country and regional borders and activated dormant terrorist groups scattered in various places", Wang said, adding that countries needed to widen their consensus and cooperate more in the fight.

He also called for the development of expertise and technology to tackle the spread of extremism through online channels. The international community should continue providing funds and training for developing countries to help them improve their counterterrorism measures and internet security, he said.

Zhang Jiadong, a researcher at Fudan University's Center for American Studies, said the internet is even used to offer training for atrocities.

Also, social media, "a private space" online, poses a "grave challenge" for efforts to contain terrorism, Zhang said, because it can evade monitoring.

Mei Jianming, a professor of the People's Public Security University of China, said preventing terrorists from taking advantage of the internet while guaranteeing that people can enjoy fully the convenience brought by the modern technology is an issue that needs to be addressed when tackling terrorism.

Reuters
British lawmakers ask Obama to let hacking suspect face trial in UK
Monday, 24 October 2016
Byline: Staff report

London - A group of 105 British members of parliament (MPs) have asked President Barack Obama to withdraw a warrant for the extradition of an autistic Briton who is accused of hacking high-security U.S. state computers.
Lauri Love, 31, who has Asperger's syndrome, is accused of involvement in a series of hacks in 2012 and 2013 into computers at agencies including the Federal Bureau of Investigation, the U.S. army, the Missile Defense Agency and the Federal Reserve.

A London court approved his extradition in September despite warnings from his family, lawyers and supporters that he would be at risk of killing himself if sentenced to a lifetime in a U.S. prison.

In a letter to Obama, the 105 MPs from the ruling Conservative Party, the main opposition Labour Party and several other parties said they were deeply concerned about the case.

"Mr Love should face prosecution for any crimes committed in his own country where his suicide risk is exponentially reduced," the lawmakers wrote, according to a copy of the letter sent to media on Monday.

"We urge you to carry out an act of compassion in your final days as President by withdrawing Mr Love's extradition warrant."

U.S. authorities say Love was connected to Anonymous, an international group of hackers, and that his actions had caused millions of dollars' worth of damage.

The MPs argued in their letter that he should face any charges in Britain, pointing to new rules that make it easier for British courts to try people for crimes committed there but involving other countries.

They said Britain had prosecuted at least 12 people accused of hacking U.S.-based computer systems.

"Why then is the United States insistent on Mr Love's extradition despite the UK having a proven track record of appropriately sentencing and rehabilitating individuals who have committed computer hacking offences against the U.S.?" they asked.

The MPs said Love had a long history of serious mental health issues including depression and episodes of psychosis, and that he also suffered from anxiety-induced eczema that was resistant to antibiotics and very hard to manage.

"Consequently, there is significant concern that Mr Love's physical and mental well-being would deteriorate and become unmanageable if he were extradited," the MPs wrote, adding that they had "no doubt in mind" that he would be at high risk of suicide.

Fars News Agency
Iran Confirms Finding US Electronic Implants in Infrastructures
Tuesday, 25 October 2016

Tehran - Head of Iran's Civil Defense Organization Brigadier General Gholam Reza Jalali confirmed on Monday that security forces have found electronic implants in the country's infrastructures that had been placed by the US for sabotage and espionage.
"The Americans have placed implants in Iran's infrastructures with sabotage and data wiring and espionage capabilities, and we have discovered a number of them," Jalali told reporters in Tehran on Monday.

"We classified Iran's infrastructures into several groups, including power, energy, communications, oil and media and examined them, and we discovered some of them (the US implants) in certain infrastructures," he added.

Asked about Iran's plans to produce highly secure smart phones for the country's officials, Jalali said that the officials whose whereabouts are of vital importance and any information about their location could be used against them are not allowed to use smart phones.

"We have worked out some capabilities for other officials too to protect and immunize their cell phones," he said.

His remarks alluded to the New York Times' February report saying that in the early years of the Obama administration, the United States had developed an elaborate plan for a cyber attack on Iran in case the diplomatic effort to limit its nuclear program failed and led to a military conflict.

The plan, code-named Nitro Zeus, was devised to disable Iran's air defenses, communications systems and crucial parts of its power grid, and was shelved, at least for the foreseeable future, after the nuclear deal struck between Iran and six other nations was fulfilled.

At its height, the US officials said, the planning for Nitro Zeus involved thousands of American military and intelligence personnel, spending tens of millions of dollars and placing electronic implants in Iranian computer networks to "prepare the battlefield," in the parlance of the Pentagon, New York Times reported.

Tehran Times
U.S. to launch cyber war on Iran if Israel enters war with Iran
Tuesday, 25 October 2016

Tehran - The commander of Iran's Passive Defense Organization said on Monday that Washington will launch cyber-attacks on Iran's infrastructural facilities in the event of a war breaks out between Iran and the Israeli regime.
Brigadier General Gholam Reza Jalali made the remarks in a ceremony marking Passive Defense Week.
"The Americans had orchestrated two plans to infiltrate the country's infrastructures," Jalali said.

"The first possible plan would have gone into effect if nuclear negotiations with the 5+1 group had failed, and the other one will be carried out if Iran and the Israeli regime go to war," he opined.

Elsewhere in his remarks, Jalali underlined the valuable role that the Ministry of Communications and Information Technology could play in defending the country's cyber assets. "This role of the communication ministry is so important that we might call it the cyber defense ministry," he remarked.

The commander noted that the country needs to upgrade its communication infrastructure, saying, "We must employ specific strategies in this regard."

General Jalali also said the U.S. has specific plans for different levels of cyberspace, arguing that Iran must also strengthen its capabilities in this field. He called for the expansion of Iran's National Information Network, which was launched back in August after an 11-year delay.

Lebanon Daily Star
Banks becoming more vigilant on cybercrime
Tuesday, 25 October 2016
Byline: Staff Report

Beirut - The head of the Special Investigation Commission said Monday that Lebanese banks were already taking extraordinary measures to check the rise of cybercrime in Lebanon.
"The number of executed and nonexecuted financial embezzlement through cybercrime in 2016 reached 137 operations. Eighty-six were executed successfully (or 60 percent of the total operations) and this caused a loss of $2.9 million. But out of the executed $2.9 million, banks were able to retrieve $740,000, or 25 percent of the embezzled money," Abdul-Hafiz Mansour told a workshop on cybercrime.

He added that there were 51 aborted attempts to embezzle money through banks, after clients and lenders realized there was something suspicious about the requests.

Cybercrime has become a serious phenomenon in Lebanon over the past few years. The Lebanese financial authorities have called on all commercial banks to carefully double check all online financial transactions in order to protect their customers.

Mansour warned that embezzled money can be transferred through different countries in less than 24 hours, and that in many occasions it becomes impossible to trace or retrieve the money because the individuals who are behind the scheme are anonymous.

Last year, Mansour revealed that this phenomenon had increased to 84 cases in 2015 from 51 in 2014, estimating the total value of these illegal practices at $12 million in the previous year alone.

Mansour advised that the best way to avoid such crimes was to take precautionary measures, as it is very hard to recover stolen funds.

"We are dealing with a virtual world when it comes to cybercrimes, and this is why the best way to prevent the occurrence of such incidents, whether by the banks or clients, is by taking precautionary measures," he said last year.

He added that the first step toward confronting cybercrime was to provide legal and legislative measures and to raise awareness among all banks and financial institutions about this type of crime.

Toronto Star
Hackers blamed for causing Grade 10 literacy test chaos
Tuesday, 25 October 2016
Byline: Kristin Rushowy

Toronto - Ontario's education testing agency has called Toronto police about an "intentional, malicious and sustained" cyberattack that shut down the Grade 10 literacy exam across the province - a targeted strike carried out by hackers who may never be found.
The technical troubles, in what's called a sustained distributed denial of service (DDoS), affected almost 150,000 students across the province and sabotaged a $250,000 pilot project to move the test online. Although the source of the attack is not yet known and the testing agency says it may never be uncovered, one or more people could be behind it - possibly even teenagers, say cyber experts.

"I'm not sure if this kind of thing can ever be figured out," said Richard Jones, director of assessment for the Education Quality and Accountability Office, or EQAO. "There were IP addresses from all over the world, and to find the source is a really difficult thing. We are moving forward and trying to uncover as much information as we can."

The EQAO "should have foreseen this type of scenario," said cybersecurity lawyer Imran Ahmad, because such attacks are increasingly common.

A cyberattack last week that hit Twitter and Netflix, among others, is so far unconnected to the EQAO's troubles.

"This should not come as a surprise; any kind of online interface is inherently vulnerable," said Ahmad, adding the EQAO should have hired a third party solely to filter out "bad" traffic that clogs sites in such strikes.

"I would not be surprised if a teenager was behind it," added Ahmad, of Miller Thomson LLP. "The skill set among the younger generation is extremely advanced."

At the EQAO, last Thursday began with good news, Jones said, after officials learned an Ontario-run school in Egypt had completed the online test "with no issues ... they did the assessment well prior to 8 a.m. Canadian time.

"And then at 8 a.m. our time, there was a huge influx of junk traffic from IP addresses from all around the world, inundating our host application for the assessment ... As far as I'm concerned, they were absolutely targeting us. Somebody knew the timing and somebody knew the IP addresses to attack."

Despite the four hours of technical troubles that followed - where at the worst, 99 per cent of traffic was not from schools or boards - it appears almost 16,000 teens in Ontario managed to complete the test. The EQAO is now debating whether to give them credit if they were successful.

IT experts and a third-party forensic team spent the weekend trying to figure out what happened and Jones said they will "eventually be able to provide us with some advice" on how to prevent such a strike in the future.

"This was not the trial online that we expected - we are getting a trial all right," Jones said. Five prior field tests led to some minor tweaking, but found no major issues and "load" testing showed the system could handle the equivalent of 250,000 students as well as up to 10,000 teacher supervisors.

"This type of attack was so intense and so sustained that the system was not able to handle it," Jones said, adding the investigation will look at the EQAO's system, as well as their service provider's.

Jones assured that student privacy was "not breached in any way ... They were basically clogging the system so students weren't able to get into it."

But even if information was not stolen, Ahmad said, "I'm pretty sure there's a financial cost to this at some level," as well as the number of work hours of preparation, now wasted. "They'll have to go back to the drawing board and it's very difficult to layer on security after the fact."

Ahmad also wondered if the EQAO had been on the lookout for "probing" in the weeks prior, which is akin to hackers testing the system ahead of time.

"Somebody must have done their homework," he said. "You don't just launch an attack and assume it will be successful."

At Queen's Park, Education Minister Mitzie Hunter said, "It is extremely disappointing that this deliberate and manipulative attack, this malicious attack, has happened and prevented our students from completing the test as planned."

A new version of the literacy test, which teens must pass in order to graduate, will be offered online in March to all Grade 10 students. A paper-and-pen version will also be available. Hunter said she's confident the move online will go ahead.

MIT Technology Review
The Decline in Chinese Cyberattacks: The Story Behind the Numbers
Tuesday, 25 October 2016
Byline: Mara Hvistendahl

Cambridge, Mass. - Last summer, an audience of government officials, military personnel, and foreign ambassadors gathered in Aspen, Colorado, to hear John Carlin, then an assistant attorney general, speak about cyberattacks. The Aspen Security Forum, which is held every year at a breathtaking resort in the Rocky Mountains, is the sort of event where national security wonks go for hikes in T-shirts and shorts, then trade war stories over lemon-raspberry water and superfood balls. The news of the Democratic National Committee hack had broken just the day before, and many hoped that Carlin, who headed up the investigation into the incident, might speak candidly about it. Instead, he recounted the Justice Department's indictment of five hackers in China's People's Liberation Army Unit 61398 for commercial espionage--back in 2014.
A boyish Harvard-trained former prosecutor, Carlin oversaw the department's efforts to stamp out economic espionage before stepping down earlier this month. In June, the cybersecurity firm FireEye released a report describing a significant decrease since early 2013 in the number of commercial attacks from China, which is the largest source of such attacks. The firm charted attacks on clients around the world by 72 groups that are either based in China or believed to represent Chinese state interests. Beginning in mid-2014, its analysts observed a "noticeable decline" in activity. Intelligence officials have quietly echoed that claim.

For some in the Obama administration, this is proof that using both carrots and sticks to combat Chinese theft of intellectual property--what Carlin called an "all-tools" approach--is working. Indictments and so-called "naming and shaming" have been accompanied by economic sanctions and diplomatic efforts, including a September 2015 agreement between President Obama and Xi Jinping to refrain from conducting or supporting cyber-theft of intellectual property. "This approach is a giant 'No trespassing' sign," Carlin said. "It's 'Get off our lawn.'"

But others are not sure the U.S. government should get so much credit. The perceived decline in attacks from China raises a question: why? Former government officials and cybersecurity experts now offer up a range of theories--including a provocative one that questions the extent to which straight commercial

cyber-espionage, as opposed to the more targeted spying on military technologies and capabilities that many nations engage in, was ever a priority of the Chinese central government in the first place.

There is little doubt that the Chinese government invests substantial energy in stealing everything from plans for U.S. fighter jets to the 22 million records kept by the Office of Personnel Management, or that it has done little to pursue commercial spies. But some of the more commercially focused attacks carried out by Unit 61398, this theory holds, may have been illusions, while others may never have had explicit backing from Beijing to begin with.

In 2013, former FBI director Robert Mueller called for a broad effort to root out cyber-threats and seek the "warm body behind the keyboard." Speaking at the Brookings Institution the day after the Unit 61398 indictment was unveiled, Carlin said that the bureau had succeeded in "putting a face" on that warm body--or rather, on five of them. The mug shots of these men, who went by monikers like KandyGoo and UglyGorilla, were splashed across posters that read: Wanted by the FBI.

The indictment marked a break with the standard diplomatic practice of not subjecting active military officials of other countries to criminal prosecution, and many in Washington greeted it with skepticism. Some doubted whether the charges would be actionable, while others pointed out that the Justice Department's stance on commercial espionage--that collecting general economic intelligence is routine statecraft and therefore acceptable, while spying for the benefit of specific companies is not--is a distinction few other countries would recognize. Benjamin Wittes, a senior fellow at Brookings, even wondered whether the Justice Department's move might be simply "a very sophisticated form of legal PR."

Doubt continued in September 2015, after the announcement of the China-U.S. agreement. Some believed that Xi's commitment to refrain from supporting commercial hacking was little more than lip service. Director of National Intelligence James Clapper told Defense News at the time, "I personally am somewhat of a skeptic."

But as time went on, cybersecurity analysts noticed a curious change. For its recent report, FireEye started in February 2013, the month the threat intelligence firm Mandiant (now owned by FireEye) publicly tied Unit 61398 to a heavily guarded building in Shanghai. Over the years that followed, FireEye analysts logged assaults on clients in the U.S., Japan, and Europe. Attacks peaked at just over 70 per month in September 2013. By the beginning of September 2015, before Obama and Xi signed the agreement, they had slowed to 10 per month, making the accord look like a mere footnote in China's about-face.

"All indications are that China had already adjusted their policy and approach, and that the agreement was something that was feasible to them because they had already changed direction," says Daniel McWhorter, chief intelligence strategist and vice president at FireEye. The report is limited to the firm's visibility and fuzzy on details like what files the attackers took, but in April NSA director Michael Rogers testified that hacking from China had declined. In a talk at the Aspen forum, meanwhile, CIA head John

Brennan reiterated that the intelligence community was uncovering fewer attacks from China. In August, when FireEye announced that it would lay off roughly 10 percent of its staff, executives blamed the downturn in Chinese activity.

'Vacuum cleaner' espionage

The "Wanted" posters and the fanfare behind the Unit 61398 indictment reinforced the popular misconception, perpetuated by shows like Mr. Robot, that Chinese hackers are highly organized in their methods and tools. In fact, they were long known for being decentralized and sloppy. Cybersecurity experts once marveled at finding multiple Chinese hacker groups penetrating the same target, with seemingly little or no coördination. At times, such groups made elemental errors. In the 2013 report on Unit 61398, or APT1, that preceded the Justice Department's indictment, Mandiant could attribute attacks to the Chinese People's Liberation Army (PLA) in part because the hackers used the army's hacking infrastructure, which is outside China's Great Firewall, to access their personal Facebook and Twitter accounts.

Many now believe that such groups have simply cut back on some of the noise that made them easy to detect. At the same time, China has probably refined its focus "from 'vacuum cleaner' espionage to more precisely targeted intrusion and theft," says Greg Austin, a professorial fellow with the EastWest Institute and the author of Cyber Policy in China. State-sponsored hackers used to suck up large amounts of data and then sift through it later, he says. That may have artificially inflated the number of commercial attacks, as hackers targeting dual-use technologies like solar panels swept up pricing information along with design specifications. A switch to more directed national-security- related espionage would mean a reduction in perceived commercial cyberattacks.

In some cases, meanwhile, the likes of UglyGorilla may have been working under the table, without the explicit permission of the central government. The Unit 61398 indictment, for example, alleges that one state- owned enterprise "hired" the unit to "build a 'secret' database to hold corporate 'intelligence.'"

Those explanations would help solve a number of long-standing mysteries. While Beijing has long encouraged the acquisition of foreign technologies, and IP theft is rampant among Chinese companies, exactly how the state might actively facilitate theft by companies is unclear. The Chinese government has no major intelligence allies and a range of priorities in intelligence collection, including monitoring dissidents, staying abreast of the South China Sea controversy, and tracking activists in Tibet and Xinjiang. It is not known where commercial spying would rank among these priorities--and how the information pilfered in state-sponsored attacks might be systematically disseminated.

Despite close links between the Chinese government and the private sector, in many areas there is no obvious firm to receive commercial secrets. The Unit 61398 indictment, for example, charges that the defendants stole thousands of sensitive files from a U.S. subsidiary of the German company SolarWorld AV. The document implies that the hackers then passed the documents on to a Chinese company or

companies exporting solar products to the United States. But some 400 firms fit that description, notes Austin.

The notion that the PLA, as opposed to another Chinese government entity, would have been the designated arbiter for civil-sector industrial espionage is puzzling on another level. The PLA once had its hands in an estimated 20,000 businesses, including everything from pharmaceutical companies to brothels. But since the late 1990s, the Chinese government has devoted considerable energy to reducing the army's side projects--with the aim of getting military personnel thinking about operations rather than real estate deals. Since he came to power in 2012, Xi Jinping has been particularly firm about military moonlighting.

Xi has also launched an anticorruption drive that, while politically motivated, has revealed the extent of military graft. In January 2015, 16 senior military officers were placed under investigation for offenses that included selling senior positions and ranks to the highest bidder. Among those purged was Guo Boxiong, former vice chairman of the all-important Central Military Commission. So extreme is the anticorruption effort within the PLA that alcohol, a mainstay of official banquets, has been banned from military receptions in hope of warding off unsavory deals--like, say, the sale of hacked commercial secrets.

A tipping point

Against that backdrop, the Chinese commitment last September to refrain from commercial attacks appears less significant. "It's not that China's living up to the agreement because they're living up to the agreement," says James A. Lewis of the Center for Strategic and International Studies in Washington, D.C. "They're living up to the agreement because they're trying to modernize the PLA and reduce corruption." While a decline in commercial hacking isn't a significant loss for China as a whole, he adds, "it is a huge loss for individual companies and PLA units."

Still, U.S. actions may have helped matters reach a tipping point for Chinese leaders, who may well have known about the under-the-table attacks and chosen to look the other way. Former Department of Homeland Security secretary Michael Chertoff, now chairman of the security consultancy Chertoff Group, told me at the Aspen forum, "It doesn't strike me as unlikely that the word went back, 'Guys, cool the hot-rodding. If there's something worth stealing, do it, but do it in a way that's not so obvious.'"

Regardless of the reason, the drop in apparent attacks should be celebrated, says Jason Healey, a scholar at Columbia University's School for International and Public Affairs who studies cyber-conflict. Even if China has simply cut back on PLA moonlighting and refined its handling of cyber- espionage, its current approach is "much less escalatory than it was," he says. "It's more like the U.S. system: you coördinate, you figure out who is going in. Someone goes in, and you share the take. It's more the way that a professional intelligence organization works."

Ongoing talks now provide a chance to keep the pressure on. A bilateral working group formed in the wake of the 2015 agreement is meeting several times a year. "Every time we talk, we reiterate the importance of abiding by the cybersecurity commitment," says Suzanne Spaulding, the Department of Homeland Security undersecretary who led a U.S. delegation to Beijing last June when Secretary Jeh Johnson was called away by the mass shooting in Orlando, Florida. "We make clear to our counterparts in every conversation that we are watching this carefully, and that there's frankly not a lot of public confidence about this. They are aware that the jury is still out."

Agence France-Presse
Cyber attack likely mitigated, US Homeland Security says
Tuesday, 25 October 2016
Byline: Staff report

Washington - The cyber attack which darkened a large portion of the US internet on Friday has been mitigated, but officials continue to monitor the situation, the Department of Homeland Security said Monday.
The domain name services company Dynamic Network Services Inc, or Dyn, suffered successive attacks, causing outages for hours for millions of users of brand-name internet services such as Twitter, Spotify and Netflix. Services began to stabilize on Friday afternoon.

Dyn said it was struck by so-called distributed denial of service attacks in which adversaries flood servers with so much traffic they stumble or collapse under the burden.

"At this time, we believe the attack has been mitigated," Homeland Secretary Jeh Johnson said in a statement.

Johnson also said Monday his department was aware of the malware which may have been used in the attack.

"This malware is referred to as Mirai and compromises Internet of Things devices, such as surveillance cameras and entertainment systems connected to the Internet," Johnson said.

The department's National Cybersecurity and Communications Integration Center was develop ways to respond to Mirai and similar malware, according to Johnson.

"The Department has also been working to develop a set of strategic principles for securing the Internet of Things, which we plan to release in the coming weeks."

Mirai was used in an attack last month on a website belonging to the journalist Brian Krebs, a cybersecurity expert and writer who said his site suffered a massive attack of 620 gigabits per second.

Krebs reported Friday that researchers at the security firm Flashpoint had determined that the attack on Dyn had involved Mirai.

Reuters
U.S. takes aim at cyber attacks from connected devices as recalls mount
Tuesday, 25 October 2016
Byline: Joseph Menn

San Francisco - Obama administration officials sought on Monday to reassure the public that it was taking steps to counter new types of cyber attacks such as the one Friday that rendered Twitter, Spotify, Netflix and dozens of other major websites unavailable.
The Department of Homeland Security said it had held a conference call with 18 major communication service providers shortly after the attack began and was working to develop a new set of "strategic principles" for securing internet-connected devices.

DHS said its National Cybersecurity and Communications Integration Center was working with companies, law enforcement and researchers to cope with attacks made possible by the rapidly expanding number of smart gadgets that make up the "internet of Things.

Such devices, including web-connected cameras, appliances and toys, have little in the way of security. More than a million of them have been commandeered by hackers, who can direct them to take down a target site by flooding it with junk traffic.

Several networks of compromised machines were directed to attack big customers of web infrastructure company Dyn last week, Dyn officials and security researchers said.

The disruption had subsided by late Friday night in America, and two of the manufacturers whose devices had been hijacked for the attack pledged Monday to try to fix them.

But security experts said that many of the devices would never be fixed and that the broader security threat posed by the internet of Things would get worse before it gets better.

"If you expect to fix all the internet devices that are out there, force better passwords, install some mechanism for doing updates and add some native security for the operating system, you are going to be working a long time," said Ed Amoroso, founder of TAG Cyber and former chief security officer at AT&T.

Instead, Amoroso said he hoped that government officials would focus on recommending better software architecture and that business partners would insist on better standards.

In the meantime, fresh responses by two of the companies involved in the attacks illustrated the extent of the problem.

Chinese firm Hangzhou Xiongmai Technology Co Ltd, which makes components for surveillance cameras, said it would recall some products from the United States.

Another Chinese company, Dahua Technology, acknowledged that some of its older cameras and video recorders were vulnerable to attacks when users had not changed the default passwords. Like Xiongmai, it said it would offer firmware updates on its website to fix the problem and would give discounts to customers who wanted to exchange their gear.

But neither company has anything like a comprehensive list of their customers, many of whom will never learn of the problems, said Dale Drew, chief security officer with communications provider Level 3.

"I wouldn't be surprised if the only way they are going to reach their consumers is through media reports, Drew said.

Wall Street Journal
Obama Says U.S. Has No Idea Who Carried Out Cyberattack
Tuesday, 25 October 2016
Byline: Carol E. Lee, Damian Paletta

Los Angeles - President Barack Obama said the U.S. doesn't know who launched an online attack Friday that rendered more than 1,200 websites unreachable, including Netflix and Twitter.
"We don't have any idea who did that," Mr. Obama said during a taped appearance Monday for the late-night show hosted by Jimmy Kimmel.

U.S. officials and cybersecurity experts believe attackers controlled a vast collection of internet-linked devices such as cameras, video recorders and routers, to essentially overwhelm parts of the internet and make dozens of popular websites unreachable.

Web- technology developer Dynamic Network Services Inc., known as Dyn, said its domain-name-system services were subject to the attack, known as a denial of service. The attack came in several waves throughout Friday.

The Department of Homeland Security on Monday said it was still "monitoring events" tied to the attack. It said that following the incident, it held a conference call with 18 telecommunications service providers to discuss what happened, adding "at this time, we believe the attack has been mitigated."

DHS said "one type of malware potentially used in this incident" is known as Mirai and targets devices such as cameras and entertainment systems that have internet links. DHS is working to develop rules to address these types of attacks, but the timing of such a move is unclear.

For Mr. Obama to say, several days after the attacks, that the government doesn't know the culprit could be a testament to how hard it is to uncover clues after such an event. The attack is considered sophisticated, and likely within the realm of tools that foreign governments and advanced criminal groups can activate. It is unclear, though, what the motive of the perpetrators was or if they were trying to deliver any sort of warnings or message.

Mr. Obama said the incident underscores how monumental the task of dealing with cybersecurity is for his successors.

"One of the biggest challenges for the next president and the president after that and the president after that is going to be: How do we continue to get all the benefits of being in cyberspace but protect our finances, protect our privacy? How do we balance issues of security," Mr. Obama said.

"We're going to have to come up with frameworks and some of its going to involve technology, some of it's going to involve the law but this is going to be a big debate that we're going to have for a long time," he added.

Mr. Obama during the appearance also joked about the security precautions attached to his iPhone to prevent intrusions. He said most of the functions, such as making calls, texting and taking photographs, are disabled, leaving him only able to use it to send email and surf the internet.

Even with those precautions, he said, he still doesn't put anything in an email that he wouldn't want to see on the front page of the newspapers.

Le Figaro
LeEco, le nouveau champion chinois qui veut envahir le monde
Tuesday, 25 October 2016
Byline: Lucie Ronfaut

Pékin - Smartphone, TV, culture en ligne : cette société veut créer un empire de nouvelles technologies. Internet Difficile de trouver une entreprise à qui le comparer. Ni Netflix, ni Samsung, ni Google, ni Sony : LeEco, nouveau géant chinois des nouvelles technologies, est tout ça à la fois. Quasi inconnu il y a un an, le groupe pourrait vendre plus de 25 millions de téléphones en 2016, d'après les estimations du cabinet Strategy Analytics, soit 1,72 % du marché mondial. Cette part a progressé de 500 % en un an. Si ces estimations se confirment, LeEco (aussi connu sous le nom de « Leshi » en Chine) deviendra le vendeur de smartphones avec la plus forte croissance au monde. « Le marché chinois des smartphones bouge

rapidement, mais cette croissance est exceptionnelle » , souligne Neil Mawston, analyste chez Strategy Analytics, lui-même surpris de cette performance.

La Chine n'est qu'une première étape, et les ambitions de LeEco semblent sans limites. La semaine dernière, le groupe annonçait son arrivée aux États- Unis. Il s'est déjà lancé en Inde fin 2015. L'entreprise, cotée à la Bourse de Schenzen, est valorisée à 13 milliards de dollars environ. Son chiffre d'affaires s'élevait à 1,99 milliard de dollars en 2015, et pourrait tripler d'ici à 2018. Ses profits devraient, eux, s'établir à 120 millions de dollars environ cette année.

LeEco affiche un portefeuille impressionnant de produits, des smartphones en passant par les télévisions, les services en ligne, la production de séries télévisées, la réalité virtuelle et même des vélos électriques. Son dernier projet en date est le développement d'une voiture de sport électrique.

Derrière cette boulimie de produits, il émerge une vraie stratégie. LeEco veut construire un empire de nouvelles technologies capables de répondre à tous les besoins en divertissement et en communication. Le groupe, né en 2003, est d'abord baptisé LeTV. Il est alors spécialisé dans les contenus en ligne : films, séries télévisées, musique... En 2013, LeTV fait le grand saut vers les objets connectés. Il commence à vendre des télévisions connectées. En 2016, l'entreprise prend le nom de LeEco et étend ses ambitions. Elle rachète pour 2 milliards de dollars le plus grand fabricant américain de télévisions, Vizio, au mois de juillet.

Une stratégie de contenus

Mais c'est dans les smartphones que LeEco connaît le plus de succès. Il vend ses premiers appareils en 2015, d'abord en Chine. Ils fonctionnent sous Android et appartiennent à la catégorie des téléphones moyen de gamme, sous les 500 dollars. « Il s'agit d'un concurrent sérieux pour des marques comme LG, HTC ou ZTE, ou certains smartphones de Samsung » , estime Roberta Cozza, analyste chez Gartner. La force de LeEco réside dans sa stratégie de contenus. Fort de son passé dans le streaming, l'entreprise dote tous ses produits d'abonnements à ses différentes plateformes. « Beaucoup de sociétés font de bons smartphones. Peu savent produire des bons contenus » , résume Roberta Cozza. « Cela leur permet d'avoir des revenus récurrents en plus des ventes de leurs produits. » Pour son arrivée sur le marché international, LeEco a adapté cette stratégie et a passé des partenariats avec Vice, Showgate et Lionsgate. LeEco a aussi recruté l'ancien président du groupe Paramount Film, Adam Goodman, afin de produire des contenus originaux en anglais. Il n'a néanmoins pas encore le projet de se lancer sur le marché européen.

Malgré cette trajectoire impressionnante, LeEco n'est pas la première entreprise chinoise à avoir des ambitions internationales. La tâche n'est pas aisée. Un temps baptisé « l'Apple chinois » , le fabricant de smartphone Xiaomi a vu sa valorisation divisée par dix en deux ans faute de croissance à l'international. Huawei et ZTE ont, eux, affronté la méfiance des autorités américaines qui les ont accusés de vouloir faciliter l'espionnage du gouvernement chinois. Pour prouver le sérieux de ses ambitions, LeEco a annoncé vouloir embaucher plus de 12 000 personnes dans la région de San Francisco. Il disposait déjà

d'une équipe de plus de 500 employés américains à San José. « Il s'agit d'un message fort en termes de marketing » , estime Neil Mawston. « Reste à savoir s'il peut tenir ses promesses sur la durée. » Pour LeEco, le véritable défi est de ne pas finir asphyxié par son ambition démesurée. -

Associated Press
Cyberattacks steadily growing in intensity, scope
Monday, 24 October 2016
Byline: Staff report

New York - Could millions of connected cameras, thermostats and kids' toys bring the internet to its knees? It's beginning to look that way.
On Friday, epic cyberattacks crippled a major internet firm, repeatedly disrupting the availability of popular websites across the United States. A hacker group claiming responsibility says that the day's antics were just a dry run and that it has its sights set on a much bigger target. And the attackers now have a secret weapon in the increasing array of internet-enabled household devices they can subvert and use to wreak havoc.

Meet the fire hose

Manchester, New Hampshire-based Dyn Inc. said its server infrastructure was hit by distributed denial-of-service, or DDoS, attacks.

These work by overwhelming targeted machines with junk data traffic sort of like knocking someone over by blasting them with a fire hose. The attack temporarily blocked some access to popular websites from across America and Europe such as Twitter, Netflix and PayPal.

Jason Read, founder of the internet performance monitoring firm CloudHarmony, owned by Gartner Inc., said his company tracked a half-hour-long disruption early Friday affecting access to many sites from the East Coast. A second attack later in the day spread disruption to the West Coast as well as some users in Europe.

Members of a shadowy hacker group that calls itself New World Hackers claimed responsibility for the attack via Twitter, though that claim could not be verified. They said they organized networks of connected devices to create a massive botnet that threw a monstrous 1.2 trillion bits of data every second at Dyn's servers. Dyn officials wouldn't confirm the figure during a conference call later Friday with reporters.

Make that many fire hoses

DDoS attacks have been growing in frequency and size in recent months. But if the hackers' claims are true, Friday's attacks take DDoS to a new level. According to a report from the cybersecurity firm

Verisign, the largest DDoS attack perpetrated during the second quarter of this year peaked at just 256 billion bits per second.

A huge September attack that shut down security journalist Brian Krebs' website clocked in at 620 billion bits per second. Research from the cybersecurity firm Flashpoint said Friday that the same kind of malware was used in the attacks against both Krebs and Dyn.

Lance Cottrell, chief scientist for the cybersecurity firm Ntrepid, said while DDoS attacks have been used for years, they've become very popular in recent months, thanks to the proliferation of "internet of things" devices ranging from connected thermostats to security cameras and smart TVs. Many of those devices feature little in the way of security, making them easy targets for hackers.

The power of this kind of cyberattack is limited by the number of devices an attacker can connect to. Just a few years ago, most attackers were limited to infecting and recruiting "zombie" home PCs. But the popularity of new internet-connected gadgets has vastly increased the pool of potential devices they can weaponize. The average North American home contains 13 internet-connected devices, according to the research firm IHS Markit.

Since the attacks usually don't harm the consumer electronics companies that build the devices, or the consumers that unwittingly use them, companies have little incentive to boost security, Cottrell said.

What's behind the attacks

Like with other online attacks, the motivation behind DDoS attacks is usually mischief or money. Attackers have shut down websites in the past to make political statements. DDoS attacks have also been used in extortion attempts, something that's been made easier by the advent of Bitcoin.

For its part, a member of New World Hackers who identified themselves as "Prophet" told an AP reporter via Twitter direct message exchange that collective isn't motivated by money and doesn't have anything personal against Dyn, Twitter or any of the other sites affected by the attacks. Instead, the hacker said, the attacks were merely a test, and claimed that the next target will be the Russian government for committing alleged cyberattacks against the U.S. earlier this year.

"Twitter was kind of the main target. It showed people who doubted us what we were capable of doing, plus we got the chance to see our capability," said "Prophet." The claims couldn't be verified.

The collective has in the past claimed responsibility for similar attacks against sites including ESPNFantasySports.com in September and the BBC on Dec. 31. The attack on the BBC marshalled half the computing power of Friday's attacks.

A shifting global assault

Dyn said it first became aware of an attack around 7:00 a.m. local time, focused on data centers on the East Coast of the U.S. Services were restored about two hours later. But then attackers shifted to offshore data centers, and the latest wave of problems continued until Friday evening Eastern time.

"Prophet" told the AP that his group actually had stopped its attacks by Friday afternoon, but that others, including members of the hacker collective known as Anonymous, had picked up where they left off. Anonymous didn't respond to a request for comment via Twitter.

The U.S. Department of Homeland Security is monitoring the situation, White House spokesman Josh Earnest told reporters Friday. He said he had no information about who may be behind the disruption.

Cottrell noted that there are several firms that offer protection against DDoS attacks, by giving companies a way to divert the bad traffic and remain online in case of an attack. But monthly subscription fees for these services are generally equal to a typical DDoS extortion payment, giving companies little incentive to pay for them.

Meanwhile not much is required in the way of resources or skill to mount a botnet attack, he said, adding that would-be attackers can rent botnets for as little as $100. Cottrell said the long-term solution lies in improving the security of all internet- connected devices.

The Australian
Information breaches are a management issue
Tuesday, 25 October 2016
Byline: Paul Wallbank

Comment: Cybersecurity is becoming an important responsibility for executives and directors. Often shortened to "cyber", it's easy to dismiss cybersecurity as just being the latest industry buzzword. However, ensuring information systems are secure is now firmly a management issue.
Information breaches have become embarrassingly common in recent times with events ranging from Target exposing 40 million customer records in 2013, a breach that cost the company $162 million, through to national security embarrassments like the Snowden revelations.

Exacerbating the risks to businesses is the dependency upon information systems for normal operations, and the damage from denial-of-service attacks such as the outage across much of the US last weekend can be debilitating and costly. The recent Australian census saga, that cost taxpayers $30m, is an illustration of how costly poorly planned responses to service interruptions and security breaches can be.

Compounding the risks for Australian executives are the breach disclosure laws tabled in federal parliament last week, which threaten $340,000 in fines for individuals and $1.7m for corporations that fail to act quickly on data privacy failures.

In such a high-risk environment, business leaders need to be proactive. The legislation is squarely aimed at organisations that are either wilfully blind or like to employ the concept "plausible deniability".

As that period of "wilful blindness" and "plausible deniability" comes to an end, executives and directors have to start taking their responsibilities in protecting data far more seriously. The challenge lies in understanding the risks.

The defining feature of this process for organisations is figuring out what's important and what's noise. This so-called "crown jewels assessment" doesn't just apply to figuring out what might be crucial data for the business but also to whom it may be attractive.

Credit card numbers may be the crown jewels for a business and while they may attract criminals they will be of little interest to foreign intelligence agencies. Contextualisation is critical as is understanding where the risks lie for critical data and processes.

In understanding what those "crown jewels" are, it is important to consider what is valuable within the organisation. While to the marketing team the most valuable information may be customer data, to the chief operating officer it may be ensuring continuity of service, while to external parties it could be pricing details or legal correspondence.

Organisations will also be well served by reviewing their contracts and getting comfortable with the fine print. If you have a cloud services provider that experiences a breach, how are they going to go about doing the notification?

Staying on top of these little details can save a business a lot of heartache if and when customer data is compromised.

In a world where subcontracting and outsourcing is normal business practice, the risk from third party vendors is real and goes beyond cloud providers.

The disastrous Target hack was traced back to an air-conditioning contractor's compromised system, and Edward Snowden himself wasn't a direct government employee.

Privacy and security breach notifications are only part of the broader cybersecurity picture though and the field is becoming more complex.

Last weekend's massive denial of service attack that compromised many US-based online services was caused by the Mirai botnet, that exploits vulnerabilities in cheap internet-of-things devices.

With business processes becoming increasingly connected and automated, management concerns are extending to the security, integrity and reliability of devices being used in their organisation.

Even if the business-critical sensors being officially purchased are of high quality, everything from smartphones to connected kettles being bought into the staff tearoom could be a potential risk to the corporate network and a business's reputation.

It would be a mistake however to think cybersecurity is purely a technology problem, because there's an undeniable human element.

While employees and contractors can often become unwitting pawns sometimes, as in the case of Snowden, they can be the perpetrators as well.

The "insider threat" phenomena is all about people who use tools or technology to pilfer data and they get away with it because organisations are more focused on the technology than people.As businesses becomes more dependent upon data and connected systems it's time for the captains of industry to step up to the plate on governance, compliance and culture.

The Australian
Leaked sub secrets key to Aussie fleet, says builder
Tuesday, 25 October 2016
Byline: Cameron Stewart

Canberra - The Turnbull government's claim that the $50 billion future submarine project will not be hurt by the massive leak of confidential data from French submarine builder DCNS has been undermined by the architect who will build the boats.
Gerard Audet, the chief naval architect of the proposed new Australian submarine, the Shortfin Barracuda, has revealed in an article that the new Australian submarine will have key systems in common with the French--designed Scorpene-class of submarines which suffered the major leak of confidential data.

The Australian revealed in -August that 22,400 pages of con-fidential data detailing the combat capability of India's six new Scorpene-class submarines had been leaked from DCNS, the French company which also won the design contract for the Australian project.

At that time, Malcolm Turnbull and Defence Industry Minister Christopher Pyne played down the relevance of the leak, with the Prime Minister saying the Australian boat would be "completely different" to the -Indian Scorpene. Mr Pyne also said the Indian boat bore "no relation" to the Australian boat.

But in a little-known article published in April, only weeks -before France won the bid, Mr Audet wrote that while most of the Shortfin Barracuda will be based on the new French nuclear- powered Barracuda-class subs, some keys systems will be based on the diesel- electric Scorpene.

"The main area where Barracuda design references were not used was in the area of the electrical system (batteries and voltage), power generation (induction and diesel generators), and propulsion (main electric motor)," he wrote in an article co-authored by the head of DCNS Australia, Sean Costello, and published on the website of the Australian Strategic Policy -Institute.

"In these systems the design reference comes from the Scor-pene class of diesel electric submarines, or from an existing submarine technology within DCNS. Existing technologies are re-used in all systems in the Shortfin Barracuda Block 1A." The leaked documents revealed the combat capability of the six Scorpene-class subs which DCNS designed for the Indian navy. The documents, marked "Restricted Scorpene India", reveal information including the highly sensitive stealth capabilities of the boats, the frequencies at which they gather intelligence and the levels of noise they make.

They disclose magnetic, electromagnetic and infra-red data as well as specifications of the submarines' torpedo launch systems and even the performance parameters of its weapons systems.

However, the documents mostly reveal details of the Scorpene's combat system rather than the motor, generators and electrical system which Mr Audet says will have some commonality with the Australian boats. The Scor-pene submarines are much smaller, at about 1800 tonnes, than the Shortfin Barracuda which will be more than 4000 tonnes.

A spokesman for Mr Pyne said yesterday that there would be no "performance comparison" between the Scorpene sub-marines and the new Australian boats. "Australia's future submarine is yet to be designed. It will be a unique Australian design built for purpose," he said. "There will be no performance comparison -between the two platforms. They will be completely different." Mr Costello said yesterday; "The Australian future submarine is a new design for the Royal Australian Navy's requirement taking the French Navy Barracuda class as its design reference. Reference to, or re-use of, technologies in the Scorpene type of submarines cannot be taken to infer performances of the new Australian design." Defence Department officials told a parliamentary estimates hearing last week the key lesson from the leaked Scorpene documents was to ensure that such a major breach of security did not occur on the Australian project.

Defence is currently working with DCNS Australia on the -parameters of the security -arrangements.

DCNS has assured Defence that it will take all possible precautions to ensure the highest possible information security.

A spokesman for Mr Pyne said yesterday: "This government takes security surrounding our submarine capability very seriously. That's why we have had in place the tightest security available for the Collins-class submarines that has stood the test of time." DCNS defeated Germany and Japan to win the contract to design 12 submarine for the navy to replace the current six Collins-class boats when they are phased out from the early 2030s.

The leaked DCNS documents are believed to have been stolen from the company by a former DCNS contractor in 2011, before the data was taken to Southeast Asia and eventually to Australia.

French prosecutors are investigating the data leak, while the Indian navy is investigating the potential damage of the leak for its Scorpene fleet.

Parts of Australia's next subs that have the same design as the Scorpene subs used by India, Malaysia and Brazil * The main electric motor * Induction and diesel generators * Batteries and voltage

What they said MALCOLM TURNBULL Prime Minister 'The submarine that we will be building with the French is called the Barracuda. It is a completely different submarine to the one they are building for India

CHRISTOPHER PYNE Defence Industry Minister 'The Scorpene class of submarine build by DCNS is their export model of submarine. It bears no relation at all to the Barracuda submarine which will be built for Australia, which is a unique submarine. It will be a new design and a new build'

GERARD AUDET DCNS chief naval architect on Australia's new submarine, the Shortfin Barracuda Block 1A 'The main area where Barracuda design references were not used was in the area of the electrical system (batteries and voltage), power generation (induction and diesel generators), and propulsion (main electric motor). In these systems the design reference comes from the Scorpene class of diesel-electric submarines, or from an existing submarine technology within DCNS.Existing technologies are re-used in all systems in the Shortfin Barracuda Block 1A'

The Intercept
Spies for Hire
Monday, 24 October 2016
Byline: Jenna McLaughlin

Washington - In July, Simone Margaritelli, an Italian security researcher, boarded a Boeing 777 in Rome headed for Dubai, a city now billing itself as a tech startup hub.
He had a big job interview with a new, well-funded cybersecurity company called DarkMatter, whose self- described mission is to "safeguard the most complex organizations," from government to the private sector, by preventing and fighting malicious cyberattacks and providing secure methods of communication -- defensive cybersecurity, rather than offensive, which involves breaking into online systems and devices for espionage or destruction.

A friend of a friend had recommended Margaritelli, who was invited to spend five days in the United Arab Emirates at the company's expense to learn more about the job. When he arrived in Dubai, the City of Gold, he found a full schedule of outings and a deluxe suite at the Jannah Marina Bay Suites hotel.

Margaritelli used to be a "blackhat" -- a hacker looking to break into electronic systems. Now he works for a mobile security firm called Zimperium, where he still hunts for security flaws but does so to help people fix them. I "break stuff to make the world a safer place," his website reads. He's most well known for a portable tool he developed called Bettercap, used to perform a man-in-the- middle attack, where a hacker can eavesdrop or sometimes alter private communications between individuals.

When he arrived at the 29th floor of the Marina Plaza for his interview, the company representative described a plan to deploy electronic probes all over major cities in the UAE, which a team of hackers would then break into, guaranteeing access for DarkMatter and its customer -- the Emirati government. The mission would be for the "exclusive" benefit of national security, Margaritelli was told. "Imagine that there's a person of interest at the Dubai Mall, we've already set up all our probes all over the city, we press a button and BOOM! All the devices in the mall are infected and traceable," Margaritelli wrote in a blog post recounting his experience.

Margaritelli declined to pursue the job offer. After his post, titled "How the United Arab Emirates Intelligence Tried to Hire Me to Spy on Its People," began circulating, DarkMatter issued a single terse Twitter reply. The company said it preferred "talking reality & not fantasy."

"No one from DarkMatter or its subsidiaries have ever interviewed Mr. Margaritelli," Kevin Healy, director of communications for DarkMatter, wrote in an email to The Intercept. The man Margaritelli says interviewed him, Healy continued, was only an advisory consultant to DarkMatter -- and that relationship has since ended (though several sources say he was employed by the company and had a DarkMatter email address).

"While we respect an author's right to express a personal opinion, we do not view the content in question as credible, and therefore have no further comment," Healy wrote.

DarkMatter denied outright Margaritelli's assertions that it was recruiting hackers to research offensive security techniques. "Neither DarkMatter - nor any subsidiary, subset, research wing, or advisory department--engage in the activities described," Healy wrote. "We conduct rigorous testing on all our products to ensure they do not include any vulnerabilities."

Indeed, the idea of a UAE- based company recruiting an army of cyberwarriors from abroad to conduct mass surveillance aimed at the country's own citizens may sound like something out of a bad Bond movie, but based on several months of interviews and research conducted by The Intercept, it appears DarkMatter has been doing precisely that.

Most of those who spoke with The Intercept asked to remain anonymous, citing nondisclosure agreements, fear of potential political persecution in the UAE, professional reprisals, and loss of current and future employment opportunities. Those quoted anonymously were speaking about events based on their direct experience with DarkMatter.

Margaritelli isn't the only one who insists that DarkMatter isn't being truthful about its operations and recruitment. More than five sources with knowledge of different parts of the company told The Intercept that sometime after its public debut last November, DarkMatter or a subsidiary began aggressively seeking skilled hackers, including some from the United States, to help it accomplish a wide range of offensive cybersecurity goals. Its work is aimed at exploiting hardware probes installed across major cities for surveillance, hunting down never-before- seen vulnerabilities in software, and building stealth malware implants to track, locate, and hack basically any person at any time in the UAE, several sources explained. As Margaritelli described it in an email to me, "Basically it's big brother on steroids."

DarkMatter made its public debut when the CEO, Faisal Al Bannai, gave a keynote speech surrounded by government officials, engineers, and businesspeople at the 2nd Annual Arab Future Cities Summit in Dubai. DarkMatter launched its portfolio of cybersecurity products as a "digital defense and intelligence service" for the nation. Al Bannai's speech and DarkMatter marketing materials were peppered with buzzwords like cyber network defense and secure communications. Following its launch, the company routinely boasted, online and during conferences and radio interviews, about its would-be world-changing defensive cybersecurity missions, including developing its own encryption platforms and potentially secure phones in house, defending national and corporate networks, bug-sweeping and countersurveillance, and more, all under a single umbrella.

Local tech blogs praised the company and celebrated its connection to the UAE government. They described DarkMatter as a savior to UAE businesses and institutions at constant threat of cyber intrusion, citing attacks against several banks in 2015 that temporarily crippled the country's online banking infrastructure.

Soon, DarkMatter had hired a roster of top-level talent from major tech giants around the world, including Google, Samsung, Qualcomm, McAfee, and even a co-founder of the encrypted messaging service Wickr. The new star-studded squad traveled to conferences like San Francisco's annual RSA summit, appearing on radio and TV shows along the way. They rolled out a secure voice and chat application, partnered up with Symantec to improve digital threat detection in the Middle East, and opened a research and development center in Canada, as well as offices in China.

But sometime last year, a segment of the company's mandate grew from providing defense and forensics research to developing a powerful team capable of cyber offense, multiple sources tell The Intercept. According to one source, DarkMatter's newfound interest in offensive operations coincided with revelations contained in leaked emails that the Italian company Hacking Team had sold surveillance equipment to a large number of repressive regimes. Out of Hacking Team's ashes, DarkMatter rose.

While cybersecurity companies traditionally aim to ensure that the code in software and hardware is free of flaws -- mistakes that malicious hackers can take advantage of -- DarkMatter, according to sources familiar with the company's activities, was trying to find and exploit these flaws in order to install malware. DarkMatter could take over a nearby surveillance camera or cellphone and basically do

whatever it wanted with it -- conduct surveillance, interfere with or change any electronic messages it emitted, or block the signals entirely.

It's not clear that the company's defensive employees have any idea; in fact, multiple sources suggested those projects are likely hidden from them. One source explained how company representatives tried to insist that the offensive research they were recruiting for would be conducted outside DarkMatter, with some sort of partner organization or offshoot. But several sources, Margaritelli included, said top leadership was directly involved in interviews and knew the truth.

DarkMatter's spokesperson said the company is "privately held" and "does not receive any funding from the United Arab Emirates."

There do, however, appear to be strong links between the company and the government. In press releases, the company identifies itself as "already a strategic partner to the UAE government," and its offices are located on the 15th floor of the round Aldar Headquarters in Abu Dhabi, two floors away from the country's intelligence agency, the National Electronic Security Authority. DarkMatter's senior vice president of technology research used to hold the same position at NESA.

By the early months of 2016, DarkMatter's recruitment push was already well underway. The company's publicly identifiable employees came from across the U.S. national security establishment. According to public LinkedIn profiles, one current DarkMatter employee was a global network exploitation analyst for the U.S. Department of Defense who "strategized activities against particular networks" and supported "foreign intelligence collection." Another was a counterintelligence "special agent" for the Pentagon, whose LinkedIn boasts an "active" top-secret security clearance with a polygraph screening. Another experienced cryptographer working for DarkMatter was a senior technical adviser to the NSA, where he was intricately involved in designing "U.S. voice and data systems."

But the company hasn't been upfront about all the jobs it's recruiting top talent for, Margaritelli and multiple other sources suggest. DarkMatter's recruiters reached out to the information security community, promising high-paying, exciting jobs that would be focused on cyberdefense, according to more than a dozen security researchers interviewed by The Intercept, some of whom shared recruitment materials. A number of cybersecurity experts claimed on Twitter to have been contacted by recruiters, including Charlie Miller, an Uber security researcher and former NSA analyst; Chris Valasek, a noted car hacker who has teamed up with Miller; and Fabio Assolini, a security researcher for Kaspersky Labs.

One recruiting email reviewed by The Intercept offered a carefree, tax-free life in Dubai, with housing, meals, health care, children's education, and transportation all provided free of charge. The email said the job was with a newly formed "public/private partnership" that would be the "Cyber Security provider for all UAE Government." Another email said DarkMatter's plan was to hire 250 "geniuses" before the end of 2016. One security researcher said DarkMatter recruiters had contacted him on LinkedIn five or six separate times.

Some potential recruits didn't respond, but others were excited; the job offered the chance to innovate the cybersecurity of an entire nation. The lucrative payday also attracted them; according to one source, who requested anonymity fearing professional reprisal, some offers were as high as half a million dollars a year -- a number similar to other offers shared with The Intercept.

According to a source familiar with the company, an American citizen named Victor Kouznetsov who splits his time between the U.S. and the Middle East was a key recruiter for DarkMatter in the United States.

A man answering a cellphone identified in public records as belonging to Kouznetsov insisted that he must have been contacted in error; he did not work for DarkMatter and his name was not Victor. When asked why his voicemail message gave his name as "Victor," he hung up. Reached by The Intercept via email, Kouznetsov declined to answer questions. "As you can imagine my NDA with DarkMatter prevents me from disclosing exactly what I do for the company, but I could say that none of it is recruiting researchers in offensive security," he wrote.

Several researchers whom DarkMatter approached, including Margaritelli, confirmed they were specifically told they would be working on offensive operations. In Margaritelli's case, he was informed the company wanted to install a set of probes around Dubai, including base transceiver stations -- equipment that allows for wireless communication between a device and a network -- wireless access points, drones, surveillance cameras, and more.

The probes could be installed by DarkMatter surreptitiously or facilitated by telecoms tacitly agreeing to the surveillance setup, and the company could attach an offensive implant directly onto the probes capable of intercepting and modifying digital traffic on IP, 2G, 3G, and 4G networks. Anyone with a cellphone or using a device to connect to a wireless network connected to one of the probes would be vulnerable to hacking and tracking.

As Margaritelli explained it, the software DarkMatter originally designed to penetrate the probes "does not scale well enough" and therefore couldn't handle the massive amounts of traffic it would be intercepting -- forcing the need for a second team of hackers to do the job. The company wanted him to help solve the problem.

Margaritelli's account is the most revealing, but several other sources discussed similar projects proposed by DarkMatter, including researching and developing exploits for zero-day vulnerabilities, as well as deploying and developing some of the same stealth malware implants Margaritelli was asked to work on. DarkMatter asked one researcher, who has discovered and reported bugs to Facebook, Google, and other major technology companies, to use his vulnerability research "to allow them to have access on trusted domains." Basically, he would find a flaw in a website that would allow DarkMatter to manipulate it to help spread malware to targets without being detected. The researcher, who spoke

anonymously, said he refused, even after getting an offer for more money, because, in contrast to DarkMatter's proposal, "what I'm doing is ethical hacking."

But what two sources and several security researchers The Intercept consulted were most concerned about was DarkMatter's plan to become a certificate authority. A certificate authority is a trusted third party, typically a company or official agency, that issues digital certificates -- basically, electronic "passports" that verify a user's identity and that software is legitimate.

Web traffic and code from Microsoft, Facebook, Mozilla, and others is trustworthy because the company digitally signs off on it. But DarkMatter, as a certificate authority, could pretend to be someone else and issue its own digital certificate. There are mechanisms in place to prevent this type of attack, called certificate pinning, but many sites don't use those precautions -- and they still might not prevent DarkMatter from signing code, such as for a software update, as someone else. In theory, the company could sign an anti-virus update that looked like it came from Kaspersky Labs, when in reality it is sending malicious code.

DarkMatter, according to one source, would be able to use its authority to sign its own rootkits -- software tools that allow undetected and unauthorized access to computer systems -- in order to carry out man-in-the-middle attacks. "This is huge," the source said.

DarkMatter has a business unit dedicated to public key infrastructure "or national root certificates of trust for countries regionally and internationally," Healy confirmed. "While DarkMatter is not a central [public key infrastructure] authority for the UAE, we currently provide consulting and management services and intend to launch our own commercial Certification services soon."

While DarkMatter denied any plans to use its capabilities for cyber offense, if the company continues to develop secure messaging platforms, or hardware including its own phones, it would have access to all the internal schematics of those products: bug reports, security standards, and more. DarkMatter's hackers could secretly take advantage of that information while its defensive staff works to fix the flaw and push an update to consumer devices, a process that can take years.

When asked about the possibility of selling its own phones, Healy wrote that DarkMatter is, in fact, considering developing hardware.

Recruiting wasn't the only way DarkMatter snapped up top offensive talent. Last winter, the company poached a large number of employees from an American company, a Baltimore startup called CyberPoint International, formally on contract with the Ministry of the Interior of the United Arab Emirates. CyberPoint, founded by CEO Karl Gumtow and his wife, Vicki, in 2009, billed itself as a defensive operation -- protecting financial information, intellectual property, business records, and other forms of communications. It won multiple contracts with different parts of the U.S. government, including $6 million from the Pentagon's Defense Advanced Research Projects Agency, and Gumtow was nominated last year for the Maryland region Entrepreneur of the Year award. News articles also listed

CyberPoint as one of the companies that sent employees to the United Arab Emirates to train its intelligence agency, NESA, essentially the equivalent of the United States NSA.

But last summer, CyberPoint made headlines for teaming up with the Italian surveillance peddler Hacking Team, whose internal emails were leaked -- revealing an extensive account of sales to repressive regimes. The leaked emails indicated that representatives from CyberPoint had worked with Hacking Team to facilitate the sale of what appeared to be surveillance equipment to the UAE government. Around the end of 2015, there was an internal struggle within CyberPoint over the UAE contract, five sources familiar with the company told The Intercept. Former CyberPoint employees spoke to The Intercept on the condition of anonymity out of fear of reprisal and concern for the safety of associates still living in the Emirates.

After the Hacking Team emails leaked in July, there were loud, angry meetings in CyberPoint offices -- people deciding what to do now that their internal operations in the Middle East had been exposed to the world. As a result of those discussions, two things happened: A vast chunk of CyberPoint staff jumped ship to DarkMatter, which was already dangling massive yearly salaries and luxurious benefits. DarkMatter even helped some employees legally shift their state residency to South Dakota to get more lenient tax breaks while living overseas, according to one source. DarkMatter does not "comment on individual employment contracts," Healy wrote to The Intercept. "In summary we abide by the law in our employment and operational activities in all the jurisdictions in which we operate."

CyberPoint employees in the UAE who weren't offered -- or didn't accept -- jobs at DarkMatter weren't promised contract extensions. CyberPoint sent out a notice in December, one former employee said, announcing two months' notice on the contract. For some who left, it was a surprise, and they still aren't totally sure what happened. Others suggested DarkMatter was only interested in the more technical staff. One source described the exodus of employees as more of a "hostile takeover" directed by the United Arab Emirates government -- ending CyberPoint's original UAE contract and offering positions within the country instead, to get engineers under its own roof.

DarkMatter confirmed that some CyberPoint employees joined the UAE company but said this was nothing extraordinary. "DarkMatter recruits talent from across the globe and currently has over 400 team members, some of whom joined us from CyberPoint. They now occupy a diverse set of duties and responsibilities across several departments," Healy said.

According to Gumtow, CyberPoint's CEO, the company has gone through "quite a few changes" since it pulled out of the UAE for good. He sent responses to questions submitted by The Intercept via LinkedIn messages. There are no longer any CyberPoint employees in the Emirates, and no part of the company was acquired or bought by DarkMatter or anyone else, he wrote. CyberPoint, Gumtow said, never contracted with DarkMatter.

Additionally, Gumtow clarified that CyberPoint isn't in the business of developing "cyberweapons." Instead, the company conducts "penetration tests and security assessments," he wrote. "We use commercial and custom tools that are widely available all around the world."

However, those same tools used for improving cyberdefense can be turned around to infect unsuspecting targets. Even if the intelligence community uses those tools lawfully to infect targeted systems during national security investigations, others can steal or adapt the code to hack unsuspecting journalists or activists. "The overlap between offense and defense is very large," Nicholas Weaver, a security researcher at the International Computer Science Institute, wrote in an email to The Intercept. "Especially when it comes to network monitoring: The exact same tools can be used to monitor your network to detect attacks and monitor a network for bulk surveillance."

CyberPoint International did "good work, maybe noble, in some cases," one former employee said. But a small percentage of the work was "shady," suggesting it involved offensive research against different online platforms.

Another source stated that research, development, and coding conducted within CyberPoint ended up being used for a targeted spyware attack on journalists and activists in the Emirates between 2012 and the present. The attack involved spyware sent through Twitter, spear-phishing emails, and a malicious URL shortening service. These types of attacks are familiar to Emirati human rights activist Ahmed Mansoor. He told The Intercept that he hasn't encountered DarkMatter but was warned about the company recently by a friend, who told him, "They are doing the hacking for UAE security bodies."

Security researchers nicknamed the hacking group behind the attack "Stealth Falcon." The researchers noted that "circumstantial evidence suggests a link between Stealth Falcon and the UAE government," based on "digital artifacts."

Stealth Falcon attacked some UAE targets after CyberPoint left the UAE, and some employees who worked on the spyware or had access to it joined DarkMatter, according to the source, who said that not every instance of the malware attack has yet been detected. "There's a lot that hasn't been discovered," the source said.

DarkMatter, Healy said, is not aware of Stealth Falcon or the offensive tools used to access journalists' information. "As we have explained previously, we do not own or develop any cybersecurity solutions for offensive purposes."

At one point in time, CyberPoint was essentially capable of penetrating millions of devices regardless of brand, given its awareness of vulnerabilities -- undiscovered or unpatched -- in software around the world, one source explained. Those included vulnerabilities in Tor Browser, Firefox, Internet Explorer, and Microsoft Office.

The United Arab Emirates appears to be hoping to create its own cyber offense team, another source explained. Those capabilities could include cyber network attack teams and cyber network exploitation teams, for disruptive cyberattacks to disable adversaries' online resources, as well as for espionage and spying -- capabilities being developed in governments worldwide with varying levels of oversight and restriction.

According to Ryan Duff, a security researcher and former cyber operations tactician for U.S. Cyber Command, computer network exploitation and computer network attacks are distinguished based on the purpose of the intrusion: intelligence collection versus destruction. Exploitation "basically means gaining access to a machine for the purpose of collection. So you would have some type of software, malware, or implant installed on the machine" to monitor it, he said. Network attacks, on the other hand, also rely on gaining access but are aimed at destruction, such as "wiping a hard drive, destroying servers," or using a botnet to launch a denial of service attack. These types of network attacks are linked to military action or covert missions.

Most evidence so far points toward espionage. DarkMatter may have hired members of CyberPoint, with knowledge of code capable of infecting users through Twitter and other online platforms, to help.

"It is my understanding that ... there were some types of offensive activities that [CyberPoint International] couldn't or wouldn't do for the client and the client did not want to be told no so they sought to restructure in a way that a foreign company could not impede their efforts," one former employee said.

One thing is clear: The new arrangement led dozens of employees to leave the UAE rather than join DarkMatter. Several who opted out of the relationship cited concerns about the UAE's human rights record, including arbitrary detention and torture of activists and dissidents. One cited the issue with "free speech" as a particular sore point.

A bigger question, perhaps, is whether DarkMatter's use of American- developed hacking tools is even legal, since it may be covered by U.S. export regulations. According to the Washington Post, the State Department at one point granted CyberPoint permission to advise the UAE on cybersecurity. But two people who spoke with The Intercept questioned whether DarkMatter, which appears to have subsumed CyberPoint's earlier work in the UAE, would be covered by that license.

The world of cyber exports is a confusing one. Depending on what DarkMatter is actually doing, its sales might be regulated by multiple bodies of law. If the products involve cryptography technology, there may be some arms export restrictions -- while hacking tools and zero-days are not typically regulated that way, said Eva Galperin, a global policy analyst for the Electric Frontier Foundation and technology adviser for the Freedom of the Press Foundation. "If you want to sell surveillance malware from the UAE, nothing stops you," she said during a phone interview.

The United States, however, has attempted to regulate those types of "cyberweapons," and many U.S. officials wanted to tighten regulations in response to instances like Hacking Team's sale of surveillance tools to repressive regimes. Critics of those proposed regulations pointed out that such technologies could be used for legitimate purposes, like testing products for cybersecurity or penetration testing.

It's unclear, however, where DarkMatter's work may fall in terms of export law. If the work involving U.S.-origin technology or technical expertise involved cryptography, a license would be required from the U.S. State Department. According to Colby Goodman, director of the Security Assistance Monitor and an expert in International Traffic in Arms Regulations, any American employees working on regulated products would need some sort of export license, even if they moved overseas and started working for a foreign company. "If you were a UAE citizen, and I was telling you about something that was ITAR controlled," he explained, "that would be exporting it, unless I had a license."

"It's a similar concept with classified information," he continued. Just because you leave the country doesn't mean you forget the classified information -- and if you give it away, that's a violation.

The State Department declined to comment on whether an export license had been issued to cover DarkMatter or its employees, including those formerly from CyberPoint. The Commerce Department, which regulates some security equipment sales, did not respond to a request for comment.

DarkMatter, for its part, said it has obtained proper licenses, though it did not provide details.

"DarkMatter has provided its customers with technologies worth hundreds of millions of dollars, through its global security and technology vendors," Healy, the spokesperson, said. "A number of these contracts extend to highly sensitive security systems that DarkMatter has applied for and -- following the standard screening process -- been granted export control licenses from jurisdictions including the U.S. and various European countries."

At a crowded Las Vegas convention hall in August, representatives from DarkMatter were camped out in several large canopied stations, a short stroll from a vendor making hand-rolled cigars, several open bars, and a booth raffling off a robot dinosaur.

DarkMatter has started showing up in U.S. cybersecurity circles in recent months -- including at BlackHat USA, the massive annual security and hacking conference in Vegas, where it handed out swag to attendees, including pens and notebooks adorned with a DarkMatter insignia. A representative at the booth said the company was still busy recruiting.

In his July blog post describing his UAE interview, Margaritelli wrote that he hoped his account would "serve to warn those who, like me, might find themselves dragged into shady affairs, partially or completely unaware, as well as anyone pursuing job offers that entail moving to the UAE. Know that you would be giving up your privacy, and more importantly, your freedom of speech for money."

Not everyone I spoke with agreed with his view. French security researcher Matt Suiche, whose cybersecurity startup Comae Technologies is also based in the UAE, said that "every country does surveillance" and hiring foreign workers in the UAE was not unusual; the UAE was simply trying to establish its own technology base. "It's like the UAE Mars mission," he said.

Some of the former CyberPoint employees in the UAE said they didn't mind the surveillance work, treating it as an inevitable and natural path for a young modern nation facing legitimate threats. "I was impartial to the work I did," one former employee told me. For the UAE, the source said, using surveillance to track its own citizens has become normalized. He described himself as a "realist" though admitted he tried to minimize his "exposure to certain things" the company did.

"You can't blame the bag man for the job you gave them," he said.

In the lobby of a Vegas hotel during BlackHat, I spoke with Margaritelli about his frustrations with DarkMatter -- a Platinum sponsor at the event. He has all the trappings of a hacker from movies, including lip and nose piercings, rectangular glasses, and cigarettes. He avoids cellphones but finds other ways to communicate. He went to school for physics and engineering but never finished his degree. He has a very specific memory for numbers, network domains, addresses, and people. Though he says his English isn't very good, he can rapidly translate Italian text into colloquial English.

Margaritelli told me he started off wary of DarkMatter. He was familiar with the UAE government's reputation of locking up and disappearing dissidents and purchasing surveillance equipment from other countries. Plus, his interviewer -- a former employee of another controversial surveillance company, Verint -- seemed a little too interested in Bettercap, Margaritelli's well-known hacking tool.

While some researchers may argue that what DarkMatter is doing is simply par for the course in cybersecurity, Margaritelli said that the scale of the endeavor is unprecedented, creating a zombie hoard of infected devices, primed for hacking and surveillance. "In a near future, every single electronic device in the UAE will unwillingly be part of their state botnet," he said.

Later, in an email, Margaritelli wrote that he works with all sorts of hacking technologies, but he remains shocked by DarkMatter's ambitions to surveil an entire nation. "What they want to do," he wrote, "it's fucking insane."

The Pioneer
Cyber technology as potent terror tool in jihadi hands
Thursday, 27 October 2016

New Delhi - From its very inception in July 2014, the Islamic State in Iraq and Syria (ISIS)/Daesh utilised cyberspace for propaganda and recruitment in a manner that was both innovative and extremely hard to counter. There is an active digital jihadi group within the IS which has designed effective Android Apps, and used the comparatively secure end-to- end encrypted instant messaging app Telegram, (and to a lesser degree, WhatsApp) for propaganda, weapons procurement, and to direct and publicise lone wolf/wolf pack attacks. As entry into its communication networks is difficult, prevention and countering of such terrorist acts is one of the most challenging tasks confronting intelligence and law enforcement agencies.
The cyberjihadis (several groups such as the Cyber Caliphate, and three United Cyber Command have been identified) have proved their expertise on the dark web and have set up several websites for recruitment and tutorials on weapons-making, which can be entered only on invitation. The UCC has been able to hack (April 2016) into the Pentagon, the Department of Homeland Security, and several other federal agencies in the US, and has obtained data of around 43 personnel and put them on a so-called Kill List, which was circulated through a channel on the Telegram, Al Nashir. While the IS has not acted on the Kill List so far, the expertise of the hackers is cause for disquiet. Also, serious attempts have been made in the past one- and-a-half years to establish covert secure, encrypted financial networks.

The Paris (November 13, 2015) and Belgium (March 22, 2016) attacks underscored the danger of encrypted messaging. In both cases, security agencies were unable to get any advance information of the terrorist strikes, despite several perpetrators being on their watch-lists.

In September this year, an IS-affiliated group, Cyber Kahalifah, began to advertise the use of a lesser known technology, the ZeroNet, as the safest mode of communication. The Zero Net, which is in the public domain and can be downloaded free of charge from https.zeronet.io, is a web-hosting platform which decentralises the hosting of content and allows for asymmetric encryption of domain names and addresses.

It offers an unprecedented degree of anonymity. For instance, normally, a website is hosted at a server, and is allotted an IP address, or a series thereof. Users, identifiable by their own unique IP addresses, communicate and interact with the website by specifying the web address (url). Then, a DNS (Domain Name Server), directs the user to the IP address of the website the user wishes to access. Data can then be exchanged between the user and the website. The ZeroNet, on the other hand, can host a single website in a number of locations (for example, user computers), by leveraging Peer-to- Peer (P2P) networks, the most notable of which is BitTorrent.

In P2P networks, users (called peers) communicate and share data directly between one another, as opposed to communicating via a central server, as is the case with most websites. A server, called Tracker, connects peers to one another and handles requests for transfer(s) of data.

Other differentiators are that ZeroNet ensures the fidelity of the websites themselves is maintained through asymmetric two-way encryption. Authors of a website receive a private key, which enables only he/she to make changes to the website, while interested peers receive the public key (analogous to a website url) which allows them to access the site. This has two consequences: First, the entire build of the website remains on the author's computer, and not on any server; and second, there is guaranteed verification of the creator of the website and any files downloaded therefrom.

The ZeroNet also offers full Tor compatibility, which means that IP addresses can be masked, adding another layer of security. Moreover, ZeroNet claims that it can be used over non-Internet networks as well, such as Bluetooth, which would be a valuable enabler forjihadi networks. Finally, content can be distributed remarkably quickly, and very likely scales with the number of visitors and seeders of the site.

Cyber Kahalifah has set up a website on ZeroNet, which in late September gave calls for lone wolf attacks in various countries, and directed visitors to an application called 'Alrawi', designed by the IS, which works on Android platforms for logistic and monetary help. The IS's English online magazine, which had been called Dabiq, has been suspended and the group has brought out a replacement, Rumaiyah(Rome). The Rumaiyah contains explicit exhortations for violent action in the Dar ul-Harb and unsurprisingly has been posted on the ZeroNet.

Given the above backdrop, the use of ZeroNet by the Islamic State terror organisation and other terrorist groups is of great concern. With the IS facing international bludgeoning in Iraq and Syria, it is likely that it will lose Mosul and Aleppo sooner rather than later - and possibly Raqqa will follow. The exodus of foreign fighters from the region is now very evident, and the re-migration of a sizeable section to the Af-Pak region is a possibility.

The IS is attempting to establish itself in Afghanistan through its franchise, the Wilayat Khorasan, and has been able to attract some Indians there, notably the group of 21 young people from Kerala. One of them, Sajjer Mangalachari Abdullah, from Kozhikode, has now been identified as a key IS recruiter, and is reportedly functioning from Nangarhar in Afghanistan. Attempts to radicalise vulnerable sections are ongoing in India, and the National Investigation Agency has been able to intercept scores of such individuals. International jihadi inter-connectivity could result in the ZeroNet gaining traction in India through these networks.

From an Indian security standpoint, this is of particular concern: Local franchises of terrorist organisations with access to even meagre Internet resources, could increase the scale of propaganda and training content, and make prevention and anticipation of terror attacks a Herculean task. Agencies involved in monitoring and law enforcement need to urgently familiarise themselves with the working of ZeroNet, as jihadi groups have shown considerable fleet-footedness in adapting to technological challenges. The Indian state cannot afford to be out of sync on this issue.

The Australian
Reserve Bank fights off a new cyber attack every two seconds
Thursday, 27 October 2016
Byline: Daniel Palmer

Canberra - The Reserve Bank is fighting a war against cyber security threats, with potential hackers testing the resilience of its systems every two seconds, according to the central bank's technology chief. Sarv Girn, chief information officer at the RBA, told delegates at the Gartner Symposium on the Gold Coast that the central bank was withstanding a barrage of potential attacks.

"In this era, cyber security is an inherent dimension of operational resilience. It's something that can stop you in the race and needs more attention than ever before," he said. "We place a lot of importance in this so that appropriate defences can be established as the threats change." Mr Girn's presentation, which outlined the broad technological challenges confronting organisations, came eight months after hackers funnelled about $135 million from the Bangladeshi central bank. That scandal forced the departure of the bank's chief and was enabled by malware developed in North Korea and Pakistan.

The RBA is anxious to thwart such cyber security threats which have become commonplace hi-tech sectors.

"Our external perimeter, like most other organisations, is faced with a barrage of scans and probes; in fact we have one probe every two seconds," Mr Girn said.

"Metrics such as this serve to understand the risks to our environment so that pragmatic cost-effective mitigating controls can be established." The endeavours of hackers to gain access to RBA systems have led to a surge in suspicious emails, with around 70 per cent of the emails received by the RBA "malicious in nature".

It follows on from the moderate success of a phishing scam in November 2011 that saw six RBA staff click on a malicious link, although the issue was defused without the leaking of sensitive information.

The central bank was also hit by a denial of service attack in November 2013, with Indonesian hackers taking credit for the actions, which also impacted the Australian Federal Police.

Mr Girn said IT systems reliability had become increasingly vital, with any failure to protect core operations placing entire businesses at risk.

"Whilst attaining digital reliability has been a crucial need for many years, the impact and consequence of getting this wrong in today's economy can threaten the very viability of an organisation," he said."Your risk appetite statement has to recognise the risks ... and the extent to which they are acceptable."

Washington Free Beacon
Report: Chinese Spies Stole Pentagon Secrets
Thursday, 27 October 2016
Byline: Bill Gertz

Washington - Chinese spies repeatedly infiltrated U.S. national security agencies, including official email accounts, and stole U.S. secrets on Pentagon war plans for a future conflict with China, according to a forthcoming congressional commission report.
"The United States faces a large and growing threat to its national security from Chinese intelligence collection operations," states the late draft report of the U.S.-China Economic and Security Review Commission.

"Among the most serious threats are China's efforts at cyber and human infiltration of U.S. national security entities."

Chinese intelligence activities have "risen significantly" in the past 15 years and are conducted through several spy services, including the Ministry of State Security (MSS), the People's Liberation Army (PLA), and Communist Party military organizations such as the PLA General Political Department and the Party's United Front Work Department.

A copy of the draft annual report for 2016 was obtained by the Washington Free Beacon. The final report will be released Nov. 16.

The report identified repeated infiltrations by Chinese spies of U.S. national security entities, including the FBI and the U.S. Pacific Command.

Defense officials said one of the more damaging spy cases involved retired Lt. Col. Benjamin Pierce Bishop, a defense contractor at the U.S. Pacific Command, who pleaded guilty in March 2014 to supplying classified information to a Chinese woman he dated.

The compromised information included secret U.S. war plans, nuclear weapons and deployment information, secrets on the MQ-9 Reaper drone, and a classified report titled "The Department of Defense China Strategy."

Other Chinese human intelligence operations included the case in 2010 of James Fondren, a high-ranking Pacific Command official who passed a secret 2008 National Defense Strategy report to China; and Gregg Bergersen, who passed secrets to China until his arrest in 2008. Both were recruited by PLA spies.

In addition to targeting officials with access to secrets, Chinese intelligence is targeting American academics at think tanks involved in China studies and, in at least one case, an American student in China, Glenn Duffie Shriver.

"Chinese intelligence has repeatedly infiltrated U.S. national security entities and extracted information with serious consequences for U.S. national security, including information on the plans and operations of U.S. military forces and the designs of U.S. weapons and weapons systems," the report said.

"This information could erode U.S. military superiority by aiding China's military modernization and giving China insight into the operation of U.S. platforms and the operational approaches of U.S. forces to potential contingencies in the region."

Additionally, the report states that China cyber operations have targeted critical U.S. infrastructure, such as the electrical power grid and financial networks.

"U.S. critical infrastructure entities are a major target of Chinese cyber operations, and China is capable of significantly disrupting or damaging these entities," the report says.

Regarding intelligence targeting of American decision makers, the report noted that MSS hackers conducted the cyber attacks against the Office of Personnel Management last year involving the theft of records on 22 million federal employees.

In August, an FBI electronics technician, Kun Shan "Joey" Chun, pleaded guilty to acting as a Chinese agent after passing sensitive data to China about FBI surveillance technologies.

"Among the information extracted were 5.6 million fingerprints, some of which could be used to identify undercover U.S. government agents or to create duplicates of biometric data to obtain access to classified areas," the report said.

Chinese intelligence also hacked and infiltrated the personal email accounts of many Obama administration officials, the report said.

Chinese cyber espionage is carried out by what the report said was a "large, professionalized cyber espionage community."

"Chinese intelligence services have demonstrated broad capabilities to infiltrate a range of U.S. national security (as well as commercial) actors," the report says. "Units within the former 3PLA, in particular, have been responsible for a large number of cyber operations against U.S. actors."

Other targets of cyber attacks include U.S. diplomatic, economic, and defense industrial sectors involved in supporting American national defense programs. The data could be used to support Chinese military modernization, as well as provide Chinese Communist leaders with insights into U.S. leadership perspectives on key China issues.

Chinese military planners also would benefit from the intelligence activities by helping "build a picture of U.S. defense networks, logistics, and related military capabilities that could be exploited during a crisis."

China's government also uses unofficial spies to gather information.

"In addition to the cyber espionage elements of the MSS and PLA, many unofficial Chinese actors target the United States with cyber espionage operations," the report said.

"These actors include government contractors, independent 'patriotic hackers,' and criminal actors," the report added. "Distinguishing between the operations of official and other Chinese cyber actors is often difficult, as is determining how these groups interact with each other. Some reports suggest China is shifting cyber espionage missions away from unofficial actors to centralize and professionalize these operations within its intelligence services."

Spy targets include cyber intrusions of defense and military systems that are allowing China to spy on deployed U.S. military forces.

"Moreover, by infiltrating and attempting to infiltrate defense entities in U.S. ally and partner countries, China could affect U.S. alliance stability and indirectly extract sensitive U.S. national defense information," the report says.

The annual report also concludes that despite extensive ties between Beijing and Washington, "U.S.-China relations over the past year continued to be strained."

Among the causes of tensions are Chinese territorial claims in the South China Sea, U.S. arms sales to Taiwan, the deployment of missile defenses in South Korea, Chinese cyber attacks, and the U.S. "rebalance" to Asia.

Despite a September 2015 U.S.-China agreement not to conduct government-sponsored cyber economic espionage, "Chinese cyber espionage against a range of U.S. entities continued in 2016, to the detriment of U.S. economic and national security," the report said.

In a related development, an Agriculture Department geneticist pleaded guilty on Monday to making false statements to the FBI as part of an economic espionage case involving China.

Wengui Yan lied to FBI agents about plans by a group of Chinese tourists to steal U.S. genetically-modified rice samples, Reuters reported Wednesday.

Khaleej Times
BlackBerry's third Android phone - still 'world's most secure' - DTEK60 (Canada).
Thursday, 27 October 2016

Byline: Alvin R. Cabral

Dubai - BlackBerry has apparently thrown in the towel on its smartphone business. But apparently, they're taking it back.
The Canadian company, its devices once revered as the choice for professionals, is back at it with its third Android phone, the DTEK60.

BlackBerry's newest offering - its third running Google's operating system following the Priv and DTEK50 - once again comes with the promise of being the "world's most secure Android phone".

Well, every essential aspect is has obviously been ramped up: bigger screen, better CPU, higher RAM, double the storage, souped-up camera and longer battery life. Heck, its screen resolution is even higher than both the iPhone 7 and Google Pixel.

BlackBerry has announced that it is concentrating on its other core business, which is the enterprise. What remains to be seen is how long they'll continue dishing out new devices.

But, matter of factly, there are still BlackBerry loyalists. And they'll be thrilled that - despite the fact that BlackBerry says it's not giving up on its own OS - the company is going with the operating system of choice for almost 88 per cent of users.

Press TV
Iran unveils long-range, radar-evading drone
Thursday, 27 October 2016

Tehran - Iran has unveiled a new light-weight, long-range stealth unmanned aerial vehicle (UAV) capable of flying at a maximum altitude of 10, 000 feet.
The drone was put on show on Wednesday at an expo showcasing the latest achievements by the Iranian Aviation & Space Industries Association.

Hamed Sa'eedi, an official with the association, said that, with a total weight of less than 20 kilograms and a flight time of over 15 hours, the drone can conduct such non-military missions as those for mapping, filming and image-collecting. He said that Iran plans to export the drone to different countries.

Earlier this month, Iran's Islamic Revolution Guards Corps (IRGC) unveiled a new attack drone, the Saegheh (Thunderbolt), by reverse-engineering a US Central Intelligence Agency RQ- 170 Sentinel drone that had been captured in December 2011.

In recent years, Iran has made major breakthroughs in its defense sector and attained self-sufficiency in producing important military equipment and systems.

The Islamic Republic maintains that its military might poses no threat to other countries, stating that its defense doctrine is merely based on deterrence.

The Daily Beast
The U.S. Cyber War With Russia Will Wait for President Hillary Clinton
Thursday, 27 October 2016
Byline: Shane Harris, Nancy A. Youssef

Washington - After U.S. intelligence agencies and the Homeland Security Department publicly blamed Russia for a campaign of cyber espionage designed to interfere with the presidential election, the Obama administration promised a response "to protect [the country's] interests at a time and place of our choosing."
But that response seems unlikely to come before Election Day. The question of how to retaliate for Russia's unprecedented meddling in the U.S. political system has been the subject of meetings among national security officials, but as of now those plans are still being worked out, according to four officials knowledgeable about the deliberations.

Rather, the administration is likely to work in concert with the president-elect to fashion a response, one official said, like the others speaking on condition of anonymity to discuss sensitive internal deliberations. It would, after all, fall to that new commander-in-chief to deal with the repercussions or retaliating against Russia.

If polls are predictive, that person is likely to be Hillary Clinton, who is sure to have her own thoughts on how to respond to an espionage campaign that was partly designed to undermine her candidacy. Handing her a cyber campaign in progress--without her input--wouldn't be that wise. Nor would dumping an ongoing cyber war in President Donald Trump's lap be the brightest idea considering he has consistently denied any link between the hackers and the Kremlin, despite 17 intelligence agencies' claims to the contrary.

In an interview, Rep. Adam Schiff, the top Democrat on the House Intelligence Committee, said that he was not aware of the administration's plans for responding to Russia or how it might coordinate with the president-elect. But he urged the White House to hold its fire until after Nov. 8.

"I wouldn't want to take any step that might provoke [Russia] into a further escalation," Schiff told The Daily Beast. That escalation, he said, would likely consist of Russia posting of forged emails or documents online that couldn't be easily refuted in the runup to the vote.

"I don't think we want to take any steps in the next two weeks to provoke that response," said Schiff, who added that the ultimate decision should be made soon after the elections are decided. "It's not something I would want to see drag out too long."

With Trump alleging that the election has been "rigged" against him, officials and experts fear that voters could be misled by false information. This so-called disinformation campaign may have already begun. Earlier this month, the person, or people, going by the name Guccifer 2.0 posted documents said to have been stolen from the Clinton Foundation, but officials there said the files weren't theirs. And Clinton campaign staff have refused to verify the authenticity of some emails purportedly stolen from the account of John Podesta, the campaign chairman.

In an interview with NBC News, Vice President Joe Biden said the U.S. is "sending a message" to Russian President Vladimir Putin that there will be consequences for his country's actions.

"He'll know it," Biden said. "And it will be at the time of our choosing. And under the circumstances that have the greatest impact."

But there are no indications that the United States has taken any response, overt or covert.

Officials emphasized that Obama is not checking out early or shoving his problems off on his successor. Rather he is giving the next president a chance to gradually adjust to the role of commander-in- chief, at a time when the world that doesn't stop for a peaceful transfer of power.

For the candidates' part, Trump has said he would seek to repair deteriorating relations with Russia. And given that he doesn't share the intelligence community's view about the hacks, he would be unlikely to pursue punitive sanctions or other measures.

Clinton, on the other hand, has signaled a far tougher stance toward the Kremlin. Earlier this week, one of her advisers wrote a column spelling out a more aggressive Russia policy.

It is neither unprecedented nor particularly unusual for a serving president to consult with his successor. And that doesn't shield him from the political implications of any decision.

"If the policy doesn't turn out well, Obama would still be responsible," said Lawrence Korb, a senior fellow at the Center for American Progress and a senior adviser to the Center for Defense Information, who has worked on political transition teams.

Past U.S. presidents have maneuvered the murky period between the election to Inauguration Day with mixed results. One month after the 1992 election, George H.W. Bush ordered 28,000 troops into Somalia as part of a humanitarian mission, even as he left the exit strategy to his successor, Bill Clinton.

Nine months after Clinton took office, 19 U.S. troops died during the Battle of Mogadishu, and with that U.S. support of the effort there quickly became unpopular. Clinton ordered U.S. troops to withdraw in March 1994.

Four months before the end of the Clinton administration, the USS Cole was attacked, killing 17 sailors. Some critics charged that the lack of a forceful response by Clinton, and subsequently by the George W. Bush administration, emboldened al Qaeda, which attacked the United States less than a year later, on Sept. 11, 2001.

President Carter communicated with his successor, President Reagan, about efforts to free U.S. hostages from Iran, which notably happened the moment Reagan took the oath of office Jan. 20, 1981.

More recently, both presidential candidates in the 2008 race said they supported President George W. Bush and economic bailout plan in October of that year. The effects of the bailout, and the economic crisis that emerged from that period, fell to Obama to address throughout much of his presidency.

Addressing the question of what to do about Russian hacking, Schiff, the intelligence committee member, said decisions of such great consequence ought not to be made without regard to who has to deal with them.

"It makes all the sense in the world to coordinate that response with the president who's not only going to have to see it though but deal with the repercussions," Schiff said.

The Independent (UK)
EU security intelligence critical to fighting terror, says senior police officer
Thursday, 27 October 2016
Byline: Ashley Cowburn

London - Access to information in Europe-wide security databases, including the European Arrest Warrant, is "mission critical" in fighting terrorism, one of Britain's most senior policewomen has said. Helen Ball, the deputy assistant commissioner at the Metropolitan Police, also indicated that citizens in Europe would be at a greater threat from terrorism if Britain failed to work with its allies on the continent after Brexit. Ms Ball, who has been with the police force for over two decades, also ranked the European Arrest Warrant as ten out of ten in combating international terrorism.
When asked by the Lords' EU Home Affairs sub-committee about the importance of the European Arrest Warrant (EAW) on a scale of 1-10, Ms Ball replied: "At the moment we have very low usage of the European Arrest Warrant and there are very good reasons for that and as I look to the future I suspect we will have greater use of it. "So if I must answer your number question, I'd probably say on low usage at the moment about an eight... and if I'm looking to the future I think it's a 10. We must not be in a position where a terrorist can think, 'okay, there is a safe haven where it's going to take a very long time to be extradited and come to meet justice.'" She added if the European Arrest warrant was not to go forward, she would expect a replacement to bring "justice swiftly".

In 2015 alone European countries made almost 13,000 arrest requests for individuals in the UK using the warrant, including 320 on alleged terror related offences, 433 for murder and manslaughter and 191 for

rape. In the same year the UK used the EAW to make 228 requests for arrest from other EU countries, including four on terror charges, 19 for murder and manslaughter and 20 for rape.

Speaking to peers on the committee, she added: "I think the way that terrorists are currently operating and the way I see them operating in the future that means we have an enormous amount to lose from diminishing our ability to work with European police forces and to share our intelligence with them. We are all safer because we can work together across Europe and share information with each other - that genuinely is helping to keep citizens of Europe safe."

Ms Ball also emphasised the importance of Europol, the EU's law enforcement agency. Last week the National Crime Agency's David Armond warned an "immediate" and urgent decision is needed on Britain's membership of the organization or the UK would be forced out. The Home Office said a decision would be made in "due course". The senior counter terrorism official added access to Europe-wide security databases "is mission critical in protecting both the citizens of the UK and citizens of Europe that the UK policing effort is able to access that information

"I'm not going to say it has to be through a particular formal mechanism, that's for the negotiations to decide," she added.

Bloomberg View
How the Kremlin Handles Hacks: Deny, Deny, Deny
Wednesday, 26 October 2016
Byline: Leonid Bershidsky

Column - The U.S. presidential election has made "Russian hackers" a powerful brand. There is, however, another that surpasses it: Ukrainian hackers. And the story of their most recent hack contains valuable lessons for U.S. politicians, particularly Hillary Clinton and the Democrats.
A Ukrainian hacker collective calling itself CyberHunta -- a mocking reference to Russian propaganda outlets' moniker for the Kiev government, the junta -- claimed on Oct. 23 to have broken into an electronic mailbox that belongs to Vladislav Surkov, President Vladimir Putin's adviser for dealing with former Soviet breakaway regions. The purported hacked e-mails supposedly contain sensitive information, including, for example, a lengthy plan of "urgent measures for the destabilization of the situation in Ukraine."

Unlike Clinton's allies after their e-mails were published, the Kremlin immediately denied the authenticity of the leaked communications. Putin's press secretary, Dmitri Peskov, told reporters that Surkov didn't use e-mail, so those who claim to have broken into has mailbox "must have had to sweat quite a lot" to forge messages.

Peskov's denials have been refuted. The Atlantic Council's Digital Forensic Research Lab explained that the hackers' proof -- a large Microsoft Outlook data file -- contained header information for 2,237

messages, which would have required an impossible amount of sweat to forge. Besides, like any normal mailbox -- that of Clinton aide John Podesta, for example -- prm_surkova@gov.ru received plenty of routine and spam messages. They were all in the Ukrainian data dump, and they were consistent with those other Moscow recipients got at the same time.

The denial, however, precluded journalists from asking the Kremlin about the stolen e-mails again, and it cast just enough doubt on the Ukrainian feat to make the story a little less newsworthy. The Democrats could have said the WikiLeaks e-mails were forged or doctored -- and no one could have proved otherwise.

Besides, there was a grain of truth in the denial, which contains an even more important tip for the Democrats. The cautious Surkov, indeed, doesn't send or receive messages himself; he is known to always correspond through intermediaries, sometimes asking them to reply to an e- mail, sometimes calling a correspondent on the phone. The prm_surkova@gov.ru mailbox was checked by two women, presumably Surkov's assistants. No outgoing e-mails were directly from him.

This is a rather secure way to conduct one's affairs. Surkov doesn't even have to use encryption: His involvement in a matter cannot be proved by any kind of electronic trail. If people send documents to his office, it's their affair, not his.

Here's an example described by the Atlantic Council's Digital Forensic Research Lab. A Moscow magazine editor sent an "open letter from the residents of the Donbass" to a government official for approval and editing. The bureaucrat sent it on to Surkov's office. It's not clear whether Surkov saw or edited it, but a few days later the magazine published a slightly altered version of the "letter."

It's not clear what Surkov thought of the plan to destabilize Ukraine, sent to him by Pavel Karpov, alias Nikolai Pavlov, a Muscovite without an official government position who has often been seen in one of the rebel-held cities -- Luhansk -- coordinating the activities of pro-Russian forces. The plan called for infiltrating the Ukrainian parliament and civil society groups, providing anti-corruption activists with evidence of the misdeeds of President Petro Poroshenko and his allies.

So what if Karpov sent this document to Surkov? He might have spammed the entire Russian government with it. So what if a leader of the separatist Donetsk People's Republic sent financial plans and casualty lists to prm_surkova@gov.ru? It's known that the separatists want Moscow's support, but there's no evidence Surkov reacted to the messages. So what if a wealthy ultranationalist, Konstantin Malofeev, who is suspected of financing Russian volunteer units that backed the pro-Moscow rebellion in eastern Ukraine, sent his proposed candidacies for the separatist "republics'" leadership to the address?

As things stand, the Ukrainian hackers, though they executed an admirable deed -- Russian government communications are better protected than those of the U.S. Democrats -- did not obtain any direct evidence of Surkov's personal involvement in the running of the separatist regions or the disruption of

Ukrainian political life. There were no e-mails from Russian officials with formal roles in the government or on the presidential staff that would shed light on their role in the conflict. All kinds of freelancers and fringe characters wrote them - - but what does that prove?

The degree of Russia's involvement in eastern Ukraine is well-known, yet no one has evidence of specific Putin aides giving any incriminating orders.

It's a cynical but effective way to play the game if you believe you'll be hacked at some point -- and if your e- mails are of interest to a hostile party, you probably will be. I understand if the Democrats don't want to act the way Putin's people do: It may seem dishonest and distasteful. But it's less naive than their strategy of blaming Russia for everything that is revealed about them. They have only themselves to blame for not giving enough thought to security.

International Business Times (UK)
WikiLeaks 'sowing the seeds of its own destruction' says former NSA chief
Wednesday, 26 October 2016
Byline: James Murdock

London - A former deputy director of the US National Security Agency (NSA), John C Inglis, believes that WikiLeaks - the whistleblowing platform led by Julian Assange - has become "internally confused" in recent years and that "natural forces" may soon wipe it out.
"WikiLeaks might be in fact be sowing the seeds of its own destruction," Inglis told IBTimes UK in an exclusive interview on 25 October, indicating the organisation has overstepped a boundary by leaking material which has the potential to influence the upcoming US presidential election.

The most recent publication has revolved around the personal emails of John Podesta, a close aide to Democratic candidate Hillary Clinton. At the time of writing, WikiLeaks has disclosed well over 30,000 documents and attachments in nearly 20 separate releases.

The US government has namechecked Assange's organisation as being complicit in a Russian-led plot to influence the elections and - allegedly after a close word from US Secretary of State John Kerry - the government of Ecuador, which is hosting Assange under political asylum, was forced to step in.

"My sense is that when Ecuador shuts down the internet access of Julian Assange - they say we are no longer comfortable with what you do - it might be that WikiLeaks has lost its way," Inglis said. "Not that I agreed with what it was doing in the first place.

"I think that from a distance, over time, they have become somewhat internally confused and I'm not sure we need to kick that house over. Maybe in the fullness of time, natural forces will cause it to deteriorate and not be as interesting or as influential as it once was."

WikiLeaks and the US government have a long and strained history. Over the years, after being sent documents by whistleblowers, WikiLeaks has published US diplomatic cables, Iraq War military logs and classified files relating to the Guantánamo Bay prison camp in Cuba. In 2015, US law enforcement confirmed an "active and ongoing" investigation into the group.

Yet Inglis, who served at the NSA for 28 years, said all governments should tread carefully in any prosecution of the group and that they "need to make sure they don't become part of the problem."

He added: "If what you decry is a lack of principal or inappropriate behaviour on the part of some entity - maybe it's WikiLeaks - you can't in responding to that commit the same sin."

There have been a number of revelations gleaned from the Podesta emails so far, including unprecedented insight into Hillary Clinton's speeches to private banking giants, files showing her relationship with Wall Street and emails detailing how Qatar and Saudi Arabia were allegedly offering "clandestine" funding to the Islamic State (Isis).

Tribune de Genève
« Nous vivons l'âge d'or de la surveillance »
Thursday, 27 October 2016
Byline: Olivier Bot

Moscou - Dans un entretien virtuel, le lanceur d'alerte Edward Snowden estime que le droit à la vie privée est toujours menacé par l'Etat
« Les sociétés les plus connectées ont plus à craindre de la surveillance globale que d'un pays comme la Corée du Nord. » Depuis la Russie, où il a obtenu l'asile jusqu'en 2017, le lanceur d'alerte Edward Snowden a participé mardi à une discussion virtuelle programmée par le Global Editors Network et le quotidien allemand Süddeutsche Zeitung, dans le cadre d'un atelier sur les nouvelles formes de journalisme d'enquête. Celui qui révéla le programme « Prism » de surveillance électronique mondiale s'inquiète toujours des atteintes à la vie privée et à la liberté des citoyens grâce à l'interconnexion des données. « La NSA est à l'intersection de nombreuses sources de données, téléphone, Internet, e-mail. Cela devient terrifiant. Nous vivons l'âge d'or de la surveillance » , lance l'ex- consultant technique de la NSA et de la CIA entre 2007 et 2009 à Genève.

« Au nom de la lutte antiterroriste, AT&T a vendu des milliards de données au gouvernement depuis le 10 juillet 2008. Coïncidence, c'est la date du « Foreign Intelligence Surveillance Act » , qui autorise l'espionnage des étrangers hors des Etats-Unis » , pointe Edward Snowden. « Il n'était plus nécessaire d'avoir l'autorisationd'un juge comme auparavant. Les compagnies ont fait payer l'accès permanent aux données confidentielles. C'était légal. »

Depuis les révélations sur le programme d'écoutes des Etats-Unis, des lois étendant les pouvoirs des agences de renseignements ont été adoptées en Suisse, en Allemagne et en France. « La surveillance des

citoyens européens a augmenté » , constate le lanceur d'alerte. L'Américain, qui risque trente ans de prison aux Etats-Unis sur la base d'une loi sur l'espionnage datant de 1917, a évoqué deux catégories de citoyens particulièrement visés par la surveillance d'Etat: les activistes et les journalistes. Concernant la presse et le data-journalisme, Snowden suggère qu' « une bibliothèque qui sécuriserait les données sensibles soit accessible, au nom de l'intérêt public, aux enquêtes citoyennes et aux journalistes » .

Interrogé pour finir sur sa situation personnelle, il se réjouit qu' « une majorité au Parlement européen ait voté l'an dernier pour (sa) demande d'asile en refusant toute extradition » . Il salue aussi « la demande européenne d'une meilleure protection des lanceurs d'alerte » .

Bangkok Post
Public hearing on cybersecurity bills set for December
Friday, 28 October 2016
Byline: Komsan Tortermvasana

Bangkok - The first public hearing on the cybersecurity and data privacy draft bills, the most critical component for a bill passage, is scheduled to take place in December after almost six months of delay. The public hearing process is expected to be completed within this year. The two draft bills are expected to take effect by 2017.

If the bills pass the hearings, they are then submitted to the National Legislative Assembly (NLA) for approval, said ACM Prajin Juntong, acting minister of the Digital Economy (DE) and Society.

The bills will address both data privacy and data security to ensure organisations take greater responsibility for cybersecurity and support the digital ecosystem.

ACM Prajin admitted the two draft bills are being closely watched by critics who have expressed concerns over the benefits of using digital service, e-business and state measures governing data security protection. "We [the government] will try our best to serve the public interest," he said.

The government is pushing up processes implementing the digital economy-related laws in a drive to complement the development of the country's digital economy.

There are eight draft bills related to digital economy laws that need to be approved by the NLA to accomplish the implementation of the country's digital economy roadmap.

As of now, however, the government can enforce only a draft bill related to the establishment of the DE Ministry, which was announced in the Royal Gazette last month.

Surangkana Wayuparb, chief executive of the Electronic Transactions Development Agency (ETDA), said the draft bill promoting the digital economy will be submitted to the NLA this month and is expected to take effect by year-end.

The Digital Economy Promotion draft bill will enable the establishment of the National Economy and Society Development committee and the establishment of the Digital Economy and Society Development fund, she said.

The draft of the new National Broadcasting Telecommunications Commission (NBTC) law is being revised by a committee of the NLA before submission to Assembly members for voting, while the amended Computer Crime Act (CCA) draft bill is under hearing.

Mrs Surangkana said the first public hearing of CCA draft bill was made on Sept 30, with the second hearing scheduled for next month.

Last week, critics complained the recent draft amendment of the CCA at a public forum fails to prevent wrongful interpretations and applications of the law.

The main problem with the amended CCA is that its definition of "offences" under Section 14 is too broad, which could lead to abuse. The CCA has proven a powerful tool to silence human rights defenders reporting alleged abuse, as well as activists who exercise free speech.

The problem has not been solved in the latest draft, despite repeated calls from rights bodies such as Amnesty International and the Thai Netizen Network to address this.

Saudi Gazette
Ransomware a war to continue in the future
Friday, 28 October 2016
Byline: Layan Damanhouri

Riyadh - An estimated EUR 1.35 million in just 9 weeks were prevented from being stolen by cyber criminals after several organizations collaborated to create the No More Ransom project this year. "It's the first time where the private sector, law enforcement, and governments collaborate to fight ransomware together," IntelSecurity's Europe, Middle East and Africa CTO Raj Samani told Saudi Gazette.

IntelSecurity joined forces with Dutch National Police, Europol, Intel Security and Kaspersky Lab as well as law enforcement agencies from 13 countries to help victims of ransomware.

Ransomware is a growing issue where one new threat arises every 6 seconds. Samani says, "Cyber criminals are making good money. Organized criminals are capable of stealing millions of dollars from companies and banks all across the world."

He adds, "It's a war that's going to continue in the future. This is the evolution of crime. People don't rob banks with guns anymore. They rob it with USB sticks and malware."

Criminals no longer need to physically steal bags of money. In addition, the type of threat will be different than the previous one and criminals will have different targets, mainly consumers.

Most countries in the No Ransomware Program are European countries and more countries are expected to join in the coming months.

On Saudi Arabia, Samani says: "Saudi Arabia is certainly targeted but not necessarily higher than other countries. However, Saudi Arabia is an economy dependent on physical resources. There's a dependency on systems that manage and protect these environments. Saudi Arabia is dependent on the security both digitally and physically of their assets."

Asked about the awareness of business leaders to adopt security and IT strategies, Samani says awareness is growing. "We're briefing major governments, leaders. It's raised its profile from what it was two years ago and it has to."

He adds, "Technology is integral to every organization across the world. Ensuring that individuals, consumers, governments, can trust those systems is the most important element. You need to make sure you have the right level of protection. Consequences can lead to a company losing up to hundreds of thousands of customers."

Postmedia News
EQAO test glitch traced to cyber attack
Friday, 28 October 2016
Byline: Deborah Van Brank

Ottawa - The massive failure of last Thursday's online literacy test for Grade 10 students in Ontario has been traced to an intentional cyber attack.
The Education Quality and Accountability Office (EQAO) on Monday called the technical issues "an intentional, malicious and sustained Distributed Denial of Service (DDoS) attack -- a type of cyber attack."

It says a large volume of traffic from IP addresses around the globe was targeted at the network hosts of the test, with the intent of blocking school boards' and schools' and students' use of the server.

EQAO said it is looking at ways of ensuring there is no repeat.

A day after the EQAO testing, a similar DDOS attack took place aimed at several other servers and websites around the world and temporarily knocked out several sites, including Twitter.

Quick facts about the EQAO Grade 10 literacy test:

900 Ontario high schools participated - or tried to -- in the Oct. 20 online test

March, 2017, test would be mandatory for those who didn't write the October one) but most schools and school boards did so.

about 8 a.m. Thursday the traffic to the EQAO's server wasn't coming from schools or school boards. Instead, traffic volume overwhelmingly came from outside the system, which blocked legitimate users from logging in.

will score the tests that some students were able to complete. information was compromised during the attack.

Los Angeles Times
Putin denies hacking claims; Allegations that Russia is meddling in U.S. election are 'utter nonsense,' he says.
Friday, 28 October 2016
Byline: Mansur Mirovalev

Moscow - Russian President Vladimir Putin on Thursday vehemently rejected claims that Moscow is tampering with the U.S. presidential election, and said it was "utter nonsense" that the Kremlin favors Republican Donald Trump.
At the same time, Putin had kind words for Trump, saying that "he chose his method of getting through to voters' hearts."

This month, the White House accused the Kremlin of masterminding cyberattacks on the Democratic National Committee and leaking stolen emails. Democratic nominee Hillary Clinton has called Trump a puppet of Putin's.

The Kremlin has denied the accusations, and Putin called them a ploy to divert public attention from issues such as gun violence or the United States' growing debt.

Presidential hopefuls "apparently have nothing to say, so it's much simpler to distract people with presumed Russian hackers, spies and agents of influence and so on," he said in televised remarks at a gathering in the Black Sea city of Sochi.

"Does anybody seriously think that Russia can somehow influence the opinion of the American people? Is America some banana country? America is a great power," Putin said.

In praising Trump, he said: "He, of course, acts extravagantly, we all see that, but, I think, it's not that meaningless."

The Russian president was speaking at an annual forum of international foreign policy experts.

Putin used the opportunity to sharply criticize the Obama administration over its military involvement in Syria, and to call for a new Marshall Plan to rebuild the Middle East.

"The colossal scope of destruction requires development of a long-term and comprehensive program, a Marshall Plan of sorts, to revive the region torn by wars and conflicts," Putin said. He was referring to the U.S. program of financial and technical support to rebuild Western Europe after World War II.

Before its collapse in 1991, the Soviet Union showered Middle Eastern nations that sympathized with communist or socialist doctrine with aid projects that included construction of dams, export of technologies -- and a supply of Soviet-made weapons at discounted prices or free of charge.

Under Putin, Russia has sought to reclaim its Soviet-era clout in the region. Its major allies are Syria and Iran, but Sunni Arab nations have been alienated by Moscow's support for primarily Shiite countries.

A cease-fire Washington and Moscow brokered in Syria collapsed in September, and the Pentagon suspended its military cooperation with Russia, accusing it of targeting civilians in besieged Aleppo.

Putin claimed the cease-fire fell apart because of Washington's inability to distinguish between moderate opposition and radical jihadists, including Islamic State's allies.

"It's a fact," Putin said resolutely. Instead of distinguishing between "the healthy part of the opposition" and radical groups such as Al Nusra Front, "our American partners ruined the truce," he said.

Russia has decades-long ties to Syria, and Moscow saved President Bashar Assad's government by starting massive airstrikes on his opponents in September last year and helping his troops regain some key areas, including the ancient city of Palmyra.

Politico
States unprepared for Election Day cyber attack
Friday, 28 October 2016
Byline: Daniel Samuelsohn

Washington - State election officials around the country are woefully unprepared for a cyber disruption around Election Day.
While states have spent years thinking about and planning for other types of crisis that can mess with voting -- from hurricanes to power blackouts and terrorist attacks -- they've been slow and ill staffed to develop contingency plans responsive to a hack attack that would adequately protect their systems in time for the 2016 presidential election.

"They're waking up to it, but they largely don't know what questions to ask," said Jeremy Epstein, a senior computer scientist at the nonprofit research center SRI International and an expert on voting mechanics.

A dozen battleground state officials surveyed by POLITICO insist the voting systems themselves are safe, as nearly all parts of the balloting process take place in a secure, offline environment. But they also repeatedly acknowledged there are limits to what they can control, and they recognize they face legitimate challenges from cyber intrusions to the myriad adjacent parts that go into an election, including online registration records and publicizing vote tallies.

While any manipulation of a state's official election results is seen as unlikely, there's little denying that an Internet disruption or hack could cause significant confusion and chaos on Election Day, a dark conclusion to an ugly election plagued by accusations of Russian cyber espionage and evidence-less allegations of vote tampering and rigging.

Just last week, hackers temporarily froze a sizable chunk of the internet, a worst-case scenario that would cause serious problems around the country if duplicated on Nov. 8 -- the day more than 100 million Americans are going to the polls.

A major cyberattack would leave the states on their heels as they sign in registered voters, and it would impede their work later in the day as they try to report results. Then there are the effects of an internet shutdown on voters themselves, who in many instances would be left without an integral way to look up their polling places, do last-minute research on candidates or simply track which candidate is winning.

"Certainly if Internet access in the state is down totally that's a pretty substantial issue," said Edgardo Cortes, the commissioner of the Virginia Department of Elections, which earlier this month had to deal with its online voter registration system crashing just ahead of a key deadline.

"If something like that happens, how we react to it is going to have a lot to do with the public and press having confidence" in the election, added Georgia Secretary of State Brian Kemp.

Kemp, a Republican, said he has been printing out news reports to study last Friday's DDoS attack. That strike led to disrupted service across large parts of the country on about 80 major websites, including Twitter, Spotify and The New York Times. While declining to discuss many of the details behind Georgia's contingency planning, Kemp explained that he'll have his state police on standby and he could get additional resources if the governor was forced to declare an emergency. He also said he'll be reaching out to state and local officials to make sure they've thought through the full breath of what could happen in a cyberattack.

"I'm going to double check this morning for the third time in the last three weeks to ensure there's nothing else we need to do," he said.

Federal, state and local officials have had practice dealing with the unexpected, though to this point there's been little of substance to test them on the cyber front right around a general election. New York had to postpone a primary that was scheduled to take place the same day as the Sept. 11, 2001 terrorist attacks, and Hurricane Sandy in 2012 required the relocation of more than 250 polling places in

New York and New Jersey and an extension on the deadlines for requesting and receiving absentee ballots.

But a post-Sandy assessment of contingency planning -- convened by the National Association of Secretaries of State -- didn't broach the threats from a cyberattack, and many state officials involved in the 2016 election said they'll be tested in the moment if they face a significant attempt to mess with their systems.

"At that point, we'd go to the law books," said Arizona Secretary of State Michele Reagan, whose state was forced to shutter its voter registration system for a week earlier this year after being targeted by suspected Russian hackers.

In Utah, Lt. Gov. Spencer Cox said in an interview he would have "wiggle room" to bring in the state legislature for a special session if an emergency comes up on the cyber front that he's not equipped to handle under current law.

"We'd need 24 hours, but we could do it very quickly," he said.

Federal agencies have also been scrambling since the summer to help state and local officials prepare emergency plans for the 2016 election, including via an added emphasis on cyber risks. Breaches earlier this summer to the voter registration databases in Illinois and Arizona prompted the FBI to issue a nationwide alert to the other states. The Homeland Security Department has also gotten requests from 42 states seeking help shoring up their cyber hygiene practices and assessing their online vulnerabilities.

The Election Assistance Commission, an independent agency created in the wake of the 2000 presidential election debacle, has also been providing state and local officials with reminders relevant to a computer hack, including collecting emergency contact information ahead of time for major media outlets, election staff, utility companies, maintenance workers, polling place site owners and the attorneys and judges who would be needed in a pinch for court orders to extend voting hours or for other emergency moves.

Thomas Hicks, the EAC commissioner, said in an interview he's urging the states to reexamine their own policies to take into account how prepped they are for newer risks like cyberattacks. "Things we looked at 20 years ago in terms of threats are not the same as the threats are for today," he said.

Many of the states contacted by POLITICO explained that their primary focus when planning for election chaos had involved natural disasters, blackouts and, since 2001, the threat of a domestic terrorist attacks. But they have also begun adapting their contingency plans to take into account disruptions to the internet, including losing power and telephone services. That's meant stocking up on back-up paper ballots if their computerized machines break down. They have provisional ballots in case registration lists have been tampered with. And they're making paper printouts of the key information they'll need about polling place locations and post-election audit procedures.

"The worst case scenario is making everyone register again," said Matthew Dunlap, the Democratic secretary of State in Maine. "We could do it. It'd be an enormous undertaking. That's how fail safe our system is that you can't shut down our election."

If some kind of outside event did force a change in the voting process, Dunlap said state and local officials would have to act fast in launching a public awareness campaign. "Like what happens if there's a tsunami," he said.

Several state officials said they've made recent adjustments to their policies to take into account some of the lessons learned from Sandy in 2012. In many states, that's led to changes to the law so emergency workers can now cast absentee or online ballots if they're put into service on Election Day and miss out on a chance to vote in person. They're also requesting IT staff be on call from other state agencies. And in the event that registration rolls have been tampered with, voters will be required to sign affidavits when filling out provisional ballots. It'll be time consuming, and could lead to longer waits, but the aim is to let voters participate so long as they're in the line by a pre-established deadline.

"If a line builds up we don't turn anyone away," said Iowa Secretary of State Paul Pate.

Pate, a Republican, said Iowa officials had a chance to test their backup systems recently after a phone outage at the capitol complex in Des Moines. He also said the state won't post election results online until around 9 p.m. local time on Election Day, and it would make adjustments if the state faced any significant problems accessing the internet.

"If we sense something is going on like that, we'll turn our system off," Pate said.

Like many other state officials, Pate maintained that his election system was safe from being hacked because most parts of the balloting process were not connected to the internet.

But many computer scientists say that fails to account for the many parts of the election process that do remain susceptible to cyberattack.

James Scott, a senior fellow at the Institute for Critical Infrastructure Technology, said the states face an inevitable challenge because they don't have anywhere close to the budget or personnel expertise to deal with the many threats they face. "It's interesting to hear state officials say that it is" safe from a cyberattack, he said. "It kind of shows how unqualified they are for their positions in the digital age."

New York Times
Ukrainian Hackers Release Emails Tying Russia to Uprising
Friday, 28 October 2016
Byline: Andrew E. Kramer

Moscow - A group of Ukrainian hackers has released what it says are the emails of a senior Kremlin official that show a direct Russian role in creating and directing the rebel uprising in eastern Ukraine in 2014.
The group claimed to have hacked the account of Vladislav Y. Surkov, for years President Vladimir V. Putin's chief domestic political adviser and now the top official overseeing Russia's Ukraine policy.

The group released what it says are thousands of letters to and from Mr. Surkov's office email account, adding a fat dossier to this year's vast spill of emails around the world and showing high-level Kremlin meddling in Ukraine.

While the authenticity of the documents has yet to be fully established, several of the people who corresponded with Mr. Surkov confirmed that the messages of theirs released by the hackers were the ones they sent.

In a telephone interview, Yevgeny A. Chichvarkin, a Russian entrepreneur living in exile in London, confirmed the authenticity of his emails to Mr. Surkov's aides. "Yes, this is my original text," he said.

The Atlantic Council, a Washington think tank, analyzed the emails and determined they were genuine, based partly on the routing information.

The Kremlin's spokesman, Dmitri S. Peskov, flatly denied that emails had been leaked, saying somebody "must have had to sweat quite a lot" to forge so many messages.

Mr. Peskov also said that Mr. Surkov does not use email. And, in fact, only aides to Mr. Surkov answered the correspondence, leaving the extent of his personal involvement unclear.

While Russia's hand in Ukraine has hardly been a secret, the emails, if genuine, provide fine-grained detail of Mr. Surkov's office in setting up separatist enclaves in Ukraine's east.

They also shed light on the workaday activity of a propaganda shop, including a rare example of a draft text apparently edited in Mr. Surkov's office that can be compared with a final version.

The Ukrainian group, calling itself CyberHunta -- a mocking reference to the Russian assessment that the Kiev government is a fascist junta -- released 2,337 emails from the address prm_surkova@gov.ru, many from 2014 as the eastern Ukrainian separatists established their mini- states.

The correspondence included the spreadsheet of a budget to set up a small newspaper in Donetsk, the capital of the breakaway Donetsk People's Republic.

One email alerted Mr. Surkov's office to rebel casualties in June 2014 that included a paratrooper from Pskov, a town in northern Russia. At the time, there was considerable political sensitivity over the deaths of Russian soldiers in Ukraine.

In another letter, lists of candidates for separatist government positions arrived in Mr. Surkov's inbox before their appointments.

Mr. Surkov, a former advertising executive, is widely seen as an architect of Mr. Putin's domestic political framework and the post- Communist ideology of "sovereign democracy," a term he coined. In 2013, he told an audience in London, "I am the author, or one of the authors, of the new Russian political system."

Mr. Surkov apparently received in his email inbox a letter from a Moscow magazine editor with a draft of an "open letter from residents of the Donbas," ostensibly written by local people in Donetsk to describe the horrors of war.

While it is unclear if Mr. Surkov edited it personally, the changes that appear in the published letter suggest a deft eye for trimming and sharpening a text.

"Ukrainian soldiers and Donbas militiamen are dying," the original read. "Few of them want to risk their lives and kill, most realize this is a fratricidal war."

The punchier "Ukrainian soldiers and Donbas militiamen are dying. Most realize this is a fratricidal war," wound up in the final version.

In another edit, the original -- "Our testimony in your eyes should be weightier than the assertions of specialized propagandists" -- became the subtly improved, "Our testimony in your eyes outweighs the assertions of specialized propagandists."

The Obama administration has accused the Kremlin of hacking into the computers of the Democratic National Committee and various Democratic officials and institutions in an effort to discredit the American political system. In recent weeks, there have been reports of high-level meetings at the White House to discuss ways to punish Moscow, including sanctions and covert action against Russian targets.

Newsweek
How Snowden Smartened Up Our Spying
Friday, 28 October 2016
Byline: Jack Goldsmith

Column - Three years ago, the Guardian published the first story based on the huge archive of documents Edward Snowden stole from the National Security Agency while working as an NSA contractor.
Then-attorney general Eric Holder's Justice Department quickly charged Snowden with felonies for theft of government property and mishandling classified information.

This May, however, Holder praised Snowden. "I think that he actually performed a public service by raising the debate that we engaged in and by the changes that we made," Holder said.

This seems like an improbable claim. Snowden compromised scores of surveillance techniques, representing billions of dollars of investments over many years. U.S. firms that secretly cooperated with government intelligence agencies stopped doing so to the extent they could, and public defiance became the business- compelled norm.

Firms made encryption more readily available and easier to use, which made it harder for the U.S. government to monitor communications and access data. Many foreign governments responded with countermeasures like data localization laws, tighter privacy rules and closer judicial scrutiny of U.S. collection practices.

The Defense Department claimed that the "scope of the compromised knowledge related to U.S. intelligence capabilities" as a result of Snowden's disclosures was "staggering."

This claim is unverifiable but seems plausible in light of the breadth of and reaction to the disclosures. The intelligence losses extend beyond counterterrorism, the main context in which these issues are typically discussed.

NSA collections undergird every element of U.S. national security and foreign policy--including its extensive military operations around the globe, its pervasive diplomatic engagements and its numerous economic negotiations and initiatives.

Knowing what an adversary or other foreign intelligence target is doing or planning gives the United States a huge advantage in its myriad international affairs and is a central pillar of American power.

Such knowledge is harder to come by because of Snowden. And yet Holder is still right.

At the dawn of the Snowden revelations, many wondered whether the U.S. intelligence community would be destroyed. Some hoped that it would. But the opposite has happened: Despite undoubted intelligence losses, new collection barriers and diplomatic embarrassments, the community has emerged as a stronger organization despite, indeed because of, Snowden.

What Has Snowden Wrought?

Snowden forced the intelligence community out of its suboptimal and unsustainable obsession with secrecy. "Before the unauthorized disclosures, we were always conservative about discussing specifics of our collection programs, based on the truism that the more adversaries know about what we're doing, the more they can avoid our surveillance," Director of National Intelligence James Clapper said in 2013.

Post-Snowden, the intelligence community operates on the principle that secrecy is not an absolute value, but one that needs to be traded off for other values, including domestic legitimacy. Snowden made it realize that, in the words of former NSA Director Michael Hayden, "although the public cannot be briefed on everything, there has to be enough out there so that the majority of the population believe what they are doing is acceptable."

Forced transparency meant that the intelligence community had to justify itself before the American people for the first time ever--about what it did in the domestic arena and abroad, about the legality of and accountability for its actions and about its importance to U.S. national security.

It had to open itself up to thorough scrutiny and judgment by many new institutions, including the President's Review Group and a Privacy and Civil Liberties Oversight Board (PCLOB).

Initially, this was a painful, even bewildering process--the intelligence community had no experience at explaining itself, and thus wasn't any good at it. But the transparency turned out to bring many benefits.

First, the intelligence community opened up. It got much better at talking to the public. And the sky did not fall.

Second, the intelligence community had a good story to tell. Credible public evidence emerged that the NSA was a thoroughly accountable institution performing a vital intelligence role.

"Every program was authorized and approved, and what everyone thinks of the programs, it was not a case of running amok or exceeding its authority," said civil libertarian and Chicago law professor Geoffrey Stone, a review group member.

And the value of NSA programs was publicly revealed to a greater degree than ever. The PCLOB concluded that the Section 702 PRISM and upstream programs "played a key role in discovering and disrupting specific terrorist plots aimed at the United States and other countries."

These claims by outsiders to (and in some instances, adversary critics of) the intelligence community are significantly more credible and legitimizing than when the community itself makes the same sorts of claim.

Third, the main criticisms of the NSA ended up having silver linings. It emerged from the Snowden documents (and further voluntary releases by the government) that the NSA sometimes had problems

complying with judicial orders, usually because of the difficulty of meshing legal directives with extraordinarily complex technical collection processes.

And yet these embarrassments also showed that the Foreign Intelligence Surveillance Court that monitors the NSA in secret was not, as many claimed, a rubber stamp. It was, instead, an important independent check on NSA activities.

As a result of Snowden, the FISA court is a much more credible institution that can and in the future will be relied upon more thoroughly to monitor expanded NSA activities in secret.

Another criticism of the NSA was that its aggressive collection processes abroad did not consider the rights and interests of foreign individuals and firms. The main response was Presidential Policy Directive 28, which imposed restraints on collection abroad in the interests of non- U.S. citizens.

PPD 28 does not have sharp teeth and, while it has reportedly been a pain to implement, it will probably not have a material impact on U.S. collection practices. Like many post-Snowden reforms, it imposes process and oversight constraints and forces the NSA to be more prudent in its collection practices.

PPD 28 (along with the Judicial Redress Act, which extended Privacy Act protections to foreign citizens) has the side benefit that the United States can now proudly and truthfully claim to have the most robust protections for noncitizens of any signals collection agency in the world.

Fourth, and perhaps most surprising, the intelligence community has been able to maintain and strengthen the legal authorities for its collection practices. The bulk telephone metadata program was legally and on the merits the most controversial program that Snowden revealed, and the one that the NSA seemed least interested in preserving.

The USA Freedom Act made some important reforms to this program--most notably, by replacing NSA collection and storage of the metadata with carrier storage of the data and by requiring more-limited NSA querying of the data pursuant to court approval.

And yet the NSA has ended up in a stronger position as a result. It gets access to "a greater volume of call records" than before, according to the NSA general counsel, and probably at a lower cost, since it no longer needs to store and organize the massive quantities of data.

And even more important, the program has now been vetted publicly and expressly baked into the legal system, giving it a legitimacy and almost certainly a longevity that it never could have achieved in secret.

The improbable preservation and strengthening of the bulk telephone metadata program--the least valuable and hardest to justify of the programs that Snowden revealed--is emblematic of the types of changes Snowden wrought.

Strong and Sound

Few if any important intelligence collection programs have ended because of Snowden, and the USA Freedom Act reforms actually expanded some intelligence community authorities. The intelligence community has had to subject itself to more scrutiny and process checks, and it has had to trim its sails a bit to make its practices more proportional to the ends it seeks.

But the transparency resulted in public debates that concluded that the NSA practices were worth preserving overall. From the baseline of what almost everyone expected when the scale of Snowden's revelations first became apparent, the intelligence community and especially the NSA have emerged in astonishingly good shape.

The NSA is still very much in the business of aggressive signals intelligence around the globe. Its domestic legal authorities are sounder. Its value is more apparent to the American public. It is much more adept at public diplomacy. And its central and expanding role going forward--not just for signals intelligence collection, but for cybersecurity and offensive cyberoperations--is secure.

These are but some of the public services for which the U.S. government has Snowden to thank.

Note: Jack Goldsmith is a senior fellow at the Hoover Institution and the Henry L. Shattuck professor of law at Harvard University. From 2003 to 2004, he served as the assistant attorney general, Office of Legal Counsel. From 2002 to 2003, he served as the special counsel to the general counsel of the Department of Defense.

Le Monde
Les assureurs peinent à convaincre les PME en matière de cybersécurité
Friday, 28 October 2016
Byline: Dominique Gallois

Paris - Selon Axa, 5 % des petites et moyennes entreprises sont couvertes pour ces risques
En matière de protection contre les cyberattaques, la route est longue de l'intention à la concrétisation. Si en janvier, une étude du cabinet PwC, révélait que 52 % des entreprises françaises envisageaient de souscrire une police d'assurance pour protéger leurs données confidentielles, dix mois plus tard rien n'a bougé. " Moins de 1 % des TPE - très petites entreprises - et à peine 5 % des PME - petites et moyennes entreprises - sont couvertes, estimait Jean-Luc Montané, directeur général d'Axa Entreprises, mercredi 26 octobre, en décrivant la vulnérabilité de ces sociétés. De plus, celles qui ont déjà des contrats, ont la plupart du temps souscrit des couvertures partielles de leurs risques informatiques. " Une nette différence avec les grandes entreprises, quasiment toutes déjà prémunies contre la cybercriminalité.

La fracture est aussi nette avec l'opinion générale car " si les Français mesurent bien l'ampleur des cyber-risques, ceux-ci sont largement sous estimés par les TPE et les PME ", relevait PwC dans un

environnement où les intrusions se multiplient. Elles ont progressé en France de 51 % en 2015 contre 38 % dans le monde.

" Le risque est plus élevé pour les TPE-PME car elles n'ont pas les moyens des grandes entreprises pour se protéger ni leurs capacités financières pour y faire face en cas d'attaque ", relève M. Montané. Les entreprises les plus menacées sont celles qui vendent directement sur Internet, et les plus visées pour leurs données sensibles se trouvent dans la santé, la finance et les services. Les dégâts peuvent être multiples, allant de la perte d'exploitation à l'arrêt de l'activité, sans parler de l'impact désastreux sur l'image de l'entreprise et surtout de la perte de confiance des clients.

Comme les autres assureurs, Axa s'est engagé voici deux ans, sur ce nouveau créneau de la cybersécurité. Depuis, le groupe diversifie ses offres. L'une d'elles se fera avec le concours de Stormshield, une filiale d'Airbus spécialisée dans la sécurité des réseaux, précise le directeur des risques techniques d'Axa, Philippe Gaillard.

" Notre taux de vente est faible ", reconnaît cependant M. Montané. Ce n'est pas faute de moyens. Après avoir formé tout le réseau d'agents, près de 400 prospections ont été lancées en quelques moi s. " Il y a une prise de conscience, nous avons l'écoute du client, mais nous n'avons pas constaté le passage à l'acte ", -explique-t-il. Dans une conjoncture difficile, le coût de ce nouveau contrat peut aussi être dissuasif. Il représente une majoration de 10 % à 20 % du budget d'assurance dommages, hors santé et automobile.

" Nous en sommes au début "Le développement de ce nouveau marché se fait de manière contrastée dans le monde. En Amérique du Nord, la croissance est exponentielle, partant de 100 millions d'euros en 2001 à 2,3 milliards en 2014. Les analystes tablent sur 8 milliards prochainement. Les assureurs anglo-saxons sont donc ceux qui maîtrisent le mieux ces sujets et tiennent le marché, qui en Europe comme en Asie en est à ses balbutiements : 160 millions d'euros pour l'un et 100 millions pour l'autre.

En France, ce secteur de l'assurance pèse à peine 40 millions d'euros et les plus optimistes le voient dépasser, à terme, le milliard d'euros. Mais il faudra du temps. " Aujourd'hui tout le monde souscrit une police d'incendie alors que le risque est très faible, c'est entré dans les moeurs depuis longtemps, relève le responsable d'Axa Entreprises. Pour la cybersécurité, nous en sommes au début. " Le développement des objets -connectés d'un côté et les menaces de plus en plus fortes d'actes terroristes, de malveillance, d'espionnage ou de rançonnage, de l'autre, pourraient accélérer la prise de conscience.

Christian Science Monitor
In Russia's cyberscene: Kremlin desires, private hackers, and patriotism
Thursday, 27 October 2016
Byline: Fred Weir

Moscow - While much is known about US cyber-war and -espionage capabilities thanks to the massive data leaks of former NSA contractor Edward Snowden, Russia's capacity for such is much more obscure. But the experience of Alexander Vyarya, which came to light virtually without notice last year, may offer a few telling glimpses of it.

Mr. Vyarya, a young Russian programmer, was a team member at Qrator, a leading Russian cybersecurity company that specializes in mitigating the effects of distributed denial-of-service [DDoS] attacks. According to his account, given to the independent Russian online news service Medusa, the company was approached by an intermediary from Russia's Ministry of Communications looking for a specialist to help with a particular problem.

Vyarya was "loaned" on an unofficial basis to Rostek, the Russian state technology conglomerate, in early 2015, and sent to an office in Sofia, Bulgaria. There, he was asked to help develop software not to block, but to amplify DDoS attacks. He did - and he was appalled when the program was "tried out" before his eyes on targets like Ukraine's Defense Ministry and the liberal Russian magazine Slon, he later told Medusa. By his account, he told his contact "I am not a hacker," and subsequently fled to Finland.

Vyarya's experience - other than the young programmer's attack of conscience and relating his story to the press - is not unusual on Russia's cyberscene, says Andrei Soldatov, one of the country's foremost cybersecurity experts and co-author of The Red Web, a history of the Russian internet - and the security services' efforts to control it - that will be released in Russian next week.

Pinning down specific Russian responsibility for hacking incidents around the world is complicated by Russia's complex arrangement of Kremlin power, semi-official liaisons, and players in Russia's burgeoning IT sector - where the general surge in patriotism since the Ukraine crisis began almost three years ago has made many young specialists more inclined to be quietly cooperative with such requests. What Vyarya describes, Mr. Soldatov says, fits the model.

"Russia's landscape is very complicated, because the private sector is actually far more advanced than the state sector in IT expertise," he says. "Chinese hacking, by contrast, almost totally originates with the security services. But in Russia there is a much wider variety of informal actors."

Cyberwar and cybercrime

According to Soldatov, one of the first examples of politically motivated hacking occurred in the early 2000s, during the second Chechen war, when a group of students in the Siberian city of Tomsk started attacking pro-Chechen websites. Russian security services took notice.

Later, the Kremlin organized several patriotic youth groups, such as Nashi and Molodaya Gvardia, with the aim of using them to crush any "Orange Revolution" type street demonstrations in Russia. Nashi was later implicated in a highly successful DDoS attack against infrastructure in Estonia in 2007.

"It's quite a clever model, since you always have security services out of the picture," says Soldatov. "At least, that was the situation before the annexation of Crimea.

"Since then there has been a big change," he adds. "The technological level and scale of cyberactivities has taken a huge leap. The crisis has made it much easier for the Kremlin to mobilize Russians in general, and to approach people in our IT industry for help on an informal basis."

Unlike the US, where there is a large overlap between state and private IT sectors - think Booz Allen Hamilton - Russia's IT industry has taken off in recent years largely without state support, says Tim Bobak, a Moscow-based expert with Group-IB, a cyberthreat intelligence company.

"The Russian IT sector has emerged largely on its own," he says. "It has good professionals. Its main problem is how to export its knowledge. Individuals can leave, but relatively few companies have managed to break out of the Russian market."

Russia, with its great national strengths in maths and engineering, has given the world a great many IT experts - and also populated the criminal underworld with highly qualified hackers. According to a report on cybercrime released this year by Group-IB, "16 out of the 19 trojans most actively used for theft can be linked to Russian-speaking cybercriminals."

A Kremlin connection

How the Kremlin enlists expertise from the private IT sector, and perhaps the criminal world as well, remains murky, says Soldatov.

"We know there is a huge pool of capable talent, and at least some people who are willing to do things that are suggested to them," he says. "We know such things are being done. What we don't know is how or why such orders are formulated, and who exactly may be involved.

"I personally don't think there is a coherent strategy at work, say, to destabilize American democracy. I think there are tactical experiments that are undertaken. When they work, they get people excited. After these hacks against the Democratic Party in the US, people say 'look, they're talking about a third force in the US elections, wow, let's do more of that,' and so on," Soldatov says.

Earlier this year a massive attack, reminiscent of the ones Vyarya described, nearly shut down Ukraine's power grid and demonstrated the extreme vulnerability of public infrastructure.

Hacking and leaking information for political impact has become depressingly commonplace. Many Russians blame US secret services for the Panama Papers last spring, which implicated close friends of Vladimir Putin in financial corruption. This week a group of Ukrainian hackers released scores of email documents allegedly from accounts connected with Vladislav Surkov, a top Kremlin aide, that purport to illustrate Russian plans to destabilize Ukraine.

Cyberbarriers

Ukrainians have the advantage of knowing Russian language and habits, and may be uniquely poised to attack Russian interests. But experts say threatened attempts to retaliate against Moscow from the West may fall flat due not only to the language barrier, but also the higher levels of secrecy common in Russian society and officialdom, as well as a media culture that effectively blocks and dilutes bad news.

"The thing that is most remarkable about the alleged hacks against the DNC and Hillary Clinton's campaign is not the technological expertise of the intrusion, which was not high at all, but the level of social intelligence that was involved," says Soldatov. "You need to know who's who in the Clinton campaign, how the chain of command runs, and an awful lot of background to go in and get the information you want, and correctly evaluate it. This suggests that the simple idea that it was military intelligence, the GRU, or the FSB [Russia's internal spy service] that did these things on their own is not an accurate picture. Outside the former Soviet Union, these agencies are not all that effective."

The relative isolation of Russia in the global IT market may also work to its advantage if it comes to a major cyber- showdown with the US, experts say.

"While we don't yet have independence from foreign-made equipment and operating systems, we are almost completely self-sufficient in cybersecurity systems," says Sergei Serstobitov, head of Angara IT, a private Moscow-based security firm.

"There is a concerted effort now to correct these deficiencies, and Russia is becoming gradually less and less dependent on Western technology. Everyone is much more aware of the need for cybersecurity than we ever were before."

CBC News
Pay problems linger for thousands of public servants as Phoenix deadline arrives
Monday, 31 October 2016
Byline: Ashley Burke

Ottawa - The federal government's self-imposed Oct. 31 deadline for eliminating the backlog of Phoenix pay problems has arrived, but some public servants say they're still going into debt to pay their bills. Two weeks ago Marie Lemay, the deputy minister in charge of the system, said the bulk of the 80,000 remaining cases would be solved by today, but warned some of the more complex files may not be resolved in time.

Global Affairs Canada employee Sabrina Arrizza said she can't believe the "magical day" is here, yet she's still owed $4,000 in missing pay.

"I've reached the point of complete hopelessness," said Arrizza, who said she's had to take out a line of credit to pay her bills.

"It's extremely distressing. I was in a better financial situation when I was a student without a job."

Earlier this summer Arrizza was told her file had risen to what the pay centre calls "the war room," where cases go when compensation advisers can't figure out how to solve them.

Managers supportive, but can't help

"It was a little complicated but I'm not sure why I've been left in the backlog," said Arrizza. "I have not received a phone call. So to me, how can you even work on my case when you haven't even called me yet to discuss it?"

Arrizza transitioned from a casual contract to a term position in May but said she wasn't paid for seven weeks. When she finally got a cheque it was for a much lower pay category, she said.

On top of that, Arrizza isn't being reimbursed for dental care. She said her managers have been very supportive, but haven't been able to help solve her problem.

"It's quite sad when it gets to the point when your managers can't even do anything about it," she said.

'It should have been fixed by now'

Dean Ashby, a manager at Measurement Canada, describes himself as a "very patient guy," but said it's "disturbing" that he's waited since April for as much as $18,000 he said he's owed.

"I've waited seven months and I think it's time to voice my opinion now," said Ashby from Penticton, B.C. "One hundred per cent it should have fixed by now."

Ashby said he's burned through his savings, has had to cut back on his daughter's dance lessons and son's go-cart racing.

"Unfortunately my kids have suffered probably the most, because they haven't been able to do their sports," said Ashby.

He returned from an 18-month leave on April 1, then went seven pay periods without a cheque. When he finally got paid in June "it was completely wrong," Ashby said.

Even when the cheques started coming, they were $700 short. Ashby is in charge of nearly a dozen staff, and said he recently realized during a team meeting that he was the lowest-paid employee in the room.

"It's unfair," said Ashby. "I'm working and working and I'm not getting paid. You can't do that. It's against the law."

Rally planned for Monday

On Oct. 19 deputy minister Marie Lemay admitted the government is "tracking a bit behind," with 30,000 out of more than 80,000 cases still unresolved.

Updated figures showing how many cases could still be in the government's backlog of Phoenix files are expected at the next technical briefing, which could come as early as this afternoon.

Public servants will hold a rally in front of the prime minister's office at 12:30 p.m. Monday to express their "ongoing frustrations with the dysfunctional Phoenix pay system," according to the Public Service Alliance of Canada.

Xinhua News Agency
China's draft cybersecurity law gets 3rd reading
Monday, 31 October 2016
Byline: Staff reporter

Beijing - China's draft cybersecurity law was submitted to legislators for its third reading at the bimonthly session of the National People's Congress (NPC) Standing Committee, which began Monday. The draft allows police and other law enforcers to take measures including freezing assets, against overseas individuals or organizations that "attack, intrude, interfere with or sabotage the nation's key information infrastructure."

La Presse+
Protection des sources journalistiques Visé par 24 mandats de surveillance
Monday, 31 October 2016
Byline: Philippe Teisceira-Lessard avec Daniel Renaud

Montréal - Le Service de police de la Ville de Montréal (SPVM) a placé sous surveillance l'iPhone du chroniqueur de La Presse Patrick Lagacé afin de connaître l'identité de ses interlocuteurs pendant plusieurs mois et de pouvoir le localiser avec le GPS intégré, dans une opération sans précédent connu au Québec.
Au moins 24 mandats de surveillance concernant le téléphone du chroniqueur ont été accordés par la justice depuis le début de l'année 2016 à la demande de la section des Enquêtes spéciales de la police, a appris La Presse. Cette section est chargée de réprimer le crime au sein même des forces de l'ordre.

Trois des mandats ont permis d'obtenir les numéros entrants et sortants de l'appareil, tant pour les appels que les messages textes. Un mandat de localisation a aussi permis aux policiers du SPVM d'activer la puce GPS de l'iPhone de Patrick Lagacé afin de savoir exactement où il se trouvait, ont admis deux enquêteurs responsables du dossier. Le SPVM dit avoir utilisé cette dernière possibilité « rarement », « jamais » ou « presque jamais ».

Le vice-président à l'information de La Presse, Éric Trottier, a vivement dénoncé l'opération, qui « constitue une attaque sans équivoque contre l'institution qu'est La Presse et contre toute la profession journalistique ».

« Au Canada, les corps de police semblent tout simplement faire fi [des] règles fondamentales » qui protègent le travail des journalistes, a-t-il écrit dans une déclaration publiée aujourd'hui (voir l'écran 5). « Il faut mettre un terme à ce qui a toutes les allures d'une véritable chasse aux sources journalistiques. »

Le principal intéressé était sous le choc en apprenant avoir fait l'objet de surveillance électronique. « Je vivais dans une fiction où la police ne ferait jamais une chose pareille », a affirmé Patrick Lagacé.

« Je pensais sincèrement que pour les journalistes, quand il était question de les surveiller par des moyens judiciaires, on appliquait un test pas mal plus rigoureux que ça. »

-- Patrick Lagacé

« J'ai vraiment l'impression d'avoir été l'objet d'une partie de pêche. Je ne les crois pas une seconde quand ils disent n'avoir aucun intérêt pour les autre numéros de téléphone » qui figuraient sur les registres téléphoniques obtenus, dans un contexte de chasse aux sources au SPVM.

FEU VERT DES AFFAIRES INTERNES

Le controversé patron sortant des Affaires internes du SPVM, Costa Labos, a affirmé en entrevue avoir donné son feu vert à ce moyen d'enquête. Il a refusé de révéler si le chef de police Philippe Pichet a été informé de la mise sous surveillance de l'appareil. M. Labos a aussi affirmé qu'« à sa connaissance », aucun autre journaliste n'avait fait l'objet de surveillance du SPVM dans les dernières années, mais sans pouvoir « le garantir ».

« Je comprends que certaines personnes peuvent avoir été offusquées ou dérangées par le fait que leur téléphone ait été [l'objet de surveillance], mais il faut faire notre travail », a fait valoir M. Labos, samedi, en entrevue téléphonique. « C'est aussi simple que ça. Je ne veux pas exagérer les choses, ni les minimiser. » Il a précisé que l'obtention des numéros entrants et sortants d'un cellulaire était parmi les moyens « les moins intrusifs » à la disposition de la police.

« Non seulement avons-nous pris la situation au sérieux, mais nous comprenons le caractère délicat du travail avec des sources et de l'importance de les protéger. »

-- Costa Labos, patron sortant des Affaires internets du SPVM

Le SPVM a annoncé vendredi que l'inspecteur-chef Labos avait été muté des Affaires internes vers la division des communications opérationnelles et informations policières, qui gère notamment les télécommunications du service de police. Rien n'indique qu'un lien existe entre cette décision et la mise sous surveillance du cellulaire de Patrick Lagacé.

Cet été, le policier avait lui-même fait l'objet d'une enquête criminelle en lien avec une traque aux fuites médiatiques. Aucune accusation n'a finalement été déposée contre lui.

Le chef de police Philippe Pichet a refusé la demande d'entrevue de La Presse.

C'est la juge de paix Josée de Carufel, de Montréal, qui a autorisé la majorité des mandats de surveillance.

« VOUS ÊTES COMME UTILE À L'ENQUÊTE »

Les mandats ont été demandés et obtenus dans le cadre du « Projet Escouade » qui portait sur des allégations de fabrication de preuve par des enquêteurs spécialistes des gangs de rue et du trafic de drogue. Cinq policiers ont été arrêtés cet été à l'issue de l'enquête, et deux ont été accusés.

L'un des policiers visés dans Escouade était Fayçal Djelidi. En surveillant le cellulaire de ce dernier, la section des Enquêtes spéciales du SPVM a détecté des contacts entre le policier et Patrick Lagacé, ont expliqué les enquêteurs Iad Hanna et Normand Borduas - responsables du dossier - au cours d'une rencontre avec Patrick Lagacé tenue vendredi.

De plus, selon eux, « des articles de journaux » étaient publiés « pas longtemps après » ces contacts, et ces articles concernaient des dossiers impliquant M. Djelidi. Aucun des articles n'a été écrit par M. Lagacé, et les reportages étaient parfois publiés par d'autres médias que La Presse.

Ces présumées fuites « nuis[aient] à des projets en cours », a affirmé M. Hanna. « Des enquêtes criminelles. »

Les policiers ont alors ouvert en parallèle une enquête pour « abus de confiance » - une infraction criminelle - contre M. Djelidi en lien avec ces fuites. C'est dans le cadre de cette enquête que le cellulaire de M. Lagacé a été placé sous surveillance, ont indiqué les deux policiers.

« C'est uniquement Fayçal qui nous intéresse. Et vous dans cette chose-là, vous n'êtes pas impliqué à titre de suspect de quoi que ce soit. Vous êtes comme utile à l'enquête, dans un sens », a affirmé Iad Hanna à Patrick Lagacé, vendredi.

Arrêté au début du mois de juillet pour la façon dont il gérait ses sources policières et pour avoir sollicité des prostituées, M. Djelidi n'a fait l'objet d'aucune accusation en lien avec les supposées fuites journalistiques. L'enjeu était devenu « un pan d'enquête qui n'était pas primordial », a indiqué M. Hanna, évoquant un « petit volet » de l'investigation.

Le policier a ajouté que les données recueillies dans le cellulaire du journaliste se trouvaient maintenant sur une clé USB « de type militaire » placée dans une voûte sécurisée.

« C'EST INQUIÉTANT »

La liste obtenue par La Presse révèle l'existence de 126 mandats divers octroyés dans le cadre de l'enquête de MM. Hanna et Borduas.

En plus des trois mandats d'obtention des numéros entrants et sortants (baptisés DNR pour « dial number recorder ») et du mandat de localisation, la police a aussi obtenu 20 mandats qui visent à obtenir l'identité des interlocuteurs de Patrick Lagacé auprès de leur propre société de téléphonie. Ces ordonnances permettent d'obtenir « qui a enregistré le compte, qui le paie, avec quelle carte. Ça va donner un peu plus d'information », a expliqué Paul Laurier, ex-policier qui oeuvre maintenant au sein de la firme Artémis Renseignement.

Selon Christian Leblanc, président sortant de l'Association des avocats en droit des médias du Canada, l'obtention de tels mandats sur le téléphone cellulaire d'un journaliste est extrêmement préoccupante.

« Dans ma pratique, je n'ai jamais été en contact avec un pareil cas, c'est-à-dire un journaliste dont le téléphone faisait partie d'un mandat DNR et encore plus un mandat DNR de façon aussi large », a-t-il affirmé en entrevue.

« C'est inquiétant, a ajouté M. Leblanc. La Cour suprême est venue dire que ce n'était que dans des cas exceptionnels et qu'il fallait s'assurer que les médias ne deviennent pas le bras d'enquête des policiers parce que si c'était le cas, les sources risquaient de se tarir et que donc le droit du public à l'information allait en souffrir grandement. »

COMPARUTION CE MATIN

La Presse comparaît ce matin à la salle 3.12 du palais de justice de Montréal afin d'obtenir les documents qui ont convaincu la justice de délivrer l'ensemble des mandats utilisés dans cette enquête. C'est au cours de la préparation de cette audience que La Presse a mis la main sur la confirmation que des mandats ont été autorisés pour mettre sous surveillance le cellulaire de Patrick Lagacé.

Encadré(s) :

L'AFFAIRE EN SEPT TEMPS

Philippe Teisceira-Lessard

Fin 2015

La section des Enquêtes spéciales du SPVM ouvre une investigation concernant le policier Faycal Djelidi, un spécialiste des gangs de rue, sur la base d'allégations de fabrication de preuve.

Entre-temps

En surveillant les numéros entrants et sortants du cellulaire de Djelidi, le SPVM découvre que le policier et Patrick Lagacé entrent parfois en contact. Selon la police, des informations auxquelles Djelidi a accès sont concurremment publiées par d'autres journalistes et d'autres médias - jamais par M. Lagacé. Les enquêteurs décident d'ouvrir un nouveau pan d'enquête criminelle concernant cette situation.

13 janvier 2016

Les Enquêtes spéciales obtiennent un premier mandat de surveillance applicable au cellulaire de Patrick Lagacé, autorisé par la juge de paix Josée de Carufel. Elle en délivrera six autres la semaine suivante. L'un d'entre eux vise à obtenir les registres téléphoniques des mois précédant janvier.

Mars 2016

Le SPVM obtient un renouvellement de ses mandats.

3 mai 2016

La juge de paix de Carufel autorise un mandat de localisation sur un cellulaire de Patrick Lagacé, qui permet au SPVM de connaître sa position grâce à la puce GPS qui y est intégrée. Pendant ce même mois, elle autorisera le renouvellement de six autres mandats de surveillance concernant le cellulaire du journaliste.

7 juillet 2016

Le chef Philippe Pichet sort de ses vacances pour annoncer l'arrestation de quatre policiers (un cinquième s'ajoutera rapidement), dont Faycal Djelidi. Ce dernier fait face à une kyrielle d'accusations en lien avec ses visites présumées à des prostituées et à de la fabrication de preuve. Aucune n'est liée aux fuites d'information dont le SPVM le soupçonnait. En conférence de presse, le chef Pichet allègue qu'un ou plusieurs des policiers arrêtés avaient tenté d'entrer en contact avec les médias.

27 octobre 2016

Dans le cadre de procédures judiciaires de routine afin d'obtenir de l'information sur l'enquête, La Presse et Patrick Lagacé apprennent l'existence de 24 mandats de surveillance autorisés contre le cellulaire du journaliste.

La Presse+
Patrick Lagacé espionné par la police Une attaque en règle contre le droit du public à l'information
Monday, 31 October 2016
Byline: Éric Trottier

Montréal - L'espionnage par le Service de police de la Ville de Montréal (SPVM) des données téléphoniques de notre journaliste Patrick Lagacé constitue une attaque sans équivoque contre l'institution qu'est La Presse et contre toute la profession journalistique.
La base du travail du journaliste - et encore plus quand il s'agit de journalisme d'enquête - consiste à recueillir des sources crédibles qui sont souvent prêtes à prendre des risques pour nous révéler des faits troublants d'intérêt public, faits que les autorités ne souhaitent souvent pas voir étaler au grand jour. Sans sources, pas de journalisme digne de ce nom.

Savoir que le SPVM a ainsi pu avoir accès à l'ensemble des données téléphoniques de notre journaliste, donc à toutes ses sources, nous inquiète au plus haut point.

La liberté de la presse est un droit fondamental consacré par la Charte canadienne des droits et libertés et reconnu par la Cour suprême du Canada, qui a aussi confirmé que ce droit inclut la liberté de collecter de l'information.

La surveillance d'un journaliste constitue une atteinte claire à ce droit fondamental et à la protection des sources journalistiques ; cela compromet de manière irrémédiable le lien de confiance qui doit

exister entre un journaliste et une source journalistique afin que les citoyens puissent être informés sur des sujets d'intérêt public et participer de manière éclairée à la vie démocratique du pays.

Malheureusement, au Canada, et particulièrement au Québec, les corps de police semblent tout simplement faire fi de ces règles fondamentales.

Ainsi, nous avons appris cette année que le grand patron de la Gendarmerie royale du Canada (GRC), Bob Paulson, avait lui-même autorisé la filature de notre journaliste Joël-Denis Bellavance dans l'espoir d'en apprendre plus sur ses sources, en 2008.

Il y a deux ans, deux agents de la Sûreté du Québec (SQ) sont aussi venus rencontrer et menacer Patrick Lagacé après l'avoir incité à se mettre à table au sujet de ses sources policières dans l'affaire Ian Davidson, ce policier corrompu qui s'est suicidé en 2012.

Toujours en 2012, la même SQ avait perquisitionné la résidence du journaliste Éric Yvan Lemay, du Journal de Montréal, à la suite d'un reportage révélant que des documents confidentiels traînaient dans les corridors d'hôpitaux.

En septembre dernier, la même SQ a saisi cette fois l'ordinateur d'un autre journaliste du Journal de Montréal, Michaël Nguyen, après la parution d'un reportage embarrassant pour la juge Suzanne Vadboncoeur.

Au lendemain de cette saisie, l'Assemblée nationale a d'ailleurs adopté à l'unanimité une motion dénonçant l'intervention policière.

Il est peut-être temps que nos gouvernants se commettent davantage en se penchant sérieusement sur le travail des policiers à l'égard des journalistes : il faut mettre un terme à ce qui a toutes les allures d'une véritable chasse aux sources journalistiques.

De graves questions

Dans le cas de Patrick Lagacé, nous sommes d'autant plus inquiets que le SPVM refuse de nous confirmer catégoriquement s'il surveille (ou s'il a surveillé) les données téléphoniques d'autres journalistes de La Presse et d'autres médias. Pressé de questions à ce sujet, l'inspecteur-chef Costa Labos, responsable jusqu'à la semaine dernière des affaires internes au SPVM et celui qui a autorisé la surveillance du téléphone de notre journaliste, a répondu : « À ma connaissance, la réponse est non, mais je ne peux pas le garantir à 100 %. Pour être sûr à 100 %, il faudrait que je vérifie chacun de nos dossiers... »

Vous comprendrez que La Presse se pose de graves questions :

1. Est-ce que le SPVM en était à une première surveillance du genre à l'égard d'un de nos journalistes ? Cette pratique est-elle régulière ?

2. Y a-t-il d'autres journalistes dont le téléphone est présentement surveillé par la police ?

3. Qui a eu accès aux données téléphoniques de notre journaliste ?

4. Qu'en ont fait les policiers ?

5. Le chef du SPVM, Philippe Pichet, a-t-il autorisé la démarche de ses policiers ? S'il ne l'a pas fait, l'approuve-t-il ?

6. Le maire Denis Coderre est-il d'accord avec une telle méthode d'enquête qui pose des risques au travail journalistique et, ultimement, à notre démocratie ?

7. Le SPVM est-il allé plus loin ? A- t-il eu recours à de la filature ou de l'écoute électronique pour surveiller des journalistes ?

8. Enfin, nos gouvernants à Québec, plus particulièrement la ministre de la Justice, Stéphanie Vallée, le ministre de la Sécurité publique, Martin Coiteux, et le premier ministre Philippe Couillard, acceptent-ils de diriger la destinée d'une société où la police peut obtenir aussi facilement un mandat pour surveiller les journalistes ?

Pour notre part, nos lecteurs et nos sources doivent savoir que La Presse n'entend pas se laisser faire sans réagir. Le lien de confiance qui devrait normalement être à la base des relations entre le Service de police de la Ville de Montréal et une grande institution comme la nôtre est rompu.

Nous agirons désormais en fonction de ces nouveaux paramètres.

Wall Street Journal
America Isn't Ready for a Cyberattack
Monday, 31 October 2016
Byline: Christopher Mims

New York - The recent cyberattack that rendered more than 1,200 websites unreachable was a warning. Experts say a similar, or larger, attack could be launched tomorrow, and we'd be powerless to prevent it. No one seems to know who was behind the attack, launched by a "botnet" of thousands of internet-connected devices. The Department of Homeland Security believes it wasn't another nation.

That sounds reassuring, but is scary: It doesn't take a government or even a skillful hacker to make much of the internet inaccessible to millions. Anyone can buy similar capability for less than $1,000.

Nations, or sophisticated hackers, are capable of worse, according to cybersecurity experts. And the threat of a counter-hack, or physical attack, seems to be an incomplete deterrent. The U.S. is believed to have employed cyberweapons to cripple Iran's nuclear-fuel enrichment program, and launched a drone to kill a hacker believed to be working with Islamic State. More recently, the Obama administration promised to retaliate against Russia for hacking email accounts of prominent Americans.

The Pentagon has a Cyber Command with both defensive and, increasingly, offensive capabilities. But retired Adm. James Stavridis, former supreme allied commander of NATO, calls it a "pickup team" of personnel from other military branches.

"Fundamentally cyber is no different than air, sea or land," says Adm. Stavridis, now the dean of the Fletcher School of Law and Diplomacy at Tufts University. "It's a place. And we're going to have national-security concerns there."

That means creating both a "cyber force," as well as a director of cybersecurity, just as we created a director of national intelligence in the wake of 9/11, says Adm. Stavridis. Such a force would be able to respond not only to attacks on the U.S. government and military, but also U.S. citizens, companies and infrastructure.

A Defense Department spokesman says responses to cyberattacks need to span "the public and private sectors at all levels," as outlined in a recent directive from the White House. In most cases, the spokesman says, the Pentagon shouldn't be involved, unless an attack poses "demonstrable harm to national security or core interests" of the U.S., such as the economy, foreign relations or public health.

At the same time, U.S. domestic law-enforcement agencies are on the cusp of gaining broader authority to hack into computers suspected of involvement in a cyberattack or other crime. The proposed changes to little- known Rule 41 of the Federal Rules of Criminal Procedure will go into effect Dec. 1, unless Congress blocks them. They will allow a judge to issue a warrant allowing agents to block or disable any computer -- be it a private company's web server or a smart TV in your living room.

The lines between the military and domestic law enforcement can blur, because attacks can take many forms. Consider the case of an attack on U.S. computers launched by terrorists operating overseas.

If notions of Pentagon-bankrolled cyber commandos employing weapons developed by the NSA, or FBI agents infiltrating and attacking computers, sound scary to you, you're not alone. On Thursday, a bipartisan group of lawmakers wrote to Attorney General Loretta Lynch to express concern about the change to Rule 41.

Security experts I talked to suggested several alternatives for enhancing America's cyberdefenses.

Dave Aitel, chief executive of cybersecurity firm Immunity Inc. and a technical adviser to the U.S. Department of Commerce, says lawmakers could consider authorizing victims to "hack back" at attackers. But that would present its own challenges, requiring changes to international law and new agreements between countries, lest a private company's retribution on an attacker across the globe be construed as an act of war.

To address the problems posed by the recent botnet attack, some people have suggested new rules for internet-connected devices.

Federal regulatory agencies have limited authority in this sphere. The Federal Trade Commission generally responds only after an incident, though it can require companies to recall products and hire outside auditors. Sen. Mark Warner (D., Va.) suggested that the Federal Communications Commission vet the security of internet-connected products before they are released. Even if adopted, that wouldn't affect devices made and used outside the U.S. Nor would new rules remedy the millions of vulnerable internet-connected devices already in use.

Jeremiah Grossman, chief of security strategy at Sentinel One Inc., says device makers should be liable for damage caused by insecure devices. That would allow Netflix Inc., for example, to sue Hangzhou Xiongmai Technology Co., maker of the many of the internet-connected cameras used in the recent attack that took Netflix offline.

In the end, all the proposals for a better-defended internet feel inadequate. They lend themselves to government overreach, cyber-vigilantism, or ineffectiveness.

We may have no choice, however. Security experts consider a "cyber-9/11" inevitable. Just as with the 9/11 attacks themselves, some experts think it will take such a calamity for government agencies, and the private sector, to cooperate toward an effective response.

What a cyber 9/11 might look like is anyone's guess.

I asked Jim Gillespie, whose firm Gray Matter Systems secures industrial- control systems, which part of America's infrastructure he worries about most. "Personally I'm most worried about the water industry," he said.

New York Times
Agents Cleared to Scrutinize Email Cache
Monday, 31 October 2016
Byline: Multiple reporters

Washington - Federal investigators have obtained a warrant to begin searching a large cache of emails belonging to a top aide to Hillary Clinton, law enforcement officials said on Sunday, as prosecutors and F.B.I. agents scrambled under intense public pressure to assess their significance before Election Day. It remains unclear whether they can finish their work by then. "The process has begun," a federal law enforcement official said.

The hurried pace at the Justice Department and the F.B.I. raises the prospect that law enforcement officials will again publicly discuss a continuing investigation involving a presidential candidate in the final days of the campaign. The F.B.I. director, James B. Comey, has faced extraordinary criticism since he sent an ambiguous letter to congressional leaders telling them that agents had discovered new emails.

Agents in an unrelated investigation of Anthony D. Weiner, the disgraced former congressman, found the emails, belonging to his estranged wife, Huma Abedin, the aide to Mrs. Clinton, this month. That prompted a renewed interest among agents who had investigated Mrs. Clinton for her use of a private email server as secretary of state. That investigation centered on whether Mrs. Clinton or her aides had mishandled classified information. Prosecutors concluded that case in July without bringing charges.

A federal law enforcement official said agents had discovered hundreds of thousands of emails on Mr. Weiner's computer, but investigators expected to examine only part of the total. Agents will have probable cause to search only the messages related to the Clinton investigation. Some of Ms. Abedin's emails passed through Mrs. Clinton's private server, officials said, which means there is a high likelihood that the F.B.I. has already read them.

Officials cautioned that there was no evidence to date that changed the Justice Department's conclusion that neither Mrs. Clinton nor her aides should be charged. They said it was possible that the review would turn up nothing, but said investigators felt obligated to check.

Mr. Comey has faced widespread criticism since his announcement on Friday, and senior Justice Department and F.B.I. officials have been under tremendous pressure to review the emails quickly and assess their importance. Both Mrs. Clinton and her Republican rival, Donald J. Trump, have called for the F.B.I. to say publicly what it knows before Election Day.

The Clinton campaign kept up the pressure on Mr. Comey on Sunday by releasing a letter signed by nearly 100 former senior Justice Department officials who sharply criticized the F.B.I. director. Among the officials who signed the letter was former Attorney General Eric H. Holder Jr., with whom Mr. Comey often clashed before Mr. Holder left office in 2015.

Over the weekend, senior Justice Department officials, some of whom advised Mr. Comey not to make a public announcement about the emails, said that they would make all resources available to conduct the investigation as quickly as possible, and that the timing of the letter -- just days before the election -- gave the matter an unprecedented urgency.

Late Friday and early Saturday, law enforcement officials said there was no chance the email review could be completed before Election Day. By Sunday, officials said they would spare no resources in the investigation and try to determine whether the new emails changed the Justice Department's conclusion not to charge Mrs. Clinton or her aides.

The emails will be reviewed by the same counterintelligence team in Washington that handled the Clinton investigation from the beginning. The review will focus on whether there is evidence in the emails that Ms. Abedin mishandled classified information or impeded the F.B.I.'s original email investigation.

Investigators will also want to know whether the new trove includes messages that Ms. Abedin did not turn over to the F.B.I. months ago. Ms. Abedin has said she did not routinely delete emails, and people close to her said she did not know these emails were on Mr. Weiner's computers. It is not clear how they got there, but it is possible they were automatically backed up.

The Justice Department efforts were described by three federal law enforcement officials who spoke on the condition of anonymity because they were not authorized to discuss the case.

The F.B.I. knew weeks ago that its investigation into whether Mr. Weiner sent illicit text messages to a 15-year-old girl in North Carolina had the potential to reignite the Clinton case. After agents seized Mr. Weiner's laptop, phone and tablet on Oct. 3, they quickly learned the computer contained a trove of Ms. Abedin's emails.

The assistant F.B.I. director in charge of the New York field office then notified the deputy director in Washington about the discovery, according to one senior law enforcement official. Agents in the Weiner case were not allowed to widely search Ms. Abedin's emails, but were told to conduct a cursory review of the metadata -- the "to" and "from" information on each message -- to see if any of the emails could be relevant to the Clinton investigation.

Once it became clear that the emails were potentially significant, lawyers at the Justice Department and the F.B.I. conducted a legal analysis of how to proceed, officials said. Because Ms. Abedin's emails were not directly related to the investigation of her husband, criminal agents could neither read the contents of the emails nor pass them to their colleagues in Washington.

Late last week, the authorities decided to seek a search warrant to examine the emails. Mr. Comey's letter gave that effort a tremendous sense of urgency. Suddenly, a follow-up inquiry that was expected to take weeks or months now needed to be rushed before Election Day.

Mr. Comey's letter also opened him up to criticism from Democrats that he seemed willing to disclose every investigative wrinkle related to the Clinton investigation, but has not said anything about the scope of an F.B.I. investigation into Russian meddling in American elections. Democrats have repeatedly

asked the F.B.I. to investigate Mr. Trump and his aides as part of that case. Mr. Comey has never said if he would.

Senator Harry Reid of Nevada, the minority leader, increased the pressure on Mr. Comey late Sunday, criticizing the director for a "disturbing double standard."

"In my communications with you and other top officials in the national security community, it has become clear that you possess explosive information about close ties and coordination between Donald Trump, his top advisers and the Russian government," Mr. Reid wrote in a letter to Mr. Comey. "The public has a right to know this information."

It was unclear what Mr. Reid was referring to. A spokesman said in a telephone interview Sunday that Mr. Reid did not believe it was his place to disclose national security information, which had been told to him in confidential briefings with senior intelligence and law enforcement officials.

"The exact information is at the discretion of the national security community, but it is Senator Reid's view that there is much more that can be said publicly than has been so far," said the spokesman, Adam Jentleson.

Mr. Comey and his allies have defended his handling of the Clinton case, calling the circumstances "exceptional."

Though Justice Department guidelines discourage making public comments about continuing investigations or doing anything that could influence an election, Mr. Comey has said he believed that he was obligated to reveal the existence of the new emails. Not telling Congress, he told colleagues, would have opened up the F.B.I. to criticism and created a cloud that would have hung over the bureau for years.

Washington Post
When hackers get into the driver's seat
Saturday, 29 October 2016
Byline: Ashley Halsey III and Michael Laris

Washington - Less than a week after one of the most massive cyber attacks in U.S. history, federal officials want to ensure hackers won't be able to invade the computers that increasingly control automobiles.
Guidelines issued for automakers and developers earlier this week by the National Highway Traffic Safety Administration acknowledge that protecting increasingly autonomous cars from cyber attack will be an ongoing battle.

"In the constantly changing environment of technology and cybersecurity, no single or static approach is sufficient," NHTSA Administrator Mark Rosekind said in a statement released with the new guidance. "Everyone involved must keep moving, adapting and improving to stay ahead of the bad guys."

The NHTSA guidance suggests a layered series of protections that will prevent a vehicle from misbehaving, even when its cyber defences are penetrated.

The goal of the guidance is to make sure cyber security is a key part of designing cars in a world where hackers and foreign powers are all hungry to reach into whatever electronic realm they can, for fun, profit or strategic advantage.

The motives of hackers are as varied as their goals. For some, it's simply to overcome cyber barriers that are established to thwart them. For others, it could be to disrupt the transportation system.

"It's like building a ten-foot wall, and somebody builds an 11-foot ladder," said Paul Brubaker, chairman of the recently formed Alliance for Transportation Innovation.

That said, there are myriad ways to keep hackers from taking control of cars, according to Brubaker. Some of it should be adapted from the military and intelligence communities, areas with which he became familiar when serving as a deputy assistant secretary of defense.

"The knowledge exists to provide state-of-the-art cyber security protection to the fleet," Brubaker said. "The question is will the industry lean into their discomfort and embrace it."

One challenge is simply defining "the industry."

The players who are developing semi- autonomous and truly driverless vehicles range from Google, which has vast experience in defending against hackers, to traditional automakers, whose focus has been more on selling cars than fending off cyber attacks.

"I think the department has given industry an excellent opportunity to step up to the plate," Brubaker said. "I'd like to see some input from folks who are working in the software-defined network world as well as the software- defined radio world to help the department develop some more refined guidance."

The cyber world had a sobering moment last year when two researchers successfully hacked into a Jeep Cherokee, disabling the brakes and transmission to demonstrate the vehicle's vulnerability. They entered the car electronically through its self-parallel-parking feature. Chrysler later issued a software patch to fix the flaw.

Just as federal officials put up out-sized planters around government buildings to prevent attacks, and Internet companies have invested in ways to counter hackers, the goal of the guidance is to "harden the vehicle's electronic architecture" against potential attacks.

To do that, there's a lot of talk about being "risk based," which basically just means companies should be deliberate about figuring out where things might go particularly badly and focus on those first. The non-binding guidance recommends that "safety-critical vehicle control systems" -- things like brakes, acceleration and steering -- should be the priority, along with "personally identifiable information."

One key step is "creating an inventory" of "all vehicles and vehicle equipment that have some form of connectivity to each other or to other services," the guidelines say.

Once risks are identified, companies should also put in place "rapid detection and remediation capabilities," according to the voluntary "best practices."

"If a cyber attack is detected, the safety risk to vehicle occupants and surrounding road users should be mitigated and the vehicle should be transitioned to a reasonable risk state," the guidance says.

Which translates to: Figure out what's happening and find a way to cut the danger fast. Of course, that's easier said than done, which makes this such a fraught area.

New York Times
F.B.I. Chief James Comey Is in Political Crossfire Again Over Emails
Saturday, 29 October 2016
Byline: Multiple Reporters

Washington - James B. Comey, the director of the F.B.I., faced a dilemma on Thursday when deputies briefed him about a new trove of emails, discovered in the course of an investigation of former Representative Anthony D. Weiner, that they said might be connected to the dormant inquiry into Hillary Clinton's private email server.
Mr. Comey, who had cleared Mrs. Clinton of any criminal wrongdoing in the email affair this summer, could let Congress know about the new developments immediately, bureau officials said, an unusual step that would risk accusations that he was unfairly harming Mrs. Clinton's presidential campaign less than two weeks before the election.

Or he could delay any announcement and examine the new emails more closely, risking criticism that he had suppressed important new information if it came out after the election, despite his pledges of "transparency" in the investigation.

Mr. Comey, a Republican appointed by President Obama three years ago, decided that he could live with criticism of his judgment, aides said. So on Friday morning, the F.B.I.'s congressional liaison emailed a letter from the director to the chairmen of eight congressional committees -- virtually ensuring that it would be quickly publicized by eager Republicans.

The reaction was swift and damning, with Mrs. Clinton's supporters and even some Republicans blasting Mr. Comey. Indeed, Mr. Comey, who was attacked this summer by Democrats and Republicans for both his decision not to bring charges against Mrs. Clinton and for the way he handled it, found himself in an even stronger cross-fire on Friday.

By late Friday, Mr. Comey felt it necessary to further explain his actions in an email to F.B.I. employees in which he acknowledged that "there is significant risk of being misunderstood." He explained that he was trying to balance the obligation he felt to tell Congress that the investigation he had said was completed was continuing, with not knowing yet "the significance of this newly discovered collection of emails."

Across Pennsylvania Avenue from the F.B.I., Justice Department officials were said to be deeply upset about Mr. Comey's decision to go to Congress with the new information before it had been adequately investigated.

That decision, said several officials who spoke on condition of anonymity, appeared to contradict longstanding Justice Department guidelines discouraging any actions close to an election that could influence the outcome.

One official complained that no one at the F.B.I. or the Justice Department is even certain yet whether any of the emails included national security material or was relevant to the investigation into whether Mrs. Clinton had mishandled classified material in her use of a private email server.

"The F.B.I. has a history of extreme caution near Election Day so as not to influence the results," Senator Dianne Feinstein, Democrat of California, said in a statement. "Today's break from that tradition is appalling,"

"Was this information Congress needed to know urgently? Of course not," said Matthew Miller, a Clinton supporter who was the chief spokesman at the Justice Department under former Attorney General Eric H. Holder Jr.

Some Republicans praised Mr. Comey on Friday for his integrity and independence in coming forward with the new information. But praise was largely drowned out by criticism, with even some of Mrs. Clinton's biggest opponents upset at Mr. Comey's sudden re-emergence in what they said was a bungled case.

"This is as bad for Comey as it is for Hillary," said Tom Fitton, president of Judicial Watch, a conservative advocacy group that has successfully sued for access to thousands of Mrs. Clinton's private emails.

Mr. Fitton said that the cryptic nature of Mr. Comey's letter to Congress begged for an explanation as to what new material the F.B.I. had found, whether it involved national security material relevant to the initial investigation, and why it was not found earlier.

"This letter raises all sorts of questions that Comey and the F.B.I. should have to answer," Mr. Fitton said. "They can't roll this out in the middle of a presidential campaign and just leave it at that."

F.B.I. officials said Mr. Comey was well aware that his decision would draw fire from many sides. Mr. Comey -- who at 6-foot-8 is a dominating and charismatic figure -- has not shied from the public spotlight and has shown an independent streak throughout his career.

As deputy attorney general in the George W. Bush administration, he butted heads with top White House officials for his refusal to sign on to a National Security Agency surveillance program. And he clashed with President Obama and other administration officials last year over what he saw as a "Ferguson effect" discouraging the police from actively pursuing suspects.

Mr. Comey and his aides had hoped to put the Clinton email controversy behind them this summer, when he decided -- in unusually public fashion - not to seek criminal charges against Mrs. Clinton or anyone else after a yearlong investigation.

But tensions have lingered, with Mr. Comey facing sharp second-guessing from Republicans on Capitol Hill and ongoing questions from even his allies.

The investigation of Mrs. Clinton and her aides has been a major reason the bureau, more than at any time since at least the Watergate era, has been drawn uncomfortably into a presidential campaign.

This month, when the moderator at a conference of police chiefs in San Diego asked him about the email controversy, Mr. Comey turned the question into a laugh line. "I appreciate you bringing it up," he deadpanned. "That's behind us. Nobody really cares anymore." The chiefs responded with knowing laughter.

Mr. Comey got so many calls from former agents and others after he decided this summer not to pursue charges in the investigation that he had to change his phone number posted online. And at a recent meeting with retired agents, he was still fielding tough questions about the decision.

"I have no patience for suggestions that we conducted ourselves as anything but what we are -- honest, competent, and independent," Mr. Comey wrote in a September email to employees. "Those suggesting that we are 'political' or part of some 'fix' either don't know us, or they are full of baloney (and maybe some of both)."

But while the relentless Republican criticism of Mr. Comey's decision not to bring charges against Mrs. Clinton has received the most attention, both Democrats and Republicans have sought to help their presidential candidates, demanding investigations into their rivals one moment, then slamming Mr. Comey the next.

In recent months, the F.B.I. has dealt with the fallout from the email decision, wrestled with whether to pursue tips about the Clinton family foundation and opened a wide-ranging counterintelligence case into whether Russia is trying to influence the election. Just this week, the F.B.I. defended itself from accusations that Democrats had curried favor with the deputy director by making donations to his wife's failed State Senate campaign in Virginia.

F.B.I. agents say their community meetings invariably lead to questions about what the bureau is or is not doing in connection with the election. Mr. Comey has urged his agents to stay above the fray. But many of them worry that regardless of the election's outcome, the F.B.I. might end up the loser.

"I've never seen it this bad," said Robert E. Anderson Jr., who retired last year as the most senior agent overseeing criminal and cyber investigations. "I don't know if it's a low point for the bureau or the entire political process."

New York Times
WikiLeaks Lays Bare a Clinton Insider's Emphatic Cheers and Jeers
Sunday, 30 October 2016
Byline: Nicholas Confessore & Steve Eder

Washington - In one note, Neera Tanden groused that whoever had let Hillary Clinton use a private email address for her State Department correspondence should be "drawn and quartered."
In another, she called for Mrs. Clinton to stop stalling on whether she opposed the Keystone pipeline, worrying that "dodging another issue" would hurt her in the Democratic primaries.

And when Mrs. Clinton's team dallied over whether to publicly criticize David Brock, a longtime ally, for demanding Senator Bernie Sanders's medical records, Ms. Tanden was blunt.

"Hillary. God," Ms. Tanden wrote. "Her instincts are suboptimal."

Ms. Tanden, 46, a longtime policy adviser to Mrs. Clinton, is well known on Twitter and cable news for her peppery defenses of Mrs. Clinton and her sarcastic takedowns of Mrs. Clinton's perceived adversaries.

But her private communications with some of Mrs. Clinton's campaign aides, stolen from campaign chairman John D. Podesta and published over the last month by the activist group WikiLeaks, have revealed another side. In a sphere encrusted with suck-ups, soothers, and self-puffery, Ms. Tanden has emerged as a loyal but insistent straight- talker and acute assessor of Mrs. Clinton's stubbornness and weaknesses.

"What the emails show is somebody who is passionately invested in Hillary Clinton giving the best possible candid advice she can to advance her electoral prospects," said Howard Wolfson, a former Clinton aide and a close friend of Ms. Tanden's. He added, "And giving it privately."

The Clinton campaign declined to comment on the emails, instead saying that the hack was a product of the Russian government's meddling in the election to benefit Donald J. Trump, the Republican nominee.

But as dozens of her stolen messages have gone public, Ms. Tanden's private and profanity-laced commentary has made her something of a cult hero for an unlikely group: Trump supporters. On a Reddit page called "The_Donald," where Trump backers dissect the hacked email releases and post their findings, Ms. Tanden has garnered a slew of unwanted praise. One Trump fan called for a Neera Tanden fan club. Another dubbed her "NoFilterNeera."

Most of the stolen emails were exchanges between her and Mr. Podesta, her former boss at the Center for American Progress, a liberal think tank that Ms. Tanden now leads. Mr. Podesta is a longtime friend, and Ms. Tanden's tone is often that of a colleague grousing in the break room.

In the exchanges, Ms. Tanden can be fiercely protective of Mrs. Clinton. When Jennifer Palmieri, communications director of the Clinton campaign, wrote a sharply worded letter raising concerns about coverage of Mrs. Clinton in The New York Times, Ms. Tanden cheered. The letter "is great," she wrote to Mr. Podesta -- adding a sentence laced with profanities directed at the newspaper.

But she could also be direct about other members of Clintonworld and the candidate herself.

When news media reports began identifying potential members of Mrs. Clinton's campaign team last year, Ms. Tanden warned of griping among Democrats about racial and gender balance among Mrs. Clinton's staff picks. "I'm not the diversity police but there is grumbling on the 4 white boys running next presidential cycle," she wrote in January 2015. "So I recommend rolling out some people who look like the rest of America soon!"

In May 2015, New York City's mayor, Bill de Blasio, emailed Ms. Tanden and Mr. Podesta to let them know that he was scheduled to appear on the MSNBC show "Morning Joe" and would likely offer his opinion of Mrs. Clinton's policy vision.

"I find him a bit insufferable," Ms. Tanden wrote to Mr. Podesta. (The mayor was frozen out over the ensuing months and denied a prime speaking slot at the Democratic convention this summer.)

Ms. Tanden's internal critiques may have damaged her relationships with other members of the concentric Clinton circles, and in the immutable fashion of Washington, she seems more likely to be punished than rewarded for her honesty. Asked about the WikiLeaks releases, Ms. Tanden said in an email that while she would not authenticate any of the messages, their leaking had been "a profoundly painful experience."

"Having been a bit beaten up in the media over the last month myself, I have even greater appreciation for someone who has weathered it for 20 years," Ms. Tanden said of Mrs. Clinton, calling her a "role model." She added, "My personal efforts have been to help her be successful."

Philip J. Crowley, a former Clinton aide at the State Department who resigned in 2011 after publicly criticizing the Department of Defense for its treatment of a soldier accused of classified leaks, said he believed Ms. Tanden would still be welcome in Mrs. Clinton's inner sanctum.

"Will there have to be some conversations and a couple of beers and a mea culpa afterwards?" Mr. Crowley said. "Sure there will. But those who are experienced in the ways of Washington know how to work this."

Some of Ms. Tanden's sharpest internal criticisms concerned Mrs. Clinton's private email account, which prompted a federal investigation that is plaguing Mrs. Clinton anew. On Friday, the Federal Bureau of Investigation said it had uncovered a new trove of emails after seizing an electronic device shared by Anthony D. Weiner and his estranged wife, Huma Abedin, a top aide to Mrs. Clinton.

When Ms. Tanden first saw news reports about the private account in March 2015, she exchanged a series of emails with Mr. Podesta bemoaning how they had gotten into such a situation in the first place. She singled out other aides, including Cheryl D. Mills, a longtime senior adviser, for not recognizing the danger sooner.

"This is a cheryl special," Ms. Tanden wrote. "Know you love her, but this stuff is like her Achilles heel. Or kryptonite. she just can't say no."

As the controversy wore on, Ms. Tanden griped about the White House "crapping" on Mrs. Clinton, and insisted that Mrs. Clinton ought to make a public statement right away. She noted that Mrs. Clinton, after years of enduring attacks and scandals she regarded as trumped-up, had a tendency to be stubborn about acknowledging error.

"She always sees herself bending to their will when she hands over information, etc.," she wrote in August 2015. "But the way she has to bend here is in the remorse. Not the 'if I had to do it all over again, I wouldn't do it.' A real feeling of -- this decision I made created a mess and I'm sorry I did that."

In early September, Mrs. Clinton gave a series of interviews in which she apologized for the email issue. Mrs. Tanden joked that after one of the interviews, she "was able to breathe again."

Ms. Tanden was alert to the potential threat posed by Mr. Sanders's outsider campaign. She cautioned Mr. Podesta that aggressively going after Mr. Sanders could backfire.

"Just game out what that does to Hillary," she wrote in August 2015. "When we went after Obama, she got killed for it. Reaffirmed all her negatives, strengthened him. We had no idea it was kryptonite for us to do that, but it was."

If Ms. Tanden seemed particularly on guard, perhaps it was because she knew what a failed Clinton campaign looked like -- and how painful it could be.

During Mrs. Clinton's 2008 presidential run, Ms. Tanden wrote to Mr. Podesta about her malaise as it ended.

"I am really profoundly sad today. I thought I was over it," she wrote. "But here I am sad. She's not conceding tonight. ... And not anytime soon, either."

* For Democrats, New Focus on Clinton Email Is 'Like an 18- Wheeler Smacking Into Us'

New York Times
N.S.A. Appears to Have Missed 'Big Red Flags' in Suspect's Behavior
Sunday, 30 October 2016
Byline: Scott Shane

Washington - Year after year, both in his messy personal life and his brazen theft of classified documents from the National Security Agency, Harold T. Martin III put to the test the government's costly system for protecting secrets.
And year after year, the system failed.

Mr. Martin got and kept a top-secret security clearance despite a record that included drinking problems, a drunken-driving arrest, two divorces, unpaid tax bills, a charge of computer harassment and a bizarre episode in which he posed as a police officer in a traffic dispute. Under clearance rules, such events should have triggered closer scrutiny by the security agencies where he worked as a contractor.

Yet even after extensive leaks by Pfc. Bradley Manning in 2010 and Edward Snowden in 2013 prompted new layers of safeguards, Mr. Martin was able to walk out of the N.S.A. with highly classified material, adding it to the jumbled piles in his house, shed and car.

A federal judge in Baltimore ruled on Friday that Mr. Martin, 51, must remain jailed on charges of stealing government documents and mishandling classified information over two decades. Prosecutors say they will add new charges under the Espionage Act. Mr. Martin, whose arrest in August was disclosed by The New York Times this month, has admitted to taking the material but denies giving secrets to anyone else.

His actions, which prosecutors described in court as "breathtaking," have already cast a harsh light on the government's ability to police the 3.1 million employees and 900,000 contractors who hold clearances -- or even the much smaller number who work inside the most closely guarded programs, as Mr. Martin did. His case appears to show serious breakdowns in personnel evaluation, technology designed to detect leaks and the basic job of inspecting people leaving secure buildings.

Dennis C. Blair, a former director of national intelligence, said he was "shocked" that Mr. Martin managed to remove classified material in bulk as recently as this year, in part because the government has spent tens of millions of dollars since 2010 on measures to prevent unauthorized activity or downloads.

"If there are breakdowns in your security system, as there clearly were with Snowden and this guy, you have to look at whatever went wrong and fix it," Mr. Blair said.

Some intelligence officials sounded a defensive note. William R. Evanina, the government's top counterintelligence official, said it may be infeasible to prevent every breach at an agency like the N.S.A., with 35,000 employees.

"I don't think it's possible," Mr. Evanina said. He credited the government with doing "an amazing job" in tightening security and called the N.S.A. "one of the leaders." Despite such efforts, he said, "if someone is intent on stealing classified data, it's very hard to stop them."

But a look at Mr. Martin's past raises a question: Did his erratic behavior ever prompt a review of his top secret clearance, which allowed him to work on some of the nation's most sensitive intelligence operations over two decades at eight contractors? His record of personal and legal troubles reads like it might have been drawn from the official list of factors that can be used to deny a clearance.

In 2000, the State of Maryland put an $8,997 lien on Mr. Martin's property for unpaid taxes that he would not pay off till 2014, a sign of chronic financial difficulties. In 2003, he was charged with misdemeanor computer harassment, a result of pestering a woman with unwanted messages. The charge was eventually dismissed.

Mr. Martin has a history of "binge drinking on a monthly basis," Judge Richard D. Bennett of Federal District Court said in a detention hearing on Friday. Alcoholism does not automatically block a security clearance, officials say, but the person must acknowledge the issue and seek treatment.

In 2006, Mr. Martin was charged with driving under the influence. In 2008, he cut off another driver and in the ensuing argument, announced that he was a police officer, according to two acquaintances who did not want to be named speaking critically of him. When it turned out the other driver was an off-duty state trooper, Mr. Martin fled. The local police charged him in the incident, but the record of the episode was later expunged.

"Those are all big red flags, and reasons why you wouldn't get a clearance," said Ross Schulman, a cybersecurity expert at the Open Technology Institute at New America, a Washington research group. "What seems clear in this case is that they dropped the ball in choosing who to allow access to their material and computers in the first place."

The year after the episode of police impersonation, Mr. Martin was hired by the contractor Booz Allen Hamilton, for whom he would work at the N.S.A. for the next six years before being moved in 2015 to a Pentagon job involving offensive cyberwarfare.

A routine five-year renewal of his security clearance in 2012 should have covered all his legal tangles and the breakup of his two marriages, in the late 1990s and 2010. Such reviews include a polygraph test, in which a standard question asks about mishandling of classified information. If such a question was asked, Mr. Martin appears to have passed the polygraph.

In recent years, intelligence agencies have begun to bolster the five-year reviews with "continuous evaluation," said Mr. Evanina, the counterintelligence chief. That means public databases showing criminal or civil cases, unpaid debts and divorces should all be scanned constantly for the names of clearance-holders, he said.

In a major upgrade to the security system after the transfer of military and diplomatic files by the former Army private now known as Chelsea Manning to WikiLeaks in 2010, the N.S.A. and other agencies installed specialized software to detect unusual conduct on agency networks or large downloads of secret data. Agencies also cracked down on removable storage devices like CDs and thumb drives, literally gluing drives shut or disabling the software required to use them.

But one former senior intelligence official suggested that Mr. Martin might have dodged those safeguards because he was assigned to Tailored Access Operations, the N.S.A. hacking unit. Because the unit develops malware to break into foreign computer networks and steal secrets, its machines are segregated from N.S.A.'s main network to avoid the possibility that a rogue program could get loose and do damage.

In the separate network, the electronic alarms that sound for unusual downloads may not operate and the ban on thumb drives does not always apply, said the official, who spoke on the condition of anonymity because the investigation is continuing. "By the nature of the work he's in, you have to carve that out so as not to do harm to your own system," he said.

The last chance to stop someone from carrying off secrets is at the gates to N.S.A. facilities. Mr. Martin's lawyer, James Wyda, said in court that "there was nothing sophisticated Mr. Martin did to remove this information" from the agency. But before the lawyer could elaborate, prosecutors abruptly objected, evidently concerned about the message that security is lax.

Only the most intrusive search would detect papers or a small drive hidden under clothing, and officials fear that universal searches would be impractical and send a message of mistrust.

"You don't want to create a Stasi-like atmosphere," said Michael V. Hayden, a former N.S.A. and C.I.A. director, referring to the East German secret police. Instead, N.S.A. guards carry out random searches, which sometimes included the director, he said.

Several former N.S.A. workers said that if Mr. Martin was ever caught with a few classified pages, he might have pleaded absent-mindedness and escaped punishment. But F.B.I. agents who took 50 terabytes of data from his house found it on disks, hard drives and thumb drives. Had security guards found any of those leaving the agency, it would have set off an investigation, Mr. Martin's former colleagues said.

The N.S.A. is now conducting an internal review to track everything Mr. Martin took to its source to understand the breaches, officials said. But the case has reinforced how technology that makes it easy to store and move huge volumes of data can threaten security, Mr. Hayden said.

As more details on the case emerged last week -- including prosecutors' assertion that the documents Mr. Martin took contain the names of some intelligence officers who worked undercover -- Booz Allen Hamilton announced that it had hired the former F.B.I. director Robert S. Mueller III to review its security and management practices. For Booz Allen, Mr. Martin's arrest was a second devastating blow: Mr. Snowden was also an employee when he took hundreds of thousands of N.S.A. documents in 2013.

Senator Dianne Feinstein, the vice chairwoman of the Senate Intelligence Committee, said she expected the committee to examine the incident, both to review whether recent security upgrades at N.S.A. are sufficient and consider further improvements.

In court on Friday, Judge Bennett concluded that Mr. Martin posed too much of a flight risk to release before trial. Though there is no proof so far that Mr. Martin passed the secrets he took to others, "the harm has already occurred," the judge said, "in terms of the loss of confidence on the part of the public" in the intelligence agencies.

Bahrain News Agency
Oman participates in regional cybersecurity summit
Monday, 31 October 2016

Manama - The Sultanate of Oman has participated in the fifth Regional Cybersecurity Summit, which started Sunday in Sharm El Shaikh, Egypt. The summit is organized by the Arab Regional Cybersecurity Centre at the International Telecom Union (ITU) under the theme "Boundless Collaboration, Boundless Protection" and hosted by the National Telecommunication Regulatory Authority (NTRA).

The two-day event attracts over 300 plus CISO's senior ICT and cybersecurity officials from the MENA region, according to Oman News Agency (ONA).

The summit aims at creating shared learning and dialogue regarding cyber security challenges and issues, facilitating the exchange of information, ideas, solutions, and emerging practices that could improve cyber security posture, as well as identifying current priority areas in cyber security at the local, regional and international levels. It also seeks to enhance cross border collaboration with government, industry and critical infrastructure stakeholders that will impact regional and international preparedness.

The summit discusses potential threats and measures, as well as enhancing the cooperation between MENA regions to recognize and resolve these issues rather than only protecting their assets with the latest technologies. Furthermore, it seeks to introduce the strategic directions and plans to tackle emerging threats to the global and regional information security sector, ONA reported.

Tribune de Genève
La surveillance des données inquiète l'ONU
Monday, 31 October 2016
Byline: A.J.

Non identifié - Un expert s'étonne de voir que Yahoo a dû se plier aux demandes américaines Dernièrement, on apprenait que Yahoo avait dû espionner les courriels de ses clients à la demande des services de renseignement américains. Pour le rapporteur spécial des Nations Unies sur le droit à la liberté d'opinion et d'expression, David Kaye, c'est un vrai sujet de préoccupation. Yahoo aurait utilisé un logiciel pour analyser le trafic des boîtes mails de millions de clients dans le but de trouver les informations demandées par l'Agence de sécurité nationale des Etats-Unis et le FBI.

« La surveillance gouvernementale des communications numériques, lorsqu'elle est effectuée comme cela a été expliqué récemment, pourrait porter atteinte à la vie privée » , estime l'expert de l'ONU.

« Sur la base des allégations rapportées, je crains que la surveillance exercée de cette sorte ne réponde pas aux normes de nécessité et de proportionnalité pour la protection des intérêts légitimes d'un gouvernement » , observe-t-il. « L'adhésion apparente de Yahoo aux demandes de surveillance du gouvernement, sans contestation judiciaire évidente, soulève également une préoccupation quant à l'implication des entreprises technologiques dans les programmes gouvernementaux douteux » , ajoute David Kaye.

Dans un rapport remis au Conseil des droits de l'ONU sur la surveillance des communications en 2013, le rapporteur spécial précédent, Frank La Rue, avait conclu que « l'accès aux données de communication détenues par les acteurs des entreprises nationales » ne devait être envisagé qu'après que les « techniques moins invasives disponibles » ont été épuisées.

Montreal Gazette

Snowden: Spying by police 'radical attack on free press'

Thursday, 03 November 2016

Byline: Karen Seidman

Section: general

Montreal - To some, whistleblower Edward Snowden is a traitor. To others, he's a hero.
Whichever way you see him, Snowden - a former CIA employee and contractor for the National Security Agency (NSA) who is responsible for the largest national security breach in U.S. history - is a pivotal figure in any debate pertaining to the issue of government surveillance.

He is one of the most wanted fugitives in the world after leaking thousands of classified NSA documents to a few journalists in 2013. His disclosures revealed, among other things, that U.S. telecommunications companies were providing the NSA with virtually all their customers' phone records and that the NSA has a tool to search nearly everything a user does on the Internet.

So Snowden's talk at McGill University Wednesday night, as the city is in an uproar over police spying on La Presse reporter Patrick

Lagacé and possibly much more widespread spying as well, was timely and promised to ignite an already fierce debate on authorities overstepping their bounds and cyber spying on their own citizens.

Students lined up across the length of the campus to see him and McGill officials had to scramble to set up overflow rooms. When Snowden's giant image finally showed up on the screen, almost 90 minutes late, he was greeted with thunderous applause.

Here's what Snowden had to say, from his hideout in Russia, on some important issues: Montreal spying scandal: "The story about Montreal police spying on a journalist for the reason of uncovering sources is a radical attack on the free press," he said. "It unsettles me. It's a threat to the traditional model of our democracy." Now, he said, local police can decide that if they don't like a certain reporter, they can ask a judge to monitor their phones. It used to be such measures were reserved for real criminal threats; now they

have been repurposed to monitor journalists.

The Internet age and surveillance: We're all being watched and that's what drove Snowden to be a whistleblower. Months before he leaked the classified documents, he heard the head of the NSA outright lie, under oath, about the use of surveillance techniques. "Surveillance technologies have outpaced democratic controls," he said. Surveillance used to be too expensive to use much. Now, he said, one guy at the NSA can track with extreme precision a large number of people. "It's become technologically and financially feasible to track people."

Intelligence agencies and authorities: How do we trust intelligence agencies and officials to operate fairly? We can't, he said. Governments should establish judicial bodies with independent prosecutorial discretion to monitor these agencies and to prosecute any illegalities. "The only thing that will ensure they play fairly is the threat of criminal sanctions," said Snowden. They need to be held accountable. And the law has been failing as a guarantor of our rights, he said.

The U.S. election: He's very disappointed that the United States is going through an entire election cycle that has focused on the personalities of the candidates - with no mention of the Constitution. In any case, people should be cautious about putting all their hopes on any one political figure because they rarely deliver what they promise, Snowden said. "You can't rely on others to do the things we must do ourselves," he said. "If you want a better country, you're going to have to build it yourself."

Snowden said that while he gets a lot of attention when it comes to surveillance issues, he considers himself the least important part of the story.

Anyone who is thinking of him or his future is missing the bigger story: "What is happening to all of us."

Montreal Gazette

From words to action

Thursday, 03 November 2016

Section: general

Editorial: The bombshell that Montreal police spied on La Presse columnist Patrick Lagacé through his cellphone has prompted political leaders at all levels to speak out in defence of a free press.
Their words must be matched by action. To his credit, Quebec Premier Philippe Couillard moved swiftly to shore up protections for the media to conduct their essential work. Almost immediately, the bar will be set higher for police seeking search warrants against journalists, who will be accorded a status similar to that of lawyers, judges and MNAs.

Couillard struck a working group with representatives of the judiciary, policing and the media to make recommendations to fortify the work of journalists, a crucial pillar of a democratic society.

Among issues the group should consider is what specialized training should be required for the justices of the peace who sign offon the warrants like the ones concerning Lagacé, to ensure that they are aware of journalists' Supreme Court of Canada-recognized right to keep sources confidential. The group should also advocate better whistleblower protection, as recommended by the Charbonneau Commission, given that the Lagacé case highlights the vulnerability of sources.

Couillard initiated a probe of the Montreal, Quebec City and provincial police forces by the public security department; whether it will yield the needed answers remains in question. Unearthing the motivations and full context underlying police conduct here is crucial. So, too, is determining how widespread the practice of spying on journalists has been, as new reports surfaced Wednesday that the Sûreté du Québec was monitoring the cellphones of six journalists in 2013.

Montreal City Hall has a duty to act, too. Mayor Denis Coderre was slow to acknowledge the enormity of this disturbing episode. Police Chief Philippe Pichet has since been summoned to explain himself before the city's public safety committee. The hearing was held behind closed doors, but Coderre said a report will eventually be made public.

Transparency here is a necessity. Citizens deserve to hear what Pichet knew about this affair and when, why his force seems to be devoting so many resources to exposing officers who speak to reporters and what, if any, consequences will be meted out.

This is also a matter for federal attention. Without stronger protection for journalists and their sources, this could happen again.

The opposition wants an inquiry and is promising a private member's bill if the federal government itself doesn't act.

Politicians have rightly denounced this attack on press freedom. But how they respond now will have major repercussions on the integrity of the justice system.

CBC News

6 reporters spied on by Quebec provincial police

Thursday, 03 November 2016

Byline: Sabrina Marandola

Section: general

Quebec provincial police confirm that six members of the press were spied on in 2013 as part of a police investigation that was launched on the same day that a labour union boss filed a complaint.
Three Radio-Canada journalists said they found out today, via unnamed sources, that the Sûreté du Québec was tracking their portable phones. This comes just days after a Montreal newspaper columnist said he was similarly tracked by that city's police force.

Marie-Maude Denis and Isabelle Richer, the current hosts of the investigative program Enquête, as well as the show's former host Alain Gravel, said this afternoon that provincial police were tracking their incoming and outgoing calls and texts.

"I've just learned that my incoming and outgoing calls have been spied on by the Sûreté du Québec in 2013," Denis tweeted in French.

"My turn to get a confirmation that I was targeted by court mandates to obtain a log of my calls by the SQ," Gravel said.

Je viens d'apprendre que mes appels entrant et sortant ont été espionnés par la Sûreté du Québec en 2013.

-- @mmdenisrc

À mon tour d'avoir la confirmation comme quoi j'ai été visé par des mandats de cour pour obtenir le registre de mes appels par la SQ.

-- @gravela_rc

"Surreal ... The SQ spied on my cellphone following a formal complaint made by Michel Arsenault in 2013," Richer tweeted.

Surréaliste... La SQ a espionné mon cellulaire à la suite d'une plainte formulée par Michel Arsenault en 2013

-- @IsabelleRicher

Journal de Montreal crime reporter Eric Thibault was also under surveillance, as was La Presse's National Assembly bureau chief Denis Lessard. Another journalist, whose name hasn't been released, was also monitored.

Surveillance prompted by complaint

Arsenault's name came up a number of times at the Charbonneau Commission when, in 2013, the province's anti-corruption inquiry turned its attention to unions.

The then-president of Quebec's Federation of Labour (FTQ) came under fire after witnesses testified that Arsenault was aware of alleged links between some union leaders and organized crime but did nothing about it.

He had also been involved in a legal battle with the commission over wiretaps of his phone conversations, gathered by police in an investigation unrelated to the anti-corruption inquiry.

Arsenault sent a letter of complaint to the SQ after news that he was the subject of a police investigation was being made public.

"Michel Arsensault was under scrutiny at the time. He was upset, so he complained to the SQ, which forced police to do an inquiry ... So they decided to ask for this warrant to spy on our cellular phone," Richer said.

'We still have sources'

Richer said the three learned they had been spied on by police thanks to unnamed sources.

"We still have sources. A source told us today that we were the target of this warrant in 2013, and maybe before. Maybe we were spied for a long period of time. We don't know because those warrants are still sealed," Richer said, adding that today's revelations show that spying on journalists is systematic.

"What floored me is that this is no longer the culture at the SPVM," she said, referring to the Montreal force by its French initials. "It is also the Sûreté du Quebec."

"It's a widespread practice. With the facts we have now, it was a widespread practice," Denis added.

"It's a shock," said Gravel. "In a democratic society like ours, you never imagine that this thing could happen and be so systematic. It's two events now in the same week. So we're very concerned."

Only case in 20 years, SQ says

The Sûreté du Québec responded to the revelations late Wednesday afternoon, confirming the allegations but adding that it was the only such case in the last 20 years.

"We're talking about one case, which is one case too many, but one case going all the way back to 1995," SQ spokesman Capt. Guy Lapointe told CBC.

"The investigation targeted different individuals, some of them were reporters."

The SQ said that the investigation was closed and sealed in 2014. Current staff only found out about it now because they started looking into their procedures after the province yesterday asked police forces to investigate how they go about getting warrants.

Lapointe said that since 2013, new people and new protocols are in place at the SQ.

"You have to understand that this occurred with the prior administration of the SQ....Any investigation that is targeting a reporter...[now] needs to be authorized by the high direction, and any kind of warrant that would be obtained towards this investigation needs to be approved by the director himself."

Province to launch inquiry

Quebec Public Security Minister Martin Coiteux said the province will put together an expert panel and launch an administrative inquiry.

He said there will be an inspection of police, including the anti-corruption squad UPAC.

The inquiry will "inspect the police forces and look at the policies in place," Coiteux said. "There could be sanctions."

He also said it was "odd" that police launched an investigation on the same day that then-SQ director general Mario Laprise received a complaint from former union boss Arsenault.

"It is very peculiar. The head of the FTQ calls the SQ first thing in the morning, and that night an investigation is launched. This is a unique case which raises questions on its own, but it is the only such case in the last 20 years," Coiteux said.

When contacted by Radio-Canada, Laprise refused to comment on the matter. He would only say that the inquiry will have to take its course.

"I think we will have to wait and we will let the people do their jobs," Laprise said.

Radio-Canada said it had information that Parti Québécois MNA Stéphane Bergeron, who was Quebec's public security minister in 2013, was the one who asked Laprise to look into the FTQ case.

Bergeron denied it.

"I never asked for surveillance. It's an action that I would have never authorized. It's an initiative that I was never informed of until a few moments ago," Bergeron said Wednesday afternoon.

'A crisis'

Earlier this week, the Montreal newspaper La Presse revealed one of its columnists was the subject of a police warrant to track his cellphone communication.

Montreal police obtained 24 warrants this year to track Patrick Lagacé's whereabouts using the GPS chip in his iPhone, and to obtain the identities of everyone he communicated with.

The news prompted political leaders to call for a greater protection of journalists.

La Presse announced this afternoon it was taking legal action against the Montreal police force.

"I don't think we've seen such a crisis here in the history of journalism. We have to get the facts and then make sure that measures are taken to make sure this doesn't happen again," said Gravel.

It's not clear if the tracking is still going on because the warrants are sealed. The warrants for Lagacé will be unsealed on Nov. 24. It is not known when the warrants for the Radio-Canada reporters will be **unsealed.**
Canadian Press

Sen. Andre Pratte wants stronger protection for reporters, sources

Thursday, 03 November 2016

Byline: Jim Bronskill

Section: general

Ottawa - Independent senator and former journalist Andre Pratte wants the Liberal government to look seriously at beefing up protection for reporters and their sources.
Pratte says if the government shows no interest, he'll pursue the idea himself.

It is "quite worrisome" that Montreal police obtained warrants to monitor one of his former colleagues, La Presse columnist Patrick Lagace, Pratte said Wednesday in an interview.

"I think it is time to look at this again."

The newspaper said this week it had learned at least 24 surveillance warrants were issued for Lagace's iPhone this year in connection with an internal probe into allegations police anti-gang investigators fabricated evidence.

Public Safety Minister Ralph Goodale says the Supreme Court of Canada has already explicitly laid out the test that must be satisfied when police investigations intersect with media freedoms.

In two key 2010 rulings, the high court did not create blanket constitutional protection for journalists, saying they are a "heterogeneous and ill-defined group of writers and speakers." Instead, the court spelled out a four-point test that allows judges to weigh competing public interests on a case-by-case basis.

The Lagace case shows something more is needed, said Pratte, former lead editorial writer at La Presse.

"I don't think we can simply say, 'The Supreme Court has issued those criteria, and they're good enough.' Well, obviously, they were not good enough to protect Mr. Lagace and his sources for a period of five months."

Despite his apparent reluctance to revisit the existing regime, Goodale left the door open a crack.

"If there are those in the federation of journalists or others who have recommendations to make about how this can be more abundantly emphasized, I would certainly be glad to receive their recommendations," he said Tuesday.

Pratte said he would contact the Liberal government for a direct answer about whether it will consider a new law.

"And if they show no interest in doing it, certainly I am looking at it," he said.

"These are very complex issues, but I think we have to look at them ... especially in the light of the Lagace affair.

"If I have a strong belief that a bill is possible and a good way to go at it, I will certainly work on it and try to get a bill on the floor of the Senate."

Former Bloc Quebecois MP Serge Menard introduced a private member's bill in 2007 to bolster protection for journalistic sources, but it did not become law.

"That may be a starting point for writing a bill," Pratte said. "What I hope will not happen is that in a couple of days, after all the emotion has disappeared, everyone will forget about it."

It emerged late Wednesday that at least six Quebec journalists working for various outlets had recently come under police surveillance.

In response to the Lagace case, Quebec Premier Philippe Couillard announced a committee of experts will look into media surveillance. He also outlined plans to make it harder for police in that province to obtain a judicial warrant to monitor journalists.

Globe and Mail

More Quebec journalists confirmed as targets of police surveillance

Thursday, 03 November 2016

Byline: Ingrid Peritz

Section: general

MONTREAL - A controversy over police surveillance of the press in Quebec deepened Wednesday with revelations that six journalists, including some of the province's top investigative reporters, had their cellphones surreptitiously monitored by provincial law enforcement as far back as 2013.
The disclosures made by several media outlets and confirmed by the provincial Sûreté du Québec suggest that covert police surveillance of Quebec journalists dates further back and is more widespread than previously known.

La Presse revealed this week that one of its journalists, columnist Patrick Lagacé, had his iPhone data tracked by Montreal police for months this year after they obtained search warrants. On Wednesday, Quebec provincial police said it had also obtained court warrants to monitor the log of incoming and outgoing cellphone calls of six journalists.

The raft of disclosures has fuelled a growing sense of alarm over state surveillance of the press. On Wednesday evening, Quebec Public Security Minister Martin Coiteux told reporters his department would lead an administrative probe into the 2013 surveillance case at the Sûreté du Québec. It had been requested by its current director-general, Martin Prud'homme.

The force was under the leadership of another chief, Mario Laprise, in 2013.

"According to the information I have, this would be the only case in the last 20 years affecting journalists targeted by a Sûreté du Québec investigation," Mr. Coiteux said in Quebec City.

Still, news that more journalists were being spied on through their cellphones left several in the media industry shaken and led the executive director of news and current affairs at Radio-Canada, Michel Cormier, to refer to the situation as an "unprecedented crisis." The five that have been identified are affiliated with Radio-Canada, La Presse and Le Journal de Montréal.

"What floors me is that this is no longer the culture of the Montreal police service," Isabelle Richer said on Radio- Canada, where she is a journalist. "It's also the Sûreté du Québec. So it's a generalized hunt for sources." On Twitter, she called the news "surrealistic."

Police say the calls were not wiretapped.

Events that led to the surveillance are also raising eyebrows. They began when Michel Arsenault, former head of the Quebec Federation of Labour, was angry about media reports that he had been the subject of police surveillance. The police actions were part of a criminal investigation into the infiltration of organized crime in the construction industry in Quebec.

Mr. Arsenault complained about the media leaks to the Public Security Minister at the time, Stéphane Bergeron of the Parti Québécois. The Sûreté du Québec investigation into finding the source of the leaks began soon afterwards.

Mr. Bergeron denied on Wednesday he had a hand in ordering the journalist surveillance. "I obviously didn't ask for surveillance. It's an initiative that should have never been authorized, it's an initiative of which I had never been informed," he said.

Captain Guy Lapointe of the Sûreté du Québec said in an interview the current head of the provincial police force, Mr. Prud'homme, is "very irritated" and "preoccupied" that the surveillance had been ordered by his predecessor.

The fresh revelations have given added urgency to opposition calls in Quebec City that the Liberal government of Philippe Couillard hold an inquiry into the controversy. On Tuesday, the Premier attempted to get ahead of the controversy, announcing measures to tighten rules for obtaining search warrants against journalists and striking a panel of experts to look into the situation.

In Ottawa that day, Public Safety Minister Ralph Goodale told reporters his government is open to toughening the rules that govern how and when the federal government can investigate members of the media.

For investigative journalists, reliance on confidential sources is crucial in exposing wrongdoing and holding powerful interests accountable. And investigative journalism played a central role in Quebec in exposing corruption in the construction industry, which led to the creation of the Charbonneau Commission. The public commission produced a report exposing the wide reach of corruption in the province's multibillion-dollar public construction industry and its links to organized crime.

Meanwhile, La Presse is seeking to have the data collected on Mr. Lagacé sealed. It sent the Montreal police force a lawyer's letter on Wednesday demanding it refrain from accessing the information until a judge rules on a motion on the case.

"We think it would be a significant problem if the data was accessed by anyone because it would tend to identify the confidential sources of Mr. Lagacé," Sébastien Pierre-Roy, lawyer for La Presse, said in an interview.

"The absence of precautions taken during the collection of data from Mr. Lagacé's cellphone to protect confidential sources is a scandal and an unprecedented attack on the freedom of the press," Mr. Pierre-Roy wrote in the letter to police.

In addition to the six reporters, media reports have found that three Quebec journalists had recently been the object of police attention. Police did not obtain court warrants but had scrutinized the call logs of its officers to find out who had been speaking to the reporters.

Straits Times

New software developed by Japanese IT giant NEC can spot crooks 100 times faster

Thursday, 03 November 2016

Byline: Walter Sim

Section: general

Tokyo - New software developed by Japanese information technology giant NEC promises to help law enforcement agencies weed out criminal suspects at more than 100 times the speed of current systems. Launched on Monday on the eve of a two-day NEC trade show in Tokyo, the NeoFace Image data mining system taps artificial intelligence to scan video footage for specific individuals.

NEC said its latest software can scan through one million faces captured in closed-circuit television footage within 10 seconds, and that this could come in handy in criminal forensic investigations and in finding missing persons.

"For example, you may have 40 videos of a crime scene to find a suspicious person, and you need to look through all these videos, which will take a lot of time and effort to prove that the same person keeps appearing in all of them," a spokesman said on Monday at a media preview of the trade show.

"But the new approach matches people with similar facial features and groups them together," she said, adding that the system works regardless of the quality of the video.

Other data that can be gleaned from this information includes a person's movements, the number of times one might have visited a specific location as well as the people one might have met.

"In recent years, there is growing demand for advanced analysis of camera footage for use in security and marketing applications," said Mr Noritaka Taguma, the general manager of NEC's transport and city infrastructure division.

The new program "meets this demand by providing high-speed, high-precision searches for persons who appear in specific patterns, which could not be achieved through manual searches or conventional technology", he said.

NEC, which runs a research laboratory and a cyber security outfit in Singapore, is a world leader in biometric technology.

Its biometric systems are being used in more than 40 territories, including in Singapore's passport and Macau's border control systems. A deal was announced in May for NEC to provide its facial recognition technology to New York's John F. Kennedy Airport.

In Japan, the technology is also being used in visitor passes to Universal Studios as well as to prevent ticket scalping at concerts.

The facial recognition technology market is worth US$200 billion (S$278 billion) and growing by about 20 per cent annually, said NEC principal research fellow Hitoshi Imaoka, who does research in facial recognition technology.

He said on Monday that some new areas that NEC is working on developing include the use of facial recognition in cashless payment and, in hospitals, the identification of patients without the need to register each time.

On the NeoFace Image system, he acknowledged that it is not always foolproof but said: "In the United States, it is common understanding that the biometric approach combines multiple methods, such as fingerprints or passwords, to have more accuracy."

Dhaka Tribune

Cyber sleuths probing FB post that sparked anti-Hindu violence

Thursday, 03 November 2016

Byline: Mohammad Jamil Khan, Mohammad Abu Bakar Siddique

Section: general

Dhaka - The Counter-Terrorism and Transnational Crime (CTTC) unit has begun probing the origin of the Facebook post that sparked the large scale communal violence against Hindus in Brahmanbaria on Sunday.
Alimuzzaman, deputy commissioner of the CTTC unit's cyber crime team, told the Dhaka Tribune that they have already started gathering information during the primary stages of the investigation.

Another cyber crime team under the Criminal Investigation Department (CID) is also helping with the probe, CID sources said.

The offending message, depicting Lord Shiva sitting atop the Kaaba, went up from the account of 30-year-old Rasraj Das on Friday. However, the illiterate youth stated in his latest post early on Saturday morning that he had no knowledge of how this photo originated from his account. Rasraj said he apologises to "Muslim brothers" and was only made aware of the post when his friends told him about it. Rasraj deleted the post early Saturday.

Later that same day Rasraj was beaten up by locals and handed over to the police. On Sunday, a mob wrecked over 100 Hindu homesteads of Nasirnagar and vandalised more than a dozen temples, injuring about 100, instigated by local radical Islamist groups.

The attacks took place following a meeting of local Muslims who had gathered on Nasirnagar playground Sunday morning to demand justice for the blasphemous Facebook post.

The attack was similar to that on the Buddhist community in Cox's Bazar in 2012, which was also sparked by a fake Facebook post.

Mizanur Rahman, superintendent of police of Brahmanbaria, told the Dhaka Tribune: "Everything will become clear after the investigation is over."

Dr AKM Ashikur Rahman of Buet's computer science and engineering department, said people are vulnerable to Facebook hacking if they log in from shared computers.

"It is easy to verify Rasraj's claim of his account being hacked by tracking the IP from which the post was made," Prof Rahman said. "Hackers could easily get hold of widely available software to gain access to

accounts or send game requests, with malware, on Facebook which allows the hacker access to a computer if the target activates the link."

Associate Professor Zahurul Hoque Mozumder of Electrical and Electronic Engineering Department of Dhaka University, said people are more susceptible to hacking if they are careless about security as Facebook already provides robust security measures.

He said law enforcers have the expertise and technology which can easily identify the IP address of a hacker.

Another computer engineer, asking not to be named, said spyware is available on the net that can be used for hacking into person's account.

A high official of the Police Headquarters said they have formed a four- member committee to probe the matter. Committee members are on the spot to investigate the incident and interrogate the detainees.

New Straits Times

Raising the alert on cybersecurity

Thursday, 03 November 2016

Byline: Ahmad Kushairi

Section: general

Kuala Lumpur - At the United States presidential debate recently, both candidates Hillary Clinton and Donald Trump were asked how they would address cybersecurity challenges and the growing international threats online.
Clinton stressed on the need for firm national resolve as she pins blame on certain countries and terrorist groups, while Trump argued that perpetrators could be anyone, including individuals launching attacks from the comfort of their homes. Whatever the argument is, cybersecurity and cyber risks have indeed become a global concern over the past few years.

As the world becomes smaller and more connected, the threat of falling victim to cyberattacks remains a clear and present danger. Governments are putting in more resources, allocations and coherent cybersecurity strategies to combat increasingly dangerous cyberattacks.

On the home front, it was reported that the armed forces' military intelligence unit has set up a cyber defence special unit to tackle cyber warfare attempts against the country.

Defence Minister Datuk Seri Hishammuddin Hussein was quoted as saying that Malaysia's sophisticated cyber defence system is expected to be among the best in the region when completed. While cyberspace continues to evolve, cybersecurity continues to become an increasing concern. Cyber crooks are everywhere. They may even be right in your living room as we speak, without us even realising it!

In this Internet age, we are vulnerable to losing more than just our privacy, but also valuable personal information.

Earlier this year, Facebook co-founder Mark Zuckerberg made headlines when he applied a piece of tape over his web cam as a protection against potential cyber spies! Whether you're an ordinary person or a multi- billionaire, no one is safe these days from cyber perpetrators, not even in the comfort of your living room.

One incident last week sparked more awareness on the cyber world. There was a staggering Distributed Denial of Service (DDoS) attack on a Domain Name Server (DNS) located somewhere in cyberspace. The attack basically tanked any site that uses the DNS. These kinds of DDoS attacks are becoming more prevalent and destructive over the years. As Internet infrastructure grows and the world becomes more connected, so do these massive cyberspace attacks.

The latest attack was identified to be caused by Mirai botnets, a type of malware that hacked Internet of Things (IoT) devices, such as close-circuit television cameras and digital video recorders to launch a massive and sustained Internet attack that caused outages and network congestion for a large number of web sites.

This attack highlights the apparent security flaws in such devices, which is quite alarming, as more of these devices get into our homes and workplaces, and may become part of our lives in the future. A simple and normal IoT device, such as your smart refrigerator or television, may succumb to cyber hacking and cause problems. While it may sound a bit farfetched to some, it is wise not to rule out the potential danger.

From a recent security assessment study by Hewlett Packard on IoT, more of such devices are connected through WiFi and social media networks, and these devices consist of daily sensitive information about our lives and personal data. HP's study concluded that 70 per cent of our smart appliances have serious security weaknesses that can expose us to cyber crooks looking for opportunities to gain access to our personal information and finances.

Cybersecurity is a bigger concern than we may realise. According to statistics provided by MyCert (Malaysia Computer Emergency Response Team, which operates under CyberSecurity Malaysia), there were over 2.7 million counts of botnet drones and malware infection attacks by unique Internet protocols (IPs) last year.

Other statistics revealed that more than 9,000 counts of cybersecurity issues were reported in Malaysia last year, such as cyber harassment, fraud, intrusion, malicious codes, denial of service, content related and spam.

The chief executive officer of CyberSecurity Malaysia, Dr Amirudin Abdul Wahab, recently said the agency has several key milestones to reach by 2020. The goal is to globalise CyberSecurity Malaysia, expand and engage initiatives through bilateral and multilateral cooperation with local and international agencies to strengthen the nation's cybersecurity strategies.

The more we engage globally with other international cybersecurity forces, the better our chances to protect the nation and people from cyberattacks.

Cybersecurity should be everyone's responsibility. While the government, through the relevant agencies are putting in place protective cybersecurity measures and strategies at the national level, it still demands a united effort from the people to counter the cyber menace.

The Internet age may have brought many conveniences, but it is still a vast, unregulated space where many bad elements are lurking in dark corners to inflict damage and misery.

It doesn't, however, mean that we should live in constant fear. But, just like in the real world, we need to be extra alert and take precautions, while reaping the wonderful benefits that the Internet age brings.

Montreal Gazette

New probe ordered in surveillance scandal

Thursday, 03 November 2016

Byline: Philip Authier and Jason Magder

Section: general

Montreal - The police spying crisis has gone from bad to worse, with Public Security Minister Martin Coiteux ordering an administrative investigation into the practises of the Sûreté du Québec dating back to 2013.
Coiteux made the announcement within hours of the provincial police force revealing it had tracked the calls and movements of six journalists that year after news reports based on leaks revealed Michel Arsenault, then president of Quebec's largest labour federation, had his phone tapped.

The controversy began Monday after Montreal media outlet La Presse reported that police had tracked columnist Patrick Lagacé's cellphone to find out if he was being leaked information from police officers.

The new investigation - to be captained by officials in the Public Security department - is over and above internal investigations Coiteux has already ordered into the work of the province's police forces in the wake of the Lagacé scandal.

Coiteux said that to his knowledge, it is the first time in 20 years such a case has emerged involving the provincial police.

This specific one, however, took on a political dimension because the man at the centre of it and now in the hot seat is Stéphane Bergeron, who was the Public Security minister at the time, in 2013 in the Parti Québécois government of Pauline Marois.

The surveillance of the six reporters was part of an internal probe ordered by then-SQ director Mario Laprise to find out which officers had leaked information to journalists about the investigation into Arsenault, who was being probed as part of an investigation into organized crime infiltrating the construction industry.

Arsenault wrote to complain about the leaks to Bergeron, and Laprise ordered the investigation soon afterward.

"What happened then was pretty unusual," Coiteux said. "A letter arrived in his (Bergeron's) office in the morning and by the evening an investigation was launched. And now we learned that under that investigation, journalists were targeted. "It's curious, to say the least. I was surprised and I was shocked and this is why we acted promptly and swiftly."

Meeting reporters earlier, Bergeron, today the PQ's critic for Public Security, appeared as perplexed as everyone about the chain of events leading to the tracking of journalists under his watch.

He confirmed he acted on Arsenault's request by asking his deputy minister to ask Laprise to check on what was happening internally to lead to such leaks. But he said he had no idea what actions Laprise took as a result.

"The nuance is important," Bergeron said at a hastily called news conference after news broke of the SQ tracking. "Never did it come into my mind that they would start poking into journalists' work. I learned today that the police started checking journalists' phones.

"I never asked for this. I never authorized this and would never have authorized this, and I was never informed of this."

SQ Cpt. Guy Lapointe confirmed the SQ investigation of journalists Wednesday, and told the Journal de Montréal police looked into allegations of illegally obtained information by the journalists. He confirmed that surveillance was done on six reporters, but would not name them.

Meanwhile, La Presse fired back on Wednesday, issuing a lawyer's letter to Montreal police demanding that all information collected from Lagacé's cellphone be locked away and kept from investigators.

In that case, police requested 24 search warrants to track Lagacé's iPhone since January, which allowed police to access the numbers Lagacé had called or received calls from, and track him by activating a GPS mechanism on his phone. At least three other journalists have since learned they were under similar surveillance by police - Félix Séguin of TVA, Monic Néron from 98.5 FM, and freelance journalist Fabrice de Pierrebourg.

"If it becomes a common occurrence for police officers to have access to all sources of all journalists who have important news reports, our fear is that no one will ever want to talk to journalists, and that would have a dramatic effect on the freedom of the press," said Sébastien Pierre-Roy, the lawyer representing La Presse.

Montreal's mayor said he still has confidence in Philippe Pichet, the city's police chief, but said that confidence is not absolute.

"He has my confidence until there is proof (of wrongdoing)," Denis Coderre told reporters Wednesday.

Montreal's police brotherhood has called on Pichet to resign, saying he showed a serious error in judgment and that the top police brass was trying to create a climate of fear around leaks.

TVA reported on Tuesday that top police brass had been ordered to crack down on police leaking information to journalists.

In a meeting held April 26 in Anjou, assistant director Mario Guérin addressed 50 high-ranking officers to tell them this kind of behaviour would no longer be tolerated. A part of the meeting was recorded by one of the officers in attendance, and Guérin could be heard saying the force needed to "break the culture" of leaking information to journalists. Coderre said the city's public security commission will examine the issue thoroughly, but despite a poll saying most Montrealers would like to see a public inquiry, the city's examination will be done behind closed doors.

"It will be done behind closed doors because I want them to ask all the questions," Coderre said.

He said the councillors will have to closely examine all the facts related to the issue before drawing any conclusions.

"The report will be deposited to the executive committee and to city council, so it will be made public," Coderre said. "But because of the sensitivity of the information, (making the inquiry public) could have an impact on investigations that are already underway."

In Quebec City, the news the police spying was far more widespread than originally believed gave the opposition fresh ammunition in its quest for a much broader, independent inquiry into events.

The Coalition Avenir Québec, which has already asked for a full public inquiry and the resignation of Montreal police chief Philippe Pichet in the case involving La Presse reporter Patrick Lagacé, cranked up the pressure.

"A full public inquiry would allow us to shed all the light on this, so the journalists can testify, the police ... to produce an extremely complete report revealing the truth, how it happened and who authorized this kind of electronic surveillance," said CAQ justice critic Simon-Jolin Barrette.

PQ leader Jean-François Lisée - who said he still has confidence in Bergeron - said the rapidly unravelling situation proves the need for an independent inquiry by the province's police incident's investigation agency, the Bureau des enquêtes indépendantes.

Journal de Montréal

Les policiers se croient-ils tout permis ?

Thursday, 03 November 2016

Byline: Richard Martineau

Section: column

Chronique - Ainsi, le SPVM n'est pas seul en cause.
La SQ aussi a espionné des journalistes et obtenu secrètement copie de leurs registres téléphoniques.
Ben coudonc. Il y a vraiment quelque chose de pourri au Royaume du Québec.

Tout ça pour protéger leur image...

UNE CULTURE DU VIOL

Dans le jargon policier, on appelle ça «colmater les fuites».

Traduction: «Faites ce que vous avez à faire, prenez tous les moyens à votre disposition, mais trouvez-moi le tabarnac qui parle aux journalistes pour qu'on lui ferme la gueule au plus sacrant.»

Que les patrons d'une entreprise essaient de savoir lequel de leurs employés coule des informations confidentielles aux journalistes est une chose. Mais on parle de la police, ici. Les représentants de la loi et l'ordre. «Les gardiens de la démocratie, les derniers remparts contre la barbarie et l'anarchie.»

Wow. J'avoue que les bras m'en tombent. Après le SPVM, la SQ. On est en droit de parler de «culture».

La culture du viol... de la vie privée. La culture du viol... de la liberté de presse.

On est la police, donc on a tous les droits.

Ça fait combien de temps que ça dure? Depuis combien de temps les forces policières utilisent-elles ce genre de méthodes hautement discutables pour protéger leur image?

Combien de journalistes ont fait l'objet de telles «attentions»?

Quelque chose me dit qu'on vient juste de gratter la surface de ce scandale. On va aller de surprise en surprise.

PISSER DANS L'OREILLE

Une idée pour l'équipe du Maclean's: après Le Québec, la province la plus corrompue au pays, Les forces policières les plus immorales au pays.

Cette fois-ci, on ne vous critiquera même pas. On va être d'accord avec vous. Je comprends que les policiers ont un devoir de réserve, qu'ils ne sont pas censés refiler des informations «sensibles» aux journalistes. Mais justement... Si des policiers -- qui, comme nous le savons tous, ont tendance à se serrer les coudes -- en viennent à «pisser» dans l'oreille de certains journalistes, c'est peut-être parce que quelque chose ne tourne pas rond chez eux, non?

Au lieu de partir à la chasse aux méchants «délateurs» présents dans leurs rangs, les directeurs de police devraient plutôt se demander pourquoi diantre certains de leurs agents ont préféré se pincer le nez et parler à des journalistes plutôt que de respecter la loi de l'omertà qui règne habituellement dans les forces, qu'elles soient militaires ou policières...

Le problème n'est pas qu'un policier ait parlé à un journaliste, c'est la situation qui a amené ce policier à parler à un journaliste.

DES MESURES ESTHÉTIQUES

Ce qui est arrivé est grave. Très grave.

Et ça va prendre plus qu'une poignée de «mesures» rédigées en catimini sur le coin d'une table pour venir à bout de cette culture de l'impunité qui semble régner dans nos forces policières.

Au moins, si les hauts gradés de la police avaient agi ainsi pour protéger la sécurité des gens, on pourrait en débattre, peser le pour ou le contre. Même pas. C'était juste pour protéger leur image. C'est honteux. Honteux et scandaleux.

Journal de Montréal

Une menace claire pour les sonneurs d'alarme, dit Snowden

Thursday, 03 November 2016

Byline: Boris Proulx

Section: general

Montréal - La surveillance policière dont ont fait l'objet au moins 10 journalistes québécois dans les dernières années représentent les agissements d'une société «antidémocratique» et «autoritaire», a déclaré le lanceur d'alerte et fugitif américain Edward Snowden, hier.
«On voit que même la police locale peut décider qu'elle n'apprécie pas les reportages d'un journaliste, et un juge peut lui donner tous les moyens d'obtenir l'information sur qui il appelle, où il se trouve», a dit M. Snowden, en vidéoconférence devant un auditorium complet de l'Université McGill, hier soir.

RÉVÉLATIONS

Il y a environ trois ans, l'informaticien américain s'est fait connaître en révélant au grand jour les pratiques de surveillance de masse de la National Security Agency (NSA).

Le film américain Snowden, paru cette année, revient d'ailleurs sur l'histoire de ses révélations. Cela pose une menace claire pour les personnes qui, comme lui, veulent dénoncer les abus commis par les gouvernements, a-t-il avancé.

«Notre habilité à résister à l'abus gouvernemental n'a jamais été aussi réduite qu'à notre époque», a-t-il dit.

Le critique de la surveillance de masse, qui habite aujourd'hui Moscou, a souligné que de nombreuses questions demeurent entières sur la manière dont les corps policiers ont justifié leurs actions.

DES PREUVES

«Nous avons des preuves que [la surveillance] a été faite, mais on ne sait toujours pas selon quelle autorité. Nous ne pouvons que faire des hypothèses. Est-ce justifié par la loi C-13 [pour lutter la cyberintimidation]? C-51 [contre le terrorisme]? Nous ne savons pas ce que la police a demandé [au juge], derrière le rideau», a-t-il soulevé.

Selon lui, les journalistes sont essentiels pour restaurer la confiance du public envers le gouvernement.

«Au lieu de faire moi-même les révélations, j'ai décidé de fournir toute l'information aux journalistes, a-t-il rappelé. Je voulais que ces journalistes parlent avec leur gouvernement, pour que les dirigeants aient des comptes à rendre en matière de surveillance.»

Journal de Montréal

La SQ a eu un cellulaire de Ken Pereira

Thursday, 03 November 2016

Byline: Améli Pineda

Section: general

Montréal - Le syndicaliste et sonneur d'alarme Ken Pereira dit avoir été naïf lorsqu'il a remis à la Sûreté du Québec le cellulaire qu'il utilisait pour contacter une trentaine de journalistes, en 2008.
«J'ai été naïf», lance-t-il en entrevue avec Le Journal.

Avec les récentes révélations concernant la surveillance des sources de journalistes, M. Pereira s'inquiète de l'utilisation qu'a pu faire la SQ des données de son cellulaire de l'époque.

«Peut-être que je panique pour rien, mais tous les journalistes qui ont été nommés jusqu'à présent, j'étais en contact avec eux à cette époque», soutient-il.

MENACE

M. Pereira raconte qu'en 2008, il était surveillé par la SQ puisque sa vie était en danger.

Un jour, il a reçu un texto menaçant.

«C'était écrit "Dans trois jours BOOM"», dit- il.

Il a déposé le téléphone sur une table et a tout de suite téléphoné à la police.

«Ils sont venus et l'ont saisi. Sincèrement, je ne m'étais jamais posé de question jusqu'à cette semaine», confie-t-il.

La Presse+

Le SPVM rencontre tous ses enquêteurs

Thursday, 03 November 2016

Byline: Louis-Samuel Perron; Daniel Renaud

Section: general

Montréal - La direction du Service de police de la Ville de Montréal (SPVM) rencontre depuis mardi tous les enquêteurs du corps policier afin de leur demander s'ils ont déjà enquêté ou enquêtent toujours sur « un journaliste, un avocat ou un politicien », soutient la Fraternité des policiers et policières de Montréal dans un message envoyé mercredi à ses membres obtenu par La Presse. Le syndicat dénonce une « stratégie improvisée » des dirigeants du SPVM ayant pour but de « prétendre » qu'ils ont été diligents. « Il s'agit évidemment d'une diversion puisque la crise origine en réalité de la haute direction, responsable de la demande d'un mandat pour espionner un journaliste et identifier ses sources dans le cadre d'une inconcevable chasse aux sorcières », écrit le vice-président de la Fraternité Mario Lanoie, qui invite les policiers à contacter le syndicat en cas « du moindre glissement vous rendant mal à l'aise » au cours de la rencontre. Joint par La Presse, la Fraternité n'avait aucun commentaire à émettre à ce sujet hier. Lundi, le président syndical Yves Francoeur avait qualifié, en entrevue avec La Presse, de « totalement inacceptable » l'espionnage de journalistes. Il avait également déploré l'« approche symptomatique d'une organisation malade et mal gérée ». Le SPVM n'a émis aucun commentaire hier soir.

Journal de Montréal

La SQ a aussi épié des reporters

Thursday, 03 November 2016

Byline: Stéphane Alarie

Section: general

Montréal - Les registres téléphoniques de six journalistes, dont un du Journal, ont été fouillés pendant plusieurs mois

L'affaire des journalistes espionnés par des policiers ne cesse de prendre de l'ampleur. Après la police de Montréal, c'était au tour de la Sûreté du Québec d'avouer hier qu'elle a déjà scruté les communications de six reporters, dont celles de notre journaliste aux affaires criminelles, Éric Thibault.

L'ex-DG de la Sûreté du Québec, Mario Laprise, a ordonné l'enquête qui a mené à l'espionnage des journalistes en 2013.

Depuis lundi, les révélations se multiplient et on compte désormais au moins 10 journalistes québécois qui ont fait l'objet d'une forme de surveillance policière ces dernières années.

Le porte-parole de la SQ, le capitaine Guy Lapointe, a ainsi confirmé qu'une «enquête sur des allégations criminelles de divulgations illégales de contenus obtenus dans le cadre d'une écoute électronique» avait été amorcée à l'automne 2013 et qu'elle visait, entre autres, six journalistes.

Ceux-ci sont connus et respectés, tant par le public que le milieu de l'information. Outre Éric Thibault, du Journal de Montréal, Marie- Maude Denis, Isabelle Richer et Alain Gravel, tous trois de Radio-Canada, figurent parmi les reporters espionnés. Le chef de bureau de La Presse à Québec, Denis Lessard, et le chroniqueur judiciaire retraité André Cédilot complètent le tableau.

L'enquête qui a mené à l'espionnage de ces journalistes a été ordonnée à l'époque par l'ancien directeur général de la SQ, Mario Laprise, comme le révélait Le Journal en primeur hier après- midi.

PLUSIEURS MOIS

En vertu d'autorisations judiciaires émises par un juge, des enquêteurs des Affaires internes ont fouillé les registres téléphoniques des journalistes pendant plusieurs mois afin d'identifier d'où provenaient certaines informations publiées concernant l'ex-président de la Fédération des travailleurs et travailleuses du Québec (FTQ), Michel Arsenault.

Peu avant, des reportages avaient dévoilé que M. Arsenault était l'objet d'une surveillance électronique par la SQ. On y apprenait que le patron de la centrale syndicale était sous écoute dans le cadre du projet Diligence -- visant à contrer l'infiltration du crime organisé dans la construction -- et qu'on l'avait du coup écarté d'un siège au sein du conseil de la Caisse de dépôt.

Mécontent que la chose soit révélée, l'ex- président de la FTQ avait écrit au ministre péquiste de la Sécurité publique de l'époque, Stéphane Bergeron, pour s'en plaindre.

Quelques heures plus tard, le directeur Laprise déclenchait l'investigation qui mènerait à la surveillance des six journalistes. Celle-ci n'a jamais abouti ni mené au dépôt d'accusations. L'affaire a été classée à l'été 2014.

Déjà à l'époque, nos sources révélaient que la décision d'enquêter ne faisait pas l'unanimité au sein de la SQ. D'ailleurs, les détails des opérations n'auraient été connus que de la garde rapprochée du directeur Laprise. Même le directeur des poursuites criminelles et pénales n'a pas été avisé ni consulté sur la marche à suivre.

M. Laprise, qui occupe maintenant le poste de vérificateur interne à Hydro-Québec, a refusé de commenter. «On va laisser aux gens le temps de faire leur travail», a-t-il glissé, en référence à l'enquête administrative qui a été annoncée hier, lorsque joint par Félix Séguin, de notre Bureau d'enquête.

Le Soleil

Discrétion demandée, mais pas d'enquête

Thursday, 03 November 2016

Byline: Journaliste maison

Section: general

Québec - Le chef de police de Québec admet qu'il doit parfois rappeler aux membres de son service leur serment de discrétion, mais assure qu'aucun journaliste n'a fait l'objet d'une enquête durant son passage à la tête du service.
Le directeur du Service de police de la Ville de Québec, Michel Desgagné, a fait cette déclaration, mercredi, en marge de la conférence de presse tenue à l'occasion de son départ à la retraite. Il confirme ainsi ce que le maire Régis Labeaume avait déclaré mardi. Il répondait à une question posée à savoir si des journalistes de la région de la capitale avaient déjà été «suivis» par la police de Québec, notamment concernant des enquêtes auprès de policiers qui auraient pu divulguer des informations aux membres des médias.

« La réponse vient de moi, précise M. Desgagné. Dans les cinq dernières années, je n'ai jamais fait d'enquête de ce type-là. Et je n'ai jamais eu connaissance de dossiers comme ça. Par contre, on a des

préoccupations sur les serments de discrétion de certains de nos collègues et on doit faire des rappels périodiques, poursuit- il. Nous [les policiers] devons avoir une certaine retenue pour la sécurité des policiers, celle de la population et pour ne pas entraver le cours de la justice.

PEU DE «COULAGE»

«C'est criminel, que ce soit pour un citoyen, un policier ou un journaliste. C'est surtout au niveau des enquêtes criminelles qu'on doit avoir une certaine retenue. Et si on pense à la sécurité des citoyens [...] et s'il y avait eu ça [entrave] dans notre organisation, on aurait fait l'enquête.»

Selon lui, il n'y a pas beaucoup «de coulage d'information» auprès des journalistes. Cependant, il dit parfois s'interroger. «Quand on arrive dans une opération planifiée depuis longtemps et que vous arrivez [sur les lieux] quasiment avant nous autres, on se questionne un petit peu.»

Sur une note plus personnelle, M. Desgagné se donne en exemple. «Je dînais et je soupais avec un journaliste. C'était mon père. Moi, j'étais policier. On était capables de se respecter et de faire la différence entre les deux. Il avait de l'information que je ne savais pas et j'avais de l'info qu'il ne savait pas. Je suis capable de distinguer les deux. »

Journal de Québec

« On a d'autres chats à fouetter », dit le chef Desgagné

Thursday, 03 November 2016

Byline: Nicolas Saillant

Section: general

Québec - Le chef de police de Québec, Michel Desgagné, affirme que son service n'a jamais lancé une enquête visant la surveillance de journalistes.
«Dans les cinq dernières années, il n'y a jamais eu d'enquête de ce type», assure M. Desgagné qui a lui-même informé le bureau du maire Labeaume sur le sujet mardi.

Plus encore, il affirme ne jamais avoir mené d'enquête interne sur des policiers de son service soupçonnés de donner de l'information aux journalistes.

«On a d'autres chats à fouetter», a-t-il lancé.

SERMENT DE DISCRÉTION

Reste que M. Desgagné a des inquiétudes face à la possibilité que de l'information sensible soit divulguée aux journalistes par ses policiers. «On a des préoccupations sur le serment de discrétion de nos collègues et on doit faire des rappels de façon périodique.»

M. Desgagné n'a pas voulu commenter directement ce qui se passe au SPVM, mais a quand même semblé prendre ses distances de la situation montréalaise.

«Si je fais une enquête interne, je vais enquêter sur les policiers, pas sur les journalistes, ce n'est pas moi votre Conseil de presse», lance celui qui prendra sa retraite en décembre (voir autre texte en page 17).

PAS PRÉOCCUPÉ

Il soutient aussi ne pas avoir de préoccupations particulières par rapport aux policiers qui parlent aux journalistes.

«Si j'avais à regarder quels numéros ils [les policiers] ont dans leur cellulaire, je serais moi-même mal pris parce qu'il y en a certains parmi vous autres qui m'appelez et j'ai déjà appelé certains d'entre vous», a-t-il dit aux journalistes.

Il ajoute tout de même que le service de police a comme priorité de protéger les enquêtes criminelles et que des accusations d'entrave à la justice peuvent être déposées tant contre un journaliste que contre les policiers.

«Au niveau des opérations criminelles [...], on doit avoir une certaine retenue», a-t-il conclu.

Le Devoir

Protection des sources - Assez les abus!

Thursday, 03 November 2016

Byline: Brian Myles

Section: editorial

Editorial - La liberté de presse est menacée au Québec. Il est grand temps d'adopter une loi sur la protection des sources pour mettre fin aux abus de la police.Il ne s'agit plus d'un cas isolé ou d'un abus

de pouvoir anecdotique par une grosse police en mal de contrôle. L'espionnage des journalistes d'enquête est un mal si répandu au Québec qu'il faut maintenant des actions fermes pour casser cette désagréable impression de vivre dans un État policier.
Ces tares ne sont pas uniques au SPVM puisque la Sûreté du Québec (SQ) fouine aussi dans les téléphones intelligents des journalistes. Radio-Canada a révélé mercredi que la police provinciale avait obtenu les registres d'appels des téléphones intelligents de trois de ses reporters, Isabelle Richer, Marie-Maude Denis et Alain Gravel. Au total, les communications d'une bonne dizaine de journalistes ont été épiées par le Service de police de la Ville de Montréal (SPVM) ou la SQ depuis 2013.

La dérive des policiers n'a d'égale que celle des juges de paix qui ont autorisé ces chasses aux sources. Deux institutions fondamentales en démocratie, la police et la justice, ont traité la liberté de presse, le journalisme d'enquête et la protection des sources avec une grossière indélicatesse.

Le resserrement des règles dans l'octroi des mandats de surveillance des journalistes, annoncé mardi par le premier ministre Philippe Couillard, est un pas dans la bonne direction. À l'avenir, les mandats de surveillance visant des journalistes devront faire l'objet d'une autorisation du Directeur des poursuites criminelles et pénales (DPCP) avant d'être soumis à un juge de paix. Les journalistes bénéficieront du même traitement que les avocats, une avancée considérable. Le combat le plus important reste à mener, afin que Québec et Ottawa adoptent des lois pour protéger les sources des journalistes. Le statut des journalistes, qui ne sont pas de véritables professionnels, contrairement aux avocats, ne devrait pas servir d'excuse à l'inaction à ce sujet.

M. Couillard doit aussi amender le projet de loi visant à protéger les lanceurs d'alerte. Dans sa mouture actuelle, le projet force les lanceurs d'alerte à contacter la police avant les médias s'ils veulent bénéficier de la protection de l'État. Ce projet fait abstraction de la réalité. Si les lanceurs d'alerte se tournent vers les médias, et non la police, pour dénoncer des irrégularités, c'est souvent parce que les organismes de surveillance, y compris la police, ont failli à leur mission.

L'effondrement du deuxième volet de " Diligence ", une enquête ratée sur les tentatives d'infiltration du crime organisé à la FTQ, est l'illustration parfaite de ce principe. Le coulage de conversations d'écoute électronique (une infraction au Code criminel) a d'ailleurs mené la SQ à enquêter sur six journalistes, dont ceux de Radio- Canada, à la suite d'une plainte de l'ancien président de la FTQ, Michel Arsenault. Les policiers et les officiers de justice ne partagent pas l'enthousiasme des journalistes sur la diffusion du matériel d'écoute électronique en dehors d'un procès ou d'une commission d'enquête. Ce contentieux ne sera pas réglé de sitôt.

C'est Stéphane Bergeron qui avait demandé à la SQ d'enquêter sur les fuites dans " Diligence ", à l'époque où il était ministre de la Sécurité publique. Il est aujourd'hui étonné que sa demande ait pu servir de prétexte pour que la SQ enquête sur des journalistes. L'actuel directeur général de la SQ, Martin Prud'homme, a annoncé un resserrement des règles internes jeudi après avoir pris connaissance de l'étendue de la chasse aux sources autorisée par son prédécesseur, Mario Laprise. À l'avenir, il faudra

obtenir l'autorisation de l'état-major avant d'enquêter ou de surveiller des journalistes. Voilà deux témoignages démontrant que la SQ a dépassé les bornes en 2013.

Une enquête, indépendante du pouvoir policier, est nécessaire.

Le Soleil

La SQ a aussi espionné des journalistes

Thursday, 03 November 2016

Byline: Simon Boivin

Section: general

Québec - Le scandale s'étend. La Sûreté du Québec (SQ) reconnaît avoir aussi espionné six journalistes et réclame une enquête sur elle-même. Le ministre de Sécurité publique de l'époque, le péquiste Stéphane Bergeron, jure n'en avoir rien su.
Il ne s'agit plus uniquement d'un corps de police municipale. En 2013, la SQ a obtenu des autorisations judiciaires pour connaître l'identité de tous ceux qui ont discuté avec une demi-douzaine de journalistes.

Parmi eux, les piliers de l'émission Enquête qui ont mis au jour les scandales dans l'industrie de la construction, Marie-Maude Denis et Alain Gravel, de même que la journaliste spécialisée en affaires juridiques à Radio-Canada, Isabelle Richer.

Les registres des appels entrants et sortants des journalistes Éric Thibault, du Journal de Montréal, et de Denis Lessard, de La Presse, ont aussi été accessibles aux policiers. Sans verser dans l'écoute électronique, ils pouvaient néanmoins identifier leurs interlocuteurs. Les journalistes étaient surveillés pour des «allégations criminelles de divulgations illégales de contenus obtenus dans le cadre d'une écoute électronique».

L'actuel directeur général de la SQ, Martin Prud'homme, a lui-même demandé à ce qu'un tiers indépendant se penche sur l'investigation déclenchée par son prédécesseur, Mario Laprise. Le ministère de la Sécurité publique mènera une enquête administrative, a assuré le ministre Martin Coiteux, mercredi, en début de soirée.

Il juge «curieux» que l'enquête de la SQ ait été déclenchée le jour même où l'ex-président de la FTQ, Michel Arsenault, s'est plaint auprès du ministre péquiste Stéphane Bergeron de fuites médiatiques liées à l'écoute électronique dont il a été l'objet.

«Une lettre est arrivée à son cabinet le matin et, le soir, une enquête était déclenchée, a souligné M.Coiteux. Et on comprend que le ministre d'alors a eu une communication avec le directeur de la SQ. C'est un cas particulier.»

Aujourd'hui porte-parole du PQ en matière de Sécurité publique, M. Bergeron se souvient d'avoir passé un coup de fil au patron de la SQ pour s'enquérir de la situation. La décision d'enquêter était déjà prise, jure-t-il. Et il ne pouvait pas se douter que les policiers allaient aller jusqu'à espionner des journalistes pour colmater les brèches dans leur propre organisation.

«Ça ne lui a pas traversé l'esprit qu'on fouille dans le travail des journalistes parce que c'est injustifié et injustifiable», a dit le chef péquiste Jean-François Lisée. Même si le dg de la SQ avait été nommé par le PQ, M. Lisée juge qu'il a pris une «mauvaise décision» en surveillant des journalistes.

Le ministre Coiteux soutient que cet épisode d'espionnage de journalistes est le seul qui se soit produit à la SQ au cours des 20 dernières années. Il juge que son ministère, auquel le corps policier est rattaché, a les coudées franches pour mener une enquête «totalement indépendante».

M. Coiteux martèle qu'il doit y avoir «une bonne distance» entre le gouvernement et les forces policières. Il ne contredit toutefois pas les propos de M. Bergeron qui soutient qu'un ex-ministre libéral, Raymond Bachand, a informé en 2009 le président de la FTQ qu'il était sous écoute. «Est-ce qu'une enquête a été déclenchée en 2009 visant des journalistes? demande M. Coiteux. Le seul cas qui aurait eu lieu a été déclenché en 2013.»

Outre la nouvelle enquête administrative, le gouvernement Couillard estime que les trois mesures annoncées mardi pour éclaircir la situation suffiront : difficulté haussée pour la délivrance d'un mandat de surveillance d'un journaliste; mise sur pied d'un comité d'experts pour formuler des recommandations sur les meilleures pratiques à adopter; inspection par le ministère de la Sécurité publique des pratiques des principaux corps policiers.

MISE EN DEMEURE

Depuis les révélations sur les mandats de surveillance lancés à l'endroit de Patrick Lagacé, des informations circulent voulant que d'autres journalistes ont aussi été sur le radar des forces policières. Mercredi, La Presse a fait savoir qu'elle mettait en demeure le Service de police de la Ville de Montréal (SPVM) pour l'empêcher d'utiliser, de copier ou de transmettre les informations obtenues grâce aux mandats de surveillance obtenus.

Le chef de l'opposition, Jean- François Lisée, maintient que Québec fait fausse route en n'utilisant pas le Bureau des enquêtes indépendantes pour faire la lumière sur la situation. Selon lui, le premier ministre choisit la «voie contrôlée et opaque» d'une vérification par le ministère de la Sécurité publique.

De son côté, la Coalition avenir Québec juge qu'une enquête publique serait la meilleure façon d'avoir l'heure juste sur ce qui s'est passé.

Mercredi, le député solidaire Amir Khadir s'est interrogé sur l'ampleur de l'espionnage exercé par la police. «Est-ce qu'il y a des politiciens qui sont sous écoute aussi? a-t-il demandé. «Ce genre de pratique appartient à des pays que je n'ose même pas nommer», a dit M. Khadir.

sboivin@lesoleil.com

Illustration(s) :

Photo 123RF

En 2013, la SQ a obtenu des autorisations pour connaître l'identité de tous ceux qui ont discuté avec une demi-douzaine de journalistes.

Journal de Montréal

Un ex-ministre de la Sécurité publique dit qu'il ne savait rien

Thursday, 03 November 2016

Byline: Marc-André gagnon

Section: general

Québec - Les révélations sur la SQ ont créé une onde de choc à Québec
Le député Stéphane Bergeron, maintenant porte-parole péquiste en matière de sécurité publique, a assuré hier qu'il ignorait que des journalistes étaient épiés par la police à l'époque où il était lui-même ministre de la Sécurité publique, en 2013.

Le député péquiste Stéphane Bergeron était accompagné de son chef Jean-François Lisée lorsqu'il a affirmé qu'il ignorait que les communications de six journalistes avaient été épiées par la SQ en 2013.

«C'est une initiative que je n'aurais jamais autorisée, et c'est une initiative dont je n'ai jamais été informé avant», a dit M.Bergeron lors d'un point de presse, accompagné du chef péquiste Jean- François Lisée, qui en a d'ailleurs profité pour réitérer sa pleine confiance envers son député.

L'ex-directeur général de la SQ Mario Laprise a ordonné l'enquête qui a mené à l'espionnage des communications de six journalistes (voir texte en page 3), alors que Stéphane Bergeron était ministre de

la Sécurité publique, a révélé Le Journal hier. Cela a eu l'effet d'une onde de choc à l'Assemblée nationale.

Pour le Parti québécois, la Coalition avenir Québec et Québec solidaire, ces nouvelles révélations confirment plus que jamais que les mesures annoncées mardi par le gouvernement Couillard sont insuffisantes.

«PATENTE À GOSSE»

La mise sur pied d'un comité d'experts, le rehaussement des règles d'émission de mandats d'écoute électronique visant des journalistes et l'inspection des procédures auprès des principaux corps policiers ne sont que l'équivalent d'une «patente à gosse» pour le député caquiste Simon Jolin Barrette.

Selon lui, les plus récentes informations démontrent la nécessité d'une enquête publique.

«La Sûreté du Québec parle au pouvoir», a déploré à son tour le député de Québec solidaire, Amir Khadir, qui en plus de demander lui aussi une commission d'enquête, souhaite que les nominations à la tête de la Sûreté du Québec soient désormais confiées à l'Assemblée nationale plutôt qu'au gouvernement.

«On parle d'une police qui malheureusement est politique depuis très longtemps», a dit le député de Mercier.

L'opposition péquiste, de son côté, maintient que le Bureau des enquêtes indépendantes (BEI) devrait être mandaté afin de faire toute la lumière, une option qu'a écartée officiellement le ministre de la Sécurité publique, Martin Coiteux, hier.

La Coalition avenir Québec a réclamé à nouveau la démission du chef de police du Service de police de la Ville de Montréal (SPVM), Philippe Pichet. Le Parti québécois propose toujours qu'il soit plutôt suspendu, mais de façon temporaire.

Au nom de l'autonomie qu'il souhaite conférer aux municipalités, le gouvernement Couillard a préféré s'en remettre aux élus de la Ville de Montréal en ce qui concerne la direction du SPVM.

La Presse+

L'alarme sonne !

Thursday, 03 November 2016

Byline: Alain Saulnier

Section: oped

Opinion - L'espionnage par le SPVM du téléphone de Patrick Lagacé a alerté bien des gens sur le danger qui guette nos démocraties.
Plusieurs grands journaux au pays et ailleurs dans le monde ont dénoncé cette situation, car elle soulève une véritable inquiétude pour la liberté d'expression et la protection de la vie privée.

Pour les journalistes, cette affaire témoigne du mépris affiché dans le milieu policier pour leur travail. Nous avons toutes les raisons d'être indignés, car ce précédent illustre avec éloquence la facilité avec laquelle il est possible à l'ère numérique d'épier à distance la vie privée de tous les journalistes et de tous les citoyens.

Le premier ministre Couillard a fait un premier pas dans la bonne direction. Il nous faut maintenant saisir cette occasion pour reprendre la discussion sur la protection des sources et des lanceurs d'alerte. Ne perdons plus de temps.

Il y a une dizaine d'années, Serge Ménard avait initié un projet de loi très bien étoffé sur la protection des sources journalistiques. La FPJQ aurait souhaité que ce dossier débloque à l'époque. Malheureusement, il n'a pas pu achever son travail. Depuis toujours, comme avocat, député et ministre de la Justice, Serge Ménard a défendu le rôle des journalistes dans notre société.

Nous pourrions l'associer à ce travail de réflexion annoncé par le premier ministre. Du même coup, il faut espérer que l'on puisse reprendre les recommandations de la commission Charbonneau afin de mieux défendre les lanceurs d'alerte, sans qui nous ne pourrions avoir une information solide sur nos institutions.

Illustration(s) :

PHOTO ARCHIVES LA PRESSE

« L'espionnage de Patrick Lagacé a alerté bien des gens », écrit Alain Saulnier.

Note(s) :

Ancien directeur général de l'information de Radio-Canada

Radio New Zealand News

The telecommunications company Spark wants the GCSB and SIS to have to have a warrant before they come asking for customers' personal information.

Thursday, 03 November 2016

Section: general

Wellington - The telecommunications company Spark wants the GCSB and SIS to have to have a warrant before they come asking for customers' personal information.
New legislation for the two agencies requires them to abide by Privacy Act principles when seeking or accessing information from government departments and private companies.

But it does not require a warrant.

Spark and the Privacy Commissioner say there should be stronger safeguards.

John Wesley-Smith, from Spark, told MPs the bill leaves it up to the company to make calls on national security.

Journal de Montréal

L'inspecteur pourrait enquêter, dit Coderre

Thursday, 03 November 2016

Byline: Amélie Pineda

Section: general

Montréal - Le maire Denis Coderre entend confier une enquête à l'inspecteur général de la Ville de Montréal s'il apprend que d'autres journalistes ont été visés par des mandats judiciaires obtenus par le SPVM.
«Si c'est le cas, le maire va donner un mandat ad hoc à Me Denis Gallant, pour procéder à une enquête administrative», a confirmé Marc-André Gosselin, attaché de presse du maire.

Il estime que Me Gallant a «une expertise en la matière». Le maire attend les conclusions des vérifications menées par le directeur de police, Philippe Pichet.

Lundi, le maire avait annoncé que la Commission de sécurité publique de la Ville se pencherait sur les procédures des policiers pour obtenir des mandats visant les journalistes. Un rapport est attendu pour janvier 2017.

Journal de Montréal

La Presse met le SPVM en demeure

Thursday, 03 November 2016

Byline: Benoit Philie

Section: general

Montréal - Le quotidien La Presse exige la mise sous scellé de toute information pouvant permettre l'identification des sources journalistiques confidentielles du chroniqueur Patrick Lagacé, dans une requête déposée à la Cour supérieure hier.
Il demande aussi au SPVM, dans une mise en demeure, de ne pas utiliser, copier ou transmettre les données colligées lors la période où le journaliste a fait l'objet d'une surveillance.

Lundi, on apprenait que les communications ainsi que les déplacements de M. Lagacé avaient été surveillés par le SPVM, entre janvier et juillet 2016, dans le cadre d'une enquête interne. Au total, 24 mandats concernant le téléphone du journaliste ont été obtenus. La Presse craint que les données ainsi colligées ne puissent servir à d'autres fins que ce qui a été préalablement autorisé par la Cour et demande donc une ordonnance pour en protéger le contenu.

«De son côté, le SPVM assure conserver les données provenant du téléphone de M. Lagacé sur «une clef USB à double encryption [...] mise dans une enveloppe scellée», peut-on lire dans une lettre signée par l'avocat du service de police, Alain Cardinal.

Radio-Canada - Nouvelles web

Journalistes surveillés par la SQ : des zones d'ombre demeurent

Thursday, 03 November 2016

Byline: Mélanie Meloche-Holubowski

Section: general

Montréal - En décidant de surveiller en 2013 le registre des appels de six journalistes, dont trois de Radio-Canada, la Sûreté du Québec (SQ) a voulu faire la lumière sur une affaire qui remonte à une dizaine d'années. Retour sur un dossier aux ramifications multiples, qui n'a pas encore livré tous ses secrets.
L'histoire commence avec l'Opération diligence menée par la SQ à la fin des années 2000 au sujet de l'infiltration de l'économie légale par le crime organisé.

La SQ entreprend une enquête au printemps 2007 après la plainte d'un entrepreneur en maçonnerie, qui affirmait que les Hells Angels tentaient d'infiltrer son entreprise.

L'enquête visait notamment à établir les liens entre la mafia, les motards et la Fédération des travailleurs du Québec (FTQ).

Puis, en septembre 2013, certains médias apprennent que Michel Arsenault, alors président de la FTQ et président du conseil d'administration du Fonds de solidarité de FTQ, a fait l'objet de surveillance électronique et de filature de la SQ, entre septembre 2008 et septembre 2009.

La fuite des transcriptions de cette surveillance électronique dans les médias arrive au moment où la commission Charbonneau se penche sur les milliers de conversations interceptées par la police au cours de l'Opération diligence.

Enquête sur les fuites

Le 10 septembre 2013, Michel Arsenault envoie une lettre à Stéphane Bergeron - alors ministre de la Sécurité publique - et l'exhorte à ouvrir une enquête sur l'origine de ces fuites. Il se dit alors victime d'une fuite d'informations illégale et « inacceptable ». Rappelons que Michel Arsenault n'a jamais fait l'objet d'accusations criminelles.

M. Arsenault confirme dans sa lettre qu'il a été avisé par la SQ au printemps 2009 qu'il était sous surveillance depuis déjà quelques mois. Il dit avoir pourtant eu l'assurance que la divulgation des transcriptions, images ou vidéos de cette surveillance était une infraction criminelle.

« Les fuites ne peuvent provenir que de deux sources, la Sûreté du Québec ou la CEIC [Commission d'enquête sur l'industrie de la construction]. Les procureurs de la CEIC ont assuré les procureurs du Fonds de solidarité FTQ que la fuite ne venait pas d'eux », écrit Arsenault dans sa missive.

M. Bergeron a affirmé en 2013 qu'il avait reçu la lettre de Michel Arsenault, mais qu'il ne lui avait pas parlé de vive voix. Une affirmation qu'il a réitérée mercredi.

Quelques heures après avoir été appelé par le ministre de la Sécurité publique, le directeur général de la SQ à cette époque, Mario Laprise, annonce le début d'une enquête pour tenter de découvrir la source de ces fuites.

Entrevue avec Guy Lapointe de la Sûreté du Québec Surveillance de six journalistes

Six journalistes, dont Marie-Maude Denis, Isabelle Richer et Alain Gravel, de Radio-Canada, et Éric Thibault, du Journal de Montréal, seront ciblés par cette investigation.

Au début de l'enquête, la Fédération professionnelle des journalistes du Québec (FPJQ) avait déclaré dans un communiqué de presse qu'elle craignait « que l'enquête n'amène à mettre des journalistes sous écoute, à saisir leur matériel ou à les forcer de révéler en cour le nom de leurs informateurs ».

Le capitaine de la SQ, Guy Lapointe, a confirmé mercredi à l'émission 24/60 que ces six journalistes avaient fait l'objet d'une enquête puisqu'ils étaient considérés comme des « suspects », en vertu de l'article 193 du Code criminel portant sur l'utilisation ou la divulgation d'une communication privée.

Il a précisé que l'opération visant ces journalistes, contrairement à celle dont a fait l'objet Patrick Lagacé, ne prévoyait aucune écoute électronique ni surveillance par géolocalisation des personnes visées.

Journalistes surveillés : Que savait Stéphane Bergeron?

Stéphane Bergeron, aujourd'hui porte-parole du Parti québécois en matière de sécurité publique, nie avoir demandé que les journalistes soient ciblés pour connaître l'origine de fuites de renseignements policiers dans les médias.

« C'est une initiative que je n'ai évidemment pas demandée, et c'est une initiative que je n'aurais jamais autorisée, et c'est une initiative dont je n'ai jamais été informé avant il y a quelques instants », a-t-il dit en conférence de presse, aux côtés de son chef, Jean-François Lisée.

Je m'attendais à ce qu'on enquête sur les fuites à l'interne, pas qu'on épluche les registres d'appels des journalistes

Stéphane BergeronRaymond Bachand, Arsenault et les fuites

Au cours d'une conférence de presse mercredi après-midi, M. Bergeron a laissé entendre que Raymond Bachand avait lui-même informé M. Arsenault du fait qu'il était sous écoute électronique.

« Bachand a communiqué avec M. Arsenault, a affirmé M. Bergeron. Comment se fait-il que Raymond Bachand ait eu cette information? [...] Comment une information aussi sensible a pu se rendre aux oreilles à un membre du conseil des ministres, qui a pris le téléphone et qui a dit au principal intéressé : "Tu fais partie d'une écoute électronique", risquant de faire dérailler une enquête policière? »

M. Bergeron s'appuie sur une conversation diffusée à la commission Charbonneau entre Raymond Bachand et M. Arsenault. Le leader syndical, qui souhaitait à l'époque être nommé au sein du conseil d'administration de la Caisse de dépôt et placement du Québec, voulait savoir pourquoi sa nomination semblait être bloquée, même si Jean Charest lui avait promis ce poste le 12 janvier 2009.

Quand M. Arsenault a demandé au ministre des Finances de l'époque, Raymond Bachand, si l'écoute électronique par la SQ était la raison pour laquelle il n'avait pas été nommé au C.A. de la Caisse de dépôt, M. Bachand n'a pas répondu. M. Arsenault a alors compris qu'il s'agissait bel et bien pour cette raison qu'il n'a pas obtenu le poste.

M. Arsenault affirme dans sa lettre à M. Bergeron qu'il a plutôt été averti par la SQ, conformément à la loi.

Global Times

Cybersecurity law to enhance State security

Thursday, 03 November 2016

Byline: Deng Xiaoci

Section: general

Beijing - China's draft cybersecurity law, which stipulates that foreign technology firms should store important business data and personal data related to their operation within China, is aimed at effectively safeguarding State security as well as protecting people's privacy, an expert said.
The comment came after Reuters reported that short-term rental company Airbnb told Chinese users that it will store their personal data locally "as foreign tech companies operating in China respond to increasing regulatory pressure."

A spokesperson with the Airbnb China confirmed with the Global Times on Wednesday on condition of anonymity that its parent company is moving Chinese mainland-based users' information including the guest bookings in China and Airbnb listings to local servers for greater localization.

Once the foreign technology firms store personal data they collect within China as the draft cybersecurity law stipulates, they have to comply with Chinese laws and will be punished if they get involved in personal data leak or dissemination of illegal information online under the Criminal Laws, Qin An, a cybersecurity expert at the China Institute for Innovation and Development Strategy, told the Global Times.

The law aims to prevent international frauds, especially the telecom scams from abroad, Qin said.

Le Soleil

Entre le marteau et l'enclume

Thursday, 03 November 2016

Byline: Gérard Latulippe

Section: oped

Opinion - Gérard Latulippe, ancien Haut commissaire(Trinité-et- Tobago) et ancien délégué général (Mexique, Bruxelles) Saint-Sauveur
Un jour, on demanda à Justin Trudeau quel gouvernement d'un autre pays il admirait le plus. Il répondit qu'il avait une certaine admiration pour le régime dictatorial de la Chine. Aujourd'hui, il est premier ministre.

L'AIGLE ET LE DRAGON

Récemment, les premiers ministres canadien et chinois se sont rendus visite mutuellement à l'intérieur d'une période d'un mois. Un partenariat stratégique en a résulté, couvrant la coopération en matière politique, économique, commerciale, sécuritaire et judiciaire. Il s'agit d'un précédent dans l'histoire de la diplomatie canadienne car il engage le Canada sur une voie qui pourrait mener à un réalignement de ses alliances traditionnelles. Cette danse avec le dragon ne se fera pas sans causer des remous chez notre voisin l'aigle américain.

Les contrastes parlent souvent par eux-mêmes. Pour les Chinois, c'est par le protocole que les messages sont clairs. Des pourparlers tenus à la Cité interdite, à Pékin, au dîner de famille au lac Harrington, à Gatineau, en passant par la mise au jeu en chandails du Canadien au Centre Bell, on a voulu démontrer le caractère historique de cette nouvelle alliance en allant bien au-delà du protocole des visites de chefs d'État. En septembre, la Chine accueille le G 20 à Hanglou. Le président Obama n'a pas eu droit au traditionnel tapis rouge à sa descente de l'avion, contrairement à tous les autres chefs d'État. Les

observateurs ont conclu avec justesse que c'était délibéré pour faire paraître les Américains diminués et faibles.

BRAS DE FER GÉOSTRATÉGIQUE ÉTATS-UNIS-CHINE

Les États-Unis et la Chine sont au coeur d'un bras de fer géostratégique à l'échelle de la planète. Le monde est témoin des tensions grandissantes et des luttes de pouvoir titanesques entre les deux pays. La puissance américaine est en voie de s'effriter au profit de la Chine. L'année dernière, l'ambassadeur de Chine a déclaré qu'il souhaitait que le Canada cesse de se concentrer sur les États-Unis et porte son regard sur la zone Asie-Pacifique. En d'autres termes, la Chine souhaite que le Canada réduise sa dépendance vis-à-vis des États-Unis pour être entraîné de plus en plus sous l'influence de la Chine.

UNE NOUVELLE MENACE VENUE DU NORD?

Le premier ministre Trudeau s'est engagé dans une coopération tous azimuts avec la Chine. La déclaration conjointe lors de la visite du premier ministre chinois contient 29 initiatives pour lesquelles des ententes ont été signées. En matière économique, la Chine s'intéresse principalement à nos ressources naturelles, nos produits agricoles, notre technologie en particulier dans les secteurs stratégiques et par-dessus tout à notre accès au marché américain. Les Chinois ne se limitent pas à importer nos ressources mais ils sont hautement intéressés à investir dans nos entreprises spécialement celles représentant un intérêt stratégique.

Or le peuple américain considère comme une menace sérieuse la montée en puissance de la Chine. Une étude récente du PEW Research Center a démontré que plus de 85 % des Américains sont préoccupés par les emplois perdus aux mains de la Chine, du déficit commercial américain, du cyberespionnage chinois et de leurs violations des droits de la personne. Peu importe le résultat des élections présidentielles, les Américains ressentiront comme un danger imminent l'influence croissante du dragon chinois chez leur voisin du nord.

Le territoire d'un pays s'impose à sa politique internationale. Demandez-le aux Ukrainiens, voisins de la Russie. Demandez-le aux Japonais voisins de la Chine. L'histoire du Canada a démontré l'impact sur nos choix de politique extérieure de notre proximité territoriale avec les États- Unis.

Un accord de libre-échange Canada-Chine soulèvera des inquiétudes aux États-Unis. Il existe des risques importants que la Chine puisse utiliser l'effet combiné d'un éventuel accord de libre-échange avec le Canada et de l'ALENA pour exporter aux États Unis des biens exempts de droits de douane. Cet accès privilégié au marché américain leur est impossible actuellement. Or, l'opinion américaine est déjà défavorable à l'ALENA et plus de 75 % des exportations de marchandises canadiennes sont destinées à nos voisins américains. La table est mise pour des tensions à venir.

Récemment, le club des milliardaires chinois a visité le Canada. Ils n'ont pas caché leur intérêt à investir dans les industries technologiques. Qu'il s'agisse des technologies environnementales, de l'énergie

propre, de la robotique, les États-Unis, au même titre que le Canada, n'ont pas intérêt à ce que la Chine s'empare des secrets industriels d'importance pour la conquête des marchés mondiaux.

Les intérêts sécuritaires canadiens et américains sont intrinsèquement liés. L'espionnage stratégique et industriel chinois constitue une préoccupation majeure pour les Américains. Le gouvernement et les entreprises canadiennes sont aussi victimes du cyberespionnage chinois. Les services d'intelligence canadiens et américains collaborent étroitement sur la question sécuritaire à travers le monde, incluant les risques émanant de la Chine. Il existe un partenariat stratégique très étroit entre la Chine et la Russie, trop souvent sous-estimé. Au mois de juillet dernier, Putin effectuait sa 15e visite en Chine. Ce partenariat stratégique est clairement dirigé contre les États-Unis et leurs alliés, en particulier l'OTAN.

L'intensification radicale des relations avec la Chine finira-t elle par miner la collaboration stratégique en matière de sécurité du Canada avec les États-Unis et ses alliés de l'OTAN? Nul doute qu'il s'agit d'un objectif à long terme de la Chine.

LA NAÏVETÉ N'A PAS DROIT DE CITÉ

La Chine est la deuxième puissance mondiale. Ottawa a évidemment intérêt à conserver de bonnes relations et accroître son commerce bilatéral. Le régime chinois est brutal et impitoyable. Il considère la nouvelle relation avec le Canada comme une opportunité en or dans la partie d'échecs avec les États-Unis pour la primauté universelle. Le gouvernement Trudeau n'a entrepris aucune consultation et débat public avant de s'engager dans cette nouvelle alliance comportant autant de dangers que de bénéfices. Elle compte des risques considérables pour notre relation bilatérale avec les États-Unis et notre relation multilatérale avec le monde occidental. La naïveté n'a pas droit de cité dans ce contexte.

Illustration(s) :

PHOTOTHÈQUE LE SOLEIL

Selon l'auteur, on a voulu démontrer le caractère historique de la nouvelle alliance entre le Canada et la Chine en allant au-delà du protocole des visites de chefs d'État, notamment en procédant à une mise au jeu en chandails du Canadien de Montréal.

Journal de Montréal

Le ministre veut une enquête administrative

Thursday, 03 November 2016

Byline: Marc-André Gagnon

Section: general

Québec - La surveillance des registres téléphoniques d'au moins six journalistes par des policiers en 2013 serait une première en 20 ans pour la Sûreté du Québec, a fait savoir hier le ministre de la Sécurité publique, Martin Coiteux, qui a donné le feu vert à une enquête administrative.
«L'enquête qu'on va faire [...] pourrait donner lieu à des sanctions contre des personnes qui auraient mal agi, qui n'auraient pas respecté les règles», a souligné le ministre en début de soirée, hier.

M. Coiteux a assuré que cette enquête se fera «en totale indépendance» même si la SQ relève de son ministère.

APRÈS UNE PLAINTE

Le ministre trouve aussi «assez particulier» que l'enquête policière au cours de laquelle des journalistes ont été épiés par la SQ en 2013 ait été lancée après une intervention du ministre de la Sécurité publique de l'époque, le député péquiste Stéphane Bergeron (voir autre texte)

«C'est quand même curieux ce qui s'est passé, a réagi M. Coiteux. [...] Une lettre est arrivée à son cabinet le matin et le soir, une enquête était déclenchée [par la SQ]. [...] La coïncidence est grande.»

La Presse+

La protection gruyère

Thursday, 03 November 2016

Byline: Paul Journet

Section: editorial

Editorial - « Le projet de loi déposé l'année dernière par le gouvernement Couillard n'offre qu'une moitié de bouclier. »
Chaque jour amène de nouvelles révélations troublantes sur l'espionnage de journalistes par le Service de police de la Ville de Montréal (SPVM) et maintenant la Sûreté du Québec (SQ).

En réaction à la « grave » attaque du SPVM contre la liberté de la presse, le premier ministre Couillard a annoncé mardi trois mesures :

- Le Directeur des poursuites criminelles et pénales devra désormais autoriser tout mandat de surveillance sur un journaliste, comme c'est déjà le cas pour les avocats, juges et députés ;

- Un comité d'experts indépendants recommandera comment mieux protéger les sources journalistiques ;

- Une inspection sera menée sur la façon dont les policiers (SPVM, SPVQ et SQ) surveillent et interceptent les communications de citoyens, particulièrement les journalistes.

À Ottawa, le sénateur indépendant André Pratte et le Bloc québécois songent à déposer un projet de loi pour mieux protéger les sources journalistiques, tandis que le Nouveau Parti démocratique demande une enquête fédérale.

Puis, hier après-midi, on a appris que la SQ a surveillé six journalistes. Peu après, le ministre de la Sécurité publique, Martin Coiteux, annonçait une enquête administrative sur la SQ.

Il faudra vérifier si les mécanismes choisis sont encore adéquats pour faire la lumière sur l'ensemble des dérives. Et il faudra s'interroger sérieusement sur la confiance que méritent les patrons actuels de la police.

Mais pendant que les projecteurs se braquent sur ces crises, un mauvais projet de loi continue d'avancer tout doucement à l'Assemblée nationale : celui sur les dénonciateurs (PL87). C'est d'une triste ironie, car il concerne la chasse aux sources, cette dérive à l'origine de la surveillance des journalistes.

Le PL87 ne concerne pas que les médias. Il vise à protéger ceux qui dénoncent un problème à un journaliste, mais aussi à leur supérieur ou aux policiers.

C'est grâce à ces sonneurs d'alarme que les scandales dans l'industrie de la construction ont été révélés. Voilà pourquoi l'Unité permanente anticorruption proposait de renforcer leur protection contre les représailles. Il s'agissait même de sa toute première recommandation faite à la commission Charbonneau, qui l'a reprise dans son rapport.

Le projet de loi déposé l'année dernière par le gouvernement Couillard n'offre qu'une moitié de bouclier. Certes, les libéraux ont raison de chercher un équilibre pour ne pas créer un climat de méfiance et de dénonciation constante, mais cet équilibre ne se trouve pas dans la version actuelle du PL87.

D'abord parce qu'il ne protège pas assez de gens. Il s'applique aux employés de l'État, mais pas à ceux du municipal ni aux contractants privés. Or, la commission Charbonneau a démontré que c'est là que se situaient les pires dérives.

Ensuite, parce que le PL87 ne protège pas assez de types de dénonciations. Pour être couvertes par la loi, elles doivent être adressées à un responsable désigné de son organisme ou au Protecteur du citoyen. Les dénonciations aux médias ne sont pas protégées, sauf s'il s'agit d'une « urgence » liée à la sécurité, la santé et l'environnement, et si le problème a d'abord été signalé aux policiers...

C'est trop restrictif, car ces critères excluent par exemple le gaspillage de fonds publics. Et c'est trop contraignant, car le fardeau de la preuve repose sur le dénonciateur. Pour s'en convaincre, on n'a qu'à se souvenir de François Beaudry. En 2003, cet ingénieur découvrait la collusion dans l'attribution de contrats publics à Laval. Il a prévenu ses supérieurs du ministère des Transports, puis les policiers, et rien ne s'est passé. Six ans plus tard, il se tournait vers les médias, à ses propres risques.

Aujourd'hui, M. Beaudry juge le PL87 « cosmétique, voire inutile ». Ce projet de loi n'aurait rien fait non plus pour de courageux dénonciateurs comme Karen Duhamel, ingénieure au privé qui avait dénoncé les « mottons d'argent » échangés sur les chantiers.

Devant ces critiques, le président du Conseil du trésor, Sam Hamad, avait promis l'hiver dernier de protéger aussi les employés du municipal. Son successeur, Carlos Leitao, assure maintenant que ce sera fait dans un futur projet de loi. Mais on l'attend encore, et cela ne corrigerait pas la logique du projet de loi, qui garderait les dénonciations à l'intérieur des organismes.

Quand l'air devient vicié, il faut ouvrir les fenêtres et laisser jaillir la lumière.

Illustration(s) :

PHOTO IVANOH DEMERS, ARCHIVES LA PRESSE

Une inspection sera menée sur la façon dont les policiers (SPVM, SPVQ et SQ) surveillent et interceptent les communications de citoyens, a annoncé le premier ministre Couillard.

Journal de Montréal

Le milieu journalistique craint un climat de peur chez les sources

Thursday, 03 November 2016

Byline: Benoit Philie

Section: general

Montréal - Selon des experts, le téléphone des journalistes pourrait moins sonner
Un climat de peur pourrait se créer chez les sources à la suite des nombreuses révélations de surveillance policière dans les téléphones des reporters, déplore le milieu journalistique.

«On craint que le public et les divulgateurs prennent peur et arrêtent de contacter les journalistes, a dit Benoîte Labrosse, secrétaire-trésorière de la Fédération professionnelle des journalistes du Québec. C'est le public qui sera encore perdant et qui sera laissé dans la noirceur.»

SURVEILLANCE

En début de semaine, La Presse révélait que son chroniqueur Patrick Lagacé avait fait l'objet d'une étroite surveillance de la police de Montréal dans le cadre d'une évidente chasse aux sources journalistiques. On a aussi révélé que les registres téléphoniques de trois reporters avaient également été étudiés, soit Félix Séguin, de notre Bureau d'enquête, Monic Néron, du 98,5 FM et le journaliste indépendant Fabrice de Pierrebourg. La Sûreté du Québec a épié les téléphones de six journalistes en 2013, a-t-on aussi appris hier.

«Le journalisme, c'est un service public à la population. Il sert à surveiller et quand on y fait entrave, c'est directement la population que ça affecte», a déploré Pascale St-Onge, présidente de la Fédération nationale des communications.

La FPJQ constate que ce sont essentiellement des journalistes d'enquête qui sont concernés.

GROS DOSSIERS

«Les sources de ces gens-là concernent de gros dossiers, a dit Benoîte Labrosse. On n'a qu'à penser aux scandales de la construction et des commandites. Ce sont des cas extrêmes. S'il n'y avait pas eu de sources internes, on n'aurait jamais trouvé». La FNC s'inquiète aussi de l'effet qu'aura cette révélation sur le travail des journalistes.

«Ce n'est pas anodin que ce soit des journalistes d'enquête qui sont visés. Ils débusquent les scandales de corruption et de collusion. Ils fatiguent la police et le gouvernement», a soutenu Pascale St-Onge, présidente de la FNC.

«Tout ça pourrait refroidir certaines personnes de parler, des gens qui auraient voulu le faire et qui ne le feront pas», a-t-elle dit.

Le Droit

La police de Gatineau se défend

Thursday, 03 November 2016

Byline: Journaliste maison

Section: general

Gatineau - La police de Gatineau n'a pas, à la connaissance de son directeur adjoint, multiplié les démarches pour prendre connaissance des appels entre journalistes de la région et ses policiers. La seule exception, explique Luc Beaudoin, est celle qui a été faite envers le journaliste de TVA Gatineau-Ottawa, Pierre-Jean Séguin. Mercredi, la station de télévision indiquait que la police avait fait des vérifications après que de l'information ait été coulée. M. Beaudoin a pris l'exemple d'une intervention policière impliquant un homme barricadé. « On parle d'une enquête active, dit-il. Des policiers arrivés sur une scène étaient préoccupés par les médias déjà présents et il fallait s'assurer de la sécurité des policiers. On a regardé les communications pour savoir d'où provenait l'information. C'est un petit groupe restreint qui pouvait avoir l'information. » Cette semaine, plusieurs journalistes du Québec ont appris avoir fait l'objet de vérifications de corps policiers en ce qui a trait à leurs communications, souvent confidentielles.

Radio-Canada (Nouvelles -web)

Journalistes espionnés : une « menace à notre démocratie », dit Edward Snowden

Thursday, 03 November 2016

Byline: d'Olivier Arbour-Masse

Section: general

Montréal - « Une attaque radicale à la liberté de presse » et « une menace à notre modèle traditionnel de démocratie ». Voilà ce qu'Edward Snowden pense de « l'affaire Lagacé » et des six autres cas de journalistes espionnés par des corps de police québécois.
Le célèbre lanceur d'alerte avait déjà commenté à deux reprises sur Twitter le dossier de l'heure dans l'actualité québécoise. Il a eu l'occasion d'étayer sa pensée mercredi soir, dans une vidéoconférence organisée à l'Université McGill, à Montréal.

Des centaines d'étudiants ont fait la file pendant des heures afin de pouvoir entendre l'homme qui a permis de dévoiler les programmes de surveillance à grande échelle de la National Security Agency (NSA) aux États-Unis.

Sa conférence ne pouvait se tenir à un moment plus opportun. Quelques heures avant qu'il prenne la parole devant un amphithéâtre bondé, on apprenait que la Sûreté du Québec a épié en 2013 les appels de six journalistes, dont Marie-Maude Denis, Isabelle Richer et Alain Gravel de Radio-Canada.

En début de semaine, le Service de police de la Ville de Montréal (SPVM) s'est retrouvé sous les projecteurs pour avoir colligé les relevés d'appels et les métadonnées du journaliste de La Presse Patrick Lagacé.

Oh, Canada... https://t.co/D6kUPPDJ27 pic.twitter.com/KpmvbVYw8d

-- Edward Snowden (@Snowden) 2 novembre 2016

Snowden estime que le chef du SPVM Philippe Pichet doit démissionner pour « restaurer la confiance (du public) et rétablir les bases de l'imputabilité ».

M. Pichet, qui bénéficie toujours de l'appui du maire Denis Coderre, défend ses enquêteurs en affirmant qu'ils ont agi selon les lois en demandant et en obtenant l'autorisation d'espionner Patrick Lagacé auprès de la juge de paix Josée de Carufel.

Or, le problème se situe précisément au niveau de la loi, selon Edward Snowden.

Peut-on reconnaître ou à tout le moins débattre raisonnablement d'une nouvelle idée qui peut paraître un brin radicale? La loi commence à échouer dans sa mission de garantir nos droits.

Edward Snowden

« On ignore toujours selon quelle loi cette autorisation [de surveiller les journalistes] a été donnée », remarque-t-il.

« Le gouvernement peut s'introduire dans nos vies privées sans presque rencontrer d'entrave alors que nous, les citoyens, ne savons presque rien sur sa façon d'opérer », poursuit-il, depuis la Russie où il est réfugié pour échapper aux accusations de trahison qui pèsent contre lui aux États-Unis.

Le Canada et C-51 critiqués

Snowden est catégorique : impossible de se fier aux dirigeants des agences de renseignement pour respecter les lois protégeant la vie privée.

« La seule façon de s'assurer qu'ils jouent selon les règles, c'est en les menaçant de sanctions criminelles », lance-t- il.

Ainsi, Snowden propose de créer une autorité indépendante chargée d'étudier au cas par cas les agissements de ces agences et de les poursuivre devant les tribunaux si elles devaient transgresser la loi.

Or, « le Canada a le plus faible processus de supervision de ses services de renseignement parmi les pays occidentaux », avance l'ancien de la CIA et de la NSA.

À ses yeux, il s'agit là de la principale lacune de la loi antiterroriste C-51, adoptée par le gouvernement Harper et qualifiée par ses détracteurs de menace pour la vie privée. « Elle ne prévoit pas de supervision digne de ce nom », dit-il.

« [Justin Trudeau] a fait campagne en promettant de la réformer, mais ne l'a malheureusement pas fait, remarque Snowden. La plupart des experts estiment qu'elle est impossible à réformer de façon significative et qu'elle doit être abolie pour faire place à une nouvelle loi. »

Tous les pays surveillent leurs citoyens, détaille Snowden. « C'est la première fois de l'histoire que c'est technologiquement et logistiquement possible pour les gouvernements de traquer nos vies. Ce n'est pas de la science-fiction, ça se produit maintenant. »

Les outils technologiques qui devaient nous autonomiser sont désormais utilisés pour restreindre nos libertés.

Edward Snowden

Métadonnées et protection

Le SPVM n'a peut-être pas eu accès au contenu des conversations de Patrick Lagacé, mais les métadonnées de son téléphone sont suffisantes pour tracer un portrait précis de ses communications.

« Quand tu as les métadonnées, tu n'as pas besoin du contenu, explique Snowden. Ça dresse un rapport détaillé de la vie privée.Tu peux savoir où la personne va, qui elle rencontre, à qui elle parle, combien de temps... »

Edward Snowden suggère aux journalistes ainsi qu'à tout citoyen d'utiliser l'application Signal pour crypter leurs communications.

« Nous sommes tous surveillés, qu'on soit un criminel ou non », rappelle-t-il, ajoutant que « le droit à la vie privée est à la base de tous les autres droits ».

Le portrait qu'il dresse est sombre, mais le réfugié de 33 ans garde espoir de voir les politiques se réformer pour le mieux. « Les jours de la surveillance de masse sont comptés. Nous aurons droit à un futur plus juste et plus libre que ce dans quoi nous vivons. »

« Ce sera la décision de votre génération », a-t-il conclu en interpelant les étudiants réunis pour l'écouter.

Le Devoir (site web)

Snowden secoue le meilleur des mondes

Thursday, 03 November 2016

Byline: Sarah R. Champagne

Section: general

Moscou - Le moment n'aurait pu être mieux choisi pour entendre le plaidoyer d'Edward Snowden. La mise en garde du plus célèbre lanceur d'alerte du XXIe siècle résonne particulièrement fort au milieu de cette semaine où l'espionnage de plusieurs journalistes ne laisse plus de doutes.
Il est apparu sur écran géant en direct de Moscou, par une vidéoconférence à l'Université McGill. Le tonnerre d'applaudissements calmé, il affirme peu après : « Nous sommes tous surveillés, ce n'est pas de la science-fiction et ça arrive maintenant. » Prenant pour exemple les récents événements locaux, il s'inquiète de « cette attaque radicale de la liberté de presse, qui représente une menace au modèle traditionnel de notre démocratie ».

Ces scandales constituent en fait de nouveaux épisodes des dérives des appareils de renseignement, peu importe l'échelle. Plus important encore, le rythme des avancées technologiques de la surveillance organisée « a dépassé le contrôle démocratique » , insiste Snowden.

Le temps où une grande équipe et des moyens extrêmement coûteux étaient nécessaires pour espionner une seule personne est loin derrière. « Cette dynamique s'est inversée complètement , dit-il, dans un contexte où une seule personne, loin de ses cibles, peut en traquer un nombre extraordinairement grand avec des précisions inimaginables. » Ce changement fondamental et dangereux pour le droit à la vie privée est sa motivation première à sonner l'alarme.

En disant ces mots, son écran s'obscurcit un bref instant. Il montre à la foule une photo d'un immense entrepôt de données. « Les gouvernements n'ont pas demandé la permission du public pour s'impliquer dans ce genre de collecte » , au contraire, la négation de cette réalité a tout simplement empêché le débat.

La menace, toujours

En plus de l'innovation technologique, les gouvernements brandissent des « supermenaces, des ennemis terroristes de plus en plus grands » pour demander de plus en plus de pouvoirs. Cette « politique de la peur » a changé la manière dont les lois sont passées, selon lui. « Comment peut-on préserver une société libre dans un contexte de gouvernement illimité ? » demande-t-il à l'assistance.

La justice s'est pliée aux demandes des corps policiers au Québec après tout, a-t-il rappelé, sans que les chefs de police admettent que cette surveillance allait trop loin. « La loi est en train de faillir à son devoir de protéger nos droits » , réitère Snowden. Et ce droit à la vie privée est la base même de nos sociétés, ce qui permet au « soi » d'exister.

La forte affluence a pris au dépourvu les organisateurs. Quelques minutes avant le début de la vidéoconférence, des centaines de personnes débordées dehors et scandant « laissez-nous entrer » se sont élancées dans le bâtiment pour tenter d'entrer. Prenant acte de la popularité du rendez-vous -- et de piquets de grève qui ont dû être franchis par le public pour l'entendre -- l'ancien consultant de la National Security Agency (NSA) s'est montré patient et très attentif à la série de questions posées en majorité par des étudiants.

C'est à travers une interface virtuelle qu'il est forcé d'apparaître le plus souvent depuis trois ans, puisqu'il vit réfugié en Russie. En 2013, il a déclenché une tempête politique, diplomatique et sociale en révélant l'ampleur de la toile de surveillance des communications par les services secrets américains.

Considéré comme un héros par les groupes de défense des libertés, il est inculpé pour espionnage aux États-Unis, où il risquerait jusqu'à 30 ans de prison. Les documents obtenus par Snowden et diffusés au public grâce à deux journalistes révélaient que la NSA avait surveillé systématiquement téléphones, cellulaires, courriels. Les communications de millions de citoyens, ainsi que celles de chefs d'État, pouvaient donc potentiellement être scrutées par les autorités.

Des lois concernant la vie privée des utilisateurs d'Internet ont été modifiées depuis ces révélations. Le jeune trentenaire a demandé au président américain, Barack Obama, de lui accorder le pardon, pardon qui lui a été refusé à maintes reprises. En conclusion de sa conférence, Snowden a d'ailleurs souhaité répéter l'expérience à Montréal, en personne cette fois.

En attendant, « c'est entre vos mains ».

La Presse+

Bienvenue dans le Club

Thursday, 03 November 2016

Byline: Patrick Lagacé

Section: column

Chronique - Alain (Gravel) ! Éric (Thibault) ! Denis (Lessard) ! Marie-Maude (Denis) ! Isabelle (Richer) ! Enchanté, moi, c'est Affaire. Comme dans Affaire Lagacé. Je me suis trouvé un nouveau prénom, cette semaine.

Bienvenue, donc. Oui, bienvenue dans le Club des Journalistes espionnés ! Le local ne paie pas de mine, comme vous le voyez, mais c'est chaleureux !

Il y a de la bière dans le frigo (achetez-en de temps en temps), le mot de passe du WiFi est sur le routeur et le divan est un peu miteux, mais au moins on a le câble : RDI, LCN, TVA Sports, RDS, Canal Vie...

Pour le téléphone, avant de faire un interurbain, faites le 9 et...

C'est une blague, je n'ai pas fait installer le téléphone.

On ne sait jamais, hein ?

Blague à part, je suis content de vous recevoir. Je me sentais un peu seul, ici...

***

Je l'ai dit toute la semaine : je suis sûr que je ne suis pas le seul à avoir été espionné par la police.

Je pensais surtout au Service de police de la Ville de Montréal (SPVM), dont les réponses au sujet de l'espionnage d'autres journalistes ont été on ne peut plus évasives...

Et là, hier, paf, on a su le résultat des vérifications internes faites par la Sûreté du Québec (SQ) dans la foulée des révélations de La Presse : en 2013, six journalistes ont fait l'objet de mesures que Nixon à son plus parano n'aurait pas reniées.

Six. Et pas les moindres : le chef de bureau de La Presse à Québec, les deux têtes d'affiche de l'émission Enquête de l'époque, un journaliste d'enquête du JdeM, une star du journalisme judiciaire radio-canadien. Juste ça !

Six journalistes dont on a espionné les appels entrants et sortants, dans la foulée des révélations de Félix Séguin et d'Andrew McIntosh de TVA/Journal de Montréal, qui ont révélé le capotage scandaleux de Diligence II.

Je ne referai pas l'histoire de Diligence II. D'abord, j'aurais l'impression de me répéter encore, encore et encore.

Et puis Yves Boisvert, dans sa chronique du jour, en fait un superbe résumé, en esquintant Stéphane Bergeron, du PQ, ministre de la Sécurité publique de l'époque, qui le mérite amplement.

Mais Diligence est un cas d'école sur les dérives d'une police politique. On vient d'en constater un autre exemple, avec cet espionnage à l'échelle industrielle des journalistes...

Non, permettez que je fasse des liens entre les plus hauts échelons du SPVM et la SQ.

Chacun, à sa façon, semble être un nid d'intrigues politiques. Au SPVM, quand un directeur quitte son poste, s'engage inévitablement une campagne électorale aussi silencieuse que criarde, où à peu près tous les coups sont permis.

Je vous jure, ces courses à la direction sont l'équivalent « constabulaire » de Game of Thrones.

On fait circuler des rumeurs. On salit. On tente de « couler » aux journalistes des informations que l'on pense compromettantes, par exemple, sur l'un ou alors sur l'autre. Chacun tente de se positionner, avec sa garde rapprochée, pour gagner le siège du directeur...

Après ces campagnes électorales, le plus souvent, il faut beaucoup de temps pour nettoyer le sang. Les équipes « perdantes » voient leurs membres exilés dans quelque corps de police de banlieue, ou alors ils sont tablettés dans le SPVM...

Mettez dans l'équation un nouveau maire omnipotent qui politise l'information dans toute son administration, ledit maire qui choisit le chef de police et... Et ça fait beaucoup, beaucoup de politique dans la police de Montréal.

À la SQ, c'est House of Cards. Il y a des fonds secrets qui mènent à des enquêtes criminelles contre d'anciens officiers, des directeurs sans sécurité d'emploi qui se font sacrer dehors quand un nouveau parti arrive au pouvoir... Il y a des policiers qui se sentent obligés de « protéger » le pouvoir, par exemple en l'avertissant qu'une enquête est en cours sur des personnages bien en vue... Il y a, pendant des années, absence totale d'enquêtes sur la corruption à quelque échelle que ce soit, dans la sphère politique... Un ministre pense que c'est sa job de demander à la police « kesséça ? » quand un leader syndical rouspète, plutôt que de diriger ledit leader vers le poste de police le plus proche...

Ça fait, encore là, beaucoup, beaucoup de politique dans la police provinciale.

On ne me sortira pas de la tête que la pression politique, subtile ou pas, pousse la police à commettre des gestes stupides.

Comme tout ce qui sort depuis lundi.

***

Le Club des Journalistes espionnés a donc pignon sur rue. J'annonce par la présente que Fabrice, Monic et Félix sont pour l'instant membres stagiaires. Ils n'ont été, après tout, qu'informellement espionnés par le SPVM, via un logiciel maison qui épluchait les factures téléphoniques des flics, à la recherche de leurs numéros de téléphone...

Je suis certain que le Club admettra bientôt de nouveaux membres, c'est forcé.

Tenez, je cherche une chute pour cette chronique et je lis qu'André Cédilot, ancien as reporter aux affaires criminelles de La Presse, était également visé par la SQ...

Voici ta carte de membre permanent, André. Remplis le frigo de temps en temps, s'il te plaît...

Manque Boisvert. Ils t'espionnent pas, toi, Yves ? Me poserais des questions, à ta place...

La Presse+

Les Canadiens mal protégés contre la surveillance abusive, selon Snowden

Thursday, 03 November 2016

Byline: Marc Thibodeau

Section: general

Montréal - Le lanceur d'alerte américain prenait part à une vidéoconférence organisée par l'Université McGill, hier
Les Canadiens sont très mal protégés contre les pratiques de surveillance abusives, estime Edward Snowden, qui s'alarme des possibilités ouvertes aux services de renseignements d'ici et d'ailleurs par les nouvelles technologies de communication.

L'ex-sous-traitant de la National Security Agency (NSA), qui participait hier à une vidéoconférence organisée par l'Université McGill, a souligné que le système de régulation des services de renseignement canadiens était probablement le plus « déficient en Occident ».

Il a déploré à ce titre que le gouvernement libéral de Justin Trudeau tarde à réviser la Loi antiterroriste, dite loi C-51, qui confère des pouvoirs accrus à ces mêmes services.

Nombre d'analystes, a-t-il relevé, pensent que la loi en question est trop mal formulée pour être modifiée et devrait tout bonnement être retirée.

M. Snowden estime qu'il n'est tout simplement pas possible, ici ou ailleurs, de faire confiance aux autorités pour utiliser de manière responsable les technologies de surveillance existantes.

Longtemps, le coût et la complexité de la surveillance limitaient son utilisation, mais ce n'est plus le cas aujourd'hui, et les risques d'atteinte à la vie privée sont décuplés.

« N'importe quel gars assis loin de sa cible, comme moi quand j'étais basé à Hawaii, peut surveiller à distance un nombre inimaginable de personnes. »

-- Edward Snowden

La seule manière de s'assurer que les agences de renseignements « jouent le jeu honnêtement est la menace de poursuites criminelles », a souligné le lanceur d'alerte, qui suggère de confier à une instance indépendante le pouvoir de passer en revue les enquêtes menées par les services de renseignements pour s'assurer de leur légalité.

Le manque de transparence actuel, dit-il, confère aux États un pouvoir démesuré face aux citoyens. « Il y a un déséquilibre qui est antidémocratique et autoritaire par nature », a-t-il lancé.

Des milliers de personnes

La vidéoconférence a commencé avec une heure de retard en raison de la forte demande et des actions d'un groupe d'employés syndiqués de l'établissement qui ont perturbé l'entrée du public.

Les organisateurs ont été pris de court lorsque des milliers de personnes ont afflué vers le bâtiment où se tenait l'événement.

Après avoir longuement patienté, des personnes ont couru de l'extérieur vers la salle où se tenait la conférence dans l'espoir de s'assurer une place pour voir l'ex-employé de la NSA, qui vit aujourd'hui en exil en Russie.

C'est le cas notamment de Marco Manglaviti, étudiant de 22 ans, qui a commencé à faire la file trois heures avant l'heure d'ouverture annoncée des portes. « C'est une sorte de vedette rock, en tout cas dans le monde des technologies », a-t-il relevé avant que l'invité n'apparaisse à l'écran sous les applaudissements de la foule.

M. Snowden, qui a dû patienter à quelques reprises en raison d'ennuis techniques, s'est réjoui de cette marque d'enthousiasme à son égard.

Il a insisté du même souffle sur le fait que son histoire personnelle n'avait guère d'importance face aux enjeux suscités par les pratiques de surveillance des États.

« La question la plus importante est ce qui est en train de tous nous arriver », a-t-il déclaré.

« Il y a un déséquilibre qui est antidémocratique et autoritaire par nature. »

-- Edward Snowden, à propos du manque de transparence actuel des États

Illustration(s) :

Photo Edouard Plante-Fréchette, La Presse

Edward Snowden participait hier à une vidéoconférence organisée par l'Université McGill.

La Presse+

Ils ont dit...

Thursday, 03 November 2016

Byline: Philippe Teiscera-Lessard; Louis-Samuel Perron; Martin Croteau; Vincent Brousseau-Pouliot

Section: general

Québec - L'espionnage de journalistes par la Sûreté du Québec et le Service de police de la Ville de Montréal a soulevé une vague d'indignation et d'inquiétudes parmi les journalistes visés et au sein du monde politique.
« Je couvre la politique depuis près de 40 ans, souvent sur des dossiers délicats. On se dit toujours que c'est possible d'être épié par les policiers, mais on est convaincu qu'ils n'oseraient pas aller jusque-là. Bien, il semble qu'on se soit trompé. »

Denis Lessard, chef du bureau parlementaire de La Presse à Québec

« Je suis assez surpris de voir qu'un juge de paix ait pu autoriser un mandat à mon sujet alors que je n'avais pas écrit sur Michel Arsenault. [...] Le seul motif que je vois pour faire l'objet d'un mandat, c'est que ma conjointe [Marie-Maude Denis] avait déjà fait des reportages sur Michel Arsenault. »

Éric Thibault, Journal de Montréal

« J'ai toujours été super prudente avec mes sources confidentielles, mais évidemment, on ne se bat pas à armes égales avec la police, qui a des moyens d'enquête comme ça. L'avenir nous dira - ou peut- être ne le saurons-nous jamais - tout ce qu'ils savent sur moi. »

Marie- Maude Denis, Radio-Canada

« C'est comme si toutes nos grandes certitudes sur la société dans laquelle on vit venaient de s'effriter d'un coup sec. J'en avais, mais c'est terminé. J'en ai pas mal moins. [...] Aujourd'hui, on a eu des confirmations de la part d'une source extrêmement crédible, et je suis estomaquée. »

Isabelle Richer, Radio-Canada (Source : SRC)

« On peut parler d'un triangle PQ-FTQ-SQ. Il y a des questions qui se posent, et la proposition qu'on fait, la proposition d'une enquête publique, ça permettrait d'entendre tout le monde. »

Simon Jolin-Barrette, député de la Coalition avenir Québec

« Les révélations des dernières heures nous inquiètent énormément. [...] De toute évidence, c'est une partie de pêche parce que c'est plusieurs journalistes en même temps, ce n'était donc pas pour un mandat en raison d'une information précise. Ce genre de pratique n'appartient pas au Québec, ce genre de pratique appartient à des pays que je n'ose même pas nommer. »

Amir Khadir, député de Québec solidaire

« La réponse de la SQ de dévoiler [ces informations] démontre que le public a besoin d'être rassuré. Ce sont des questions auxquelles [la GRC et le SCRS] doivent répondre. On continue de demander une enquête publique qui nous permettrait de constater les faits : est-ce une pratique répandue ou arbitraire ? »

Matthew Dubé, porte-parole du NPD en matière de sécurité publique

« Comme n'importe qui, je vois que si la SQ et le SVPM le font, je ne tomberais pas en bas de ma chaise [si les corps policiers fédéraux le font aussi]. Le ministre Goodale doit demander des comptes aux services policiers sous sa juridiction et rendre des comptes en Chambre aussi. »

Rhéal Fortin, chef par intérim du Bloc québécois

« Bien que le premier ministre Philippe Couillard ait annoncé de nouvelles mesures afin de protéger les sources, il faudra en faire davantage pour assurer une pratique journalistique saine. Il est grand temps que le gouvernement envisage l'adoption d'une loi qui consacrerait la protection des sources. »

Pascale St-Onge, présidente de la Fédération nationale des communications (FNC- CSN)

« Les nouvelles révélations d'aujourd'hui confirment nos pires craintes, c'est-à-dire que d'autres journalistes aient été victimes d'espionnage policier. C'est pourquoi nous estimons qu'une enquête publique est plus que jamais nécessaire pour faire la lumière sur ces pratiques policières indignes d'une démocratie. Comment a-t-on pu en arriver là ? Comment des juges ont-ils pu permettre cela ? Il est impératif que les corps policiers fournissent une liste exhaustive des journalistes qui ont fait l'objet de surveillance, y compris au niveau fédéral. »

Jean-Thomas Léveillé, président de la Fédération professionnelle des journalistes du Québec (FPJQ), aussi journaliste à La Presse

Le Devoir

Liberté de presse - La SQ a espionné six journalistes

Thursday, 03 November 2016

Byline: Philippe Orfali

Section: general

Québec - Le ministre de la Sécurité publique ordonne une enquête administrative
En lieu et place de l'" affaire Lagacé ", il faudra désormais traiter du scandale de la surveillance des journalistes : la Sûreté du Québec a confirmé mercredi qu'elle avait, tout comme la police de Montréal, traqué des reporters au cours des dernières années dans le cadre d'une enquête, suscitant une nouvelle vague d'inquiétudes et de dénonciations dans l'univers des médias.

Le SPVM n'était donc pas seul à épier les faits et gestes des journalistes du Québec. En 2013, la SQ a mis sous surveillance les téléphones cellulaires de Marie-Maude Denis, Alain Gravel et Isabelle Richer de Radio-Canada, du chef du bureau de La Presse à l'Assemblée nationale, Denis Lessard, du reporter spécialiste du crime organisé André Cédilot et d'Éric Thibault du Journal de Montréal.

Le corps de police tentait alors de faire la lumière sur une fuite d'information concernant l'enquête policière qui visait le président de la Fédération des travailleurs du Québec, Michel Arsenault. La SQ en a elle-même fait la révélation mercredi.

C'est le nouveau directeur général de la SQ, Martin Prud'homme, qui aurait réclamé des vérifications internes au cours des derniers jours, dans la foulée de l'" affaire Patrick Lagacé ". Le chef de police " est très préoccupé, très irrité. Il a demandé qu'une enquête soit confiée à un tiers indépendant et veut

s'assurer que les droits de toutes les personnes visées ont été respectés, a affirmé le porte-parole Guy Lapointe. C'était sous l'ancienne administration. Les règles sont fort différentes maintenant à la SQ. "

Le ministre de la Sécurité publique Martin Coiteux a annoncé la tenue d'une enquête administrative sur les pratiques de la Sûreté, en plus des promesses faites la veille pour tenter de rassurer les entreprises médiatiques et leur personnel. Mais la Fédération professionnelle des journalistes du Québec (FPJQ) en demande bien davantage. " Il faut plus qu'un comité de quelques personnes sans pouvoirs et qu'une modeste " inspection " de trois corps policiers pour espérer rétablir l'essentiel climat de confiance qui peut inciter les divulgateurs à parler à un journaliste, a estimé le conseil d'administration de la Fédération. Pour connaître l'ampleur de la surveillance des journalistes par les différents corps policiers ainsi que les liens entre la police et le pouvoir politique, puis déterminer les moyens de corriger les problèmes, il faut une enquête publique indépendante dotée des moyens nécessaires. " Québec s'y refuse toujours.

La Presse révélait en début de semaine que le chroniqueur Patrick Lagacé avait fait l'objet de surveillance policière étroite dans le cadre d'une enquête menée contre l'un de ses policiers. Pas moins de 24 mandats de surveillance du journaliste avaient été accordés par la juge de paix. D'autres médias avaient également révélé que Félix Séguin de TVA, Monic Néron du 98,5 FM, et Fabrice de Pierrebourg, anciennement de La Presse, avaient aussi été surveillés par le SPVM.

Visée par la SQ, la journaliste de Radio-Canada Isabelle Richer a vivement réagi mercredi. " Ce n'est plus que le SPVM, c'est la SQ, c'est une chasse généralisée aux sources journalistiques ", s'est-elle indignée.

Directeur de l'information du Journal de Montréal, George Kalogerakis, a dénoncé avec véhémence les actions posées par le SPVM et la SQ au cours des dernières années. " Les médias sont là pour s'assurer que nos institutions -- la police, la classe politique, le judiciaire -- aient des comptes à rendre à la population. De voir que la SQ nous ait espionnés pour des sujets aussi mineurs démontre à quel point ce corps de police comprend mal le fonctionnement de notre démocratie ", a-t-il déclaré en entrevue.

Le SPVM mis en demeure

Brian Myles, qui dirige Le Devoir, parle quant à lui de révélations " excessivement troublantes ". " On est en présence de dérives systématiques de la part de corps policiers. Il nous apparaît urgent de faire une enquête exhaustive et indépendante. "

Dans la foulée de cette affaire, La Presse a d'ailleurs mis en demeure le SPVM, exigeant qu'il cesse d'utiliser les registres téléphoniques et les données de localisations de Patrick Lagacé. " L'absence de précautions prises lors de la collecte de données [...] de M. Lagacé pour protéger les sources confidentielles de ce dernier est un scandale et une atteinte sans précédent à la liberté de presse ", écrit Sébastien Pierre-Roy, avocat du quotidien de la rue Saint-Laurent.

" Ces données n'ont jamais appartenu au SPVM et ne lui appartiennent toujours pas. " Simultanément, le quotidien présentait une requête afin de forcer le SPVM à remettre à la justice tous les exemplaires de ces documents afin qu'ils soient éventuellement détruits.

Dans toute cette affaire, les journalistes canadiens ont-ils été naïfs de croire qu'ils étaient à l'abri de telles invasions de leur vie professionnelle et privée ? " Lundi, je vous aurais dit que l'affaire Lagacé était probablement une première dans l'histoire du droit canadien. Je suis très déçu de constater que j'ai eu tort. Il semble y avoir une facilité à obtenir ce genre d'ordonnance et il est donc tout à fait possible qu'il y en ait plus ", a confié l'avocat de La Presse, Sébastien Pierre-Roy.

Pas de démission du chef de police

Malgré la tourmente dans laquelle il se trouve plongé depuis lundi, Denis Coderre continue d'appuyer le directeur SPVM, Philippe Pichet. " Jusqu'à preuve du contraire, il a ma confiance ", a indiqué le maire mercredi.

Pour lui, toutefois, la protection des sources journalistiques demeure primordiale : " On n'est pas contents. Moi-même, quand j'ai vu ça, j'ai pété ma coche. Je trouvais ça inacceptable. Mais maintenant, il faut être factuel. On ne fera pas de lynchage public et on va s'assurer que les choses se fassent adéquatement. "

Mardi, l'administration Coderre a mandaté la Commission de la sécurité publique afin qu'elle se penche sur les procédures et les critères suivis par le SPVM pour l'obtention de mandats judiciaires visant des journalistes lors d'enquêtes. Les élus pourront alors questionner Philippe Pichet sur les méthodes des enquêteurs. Les échanges se feront à huis clos, mais le rapport que rendra la commission d'ici le 31 janvier 2017 sera public, a rappelé le maire : " On a des questions à poser tout en s'assurant qu'on n'entache pas les enquêtes et qu'on ne crée pas plus de problèmes s'il y a des causes devant les tribunaux ", a-t-il dit.

Réactions à Ottawa

À Ottawa, le premier ministre Justin Trudeau s'est montré ouvert à la possibilité de revoir les lois pour protéger la liberté de presse. " On va regarder attentivement les conversations qui vont avoir lieu entre l'Hôtel de Ville de Montréal et [le SPVM], mais [...] comme on a dit plusieurs fois, ce gouvernement [se porte] à la défense de la liberté de la presse et on va faire ce qui est nécessaire pour l'encadrer, s'il y a d'autres étapes nécessaires. "

Fait inquiétant, ni la Gendarmerie royale du Canada ni le Service canadien du renseignement de sécurité (SCRS) n'ont voulu préciser si des journalistes avaient déjà été, ou se trouvent actuellement sous écoute électronique.

Consultez la mise en demeure de La Presse au SPVM :

Encadré(s) :

L'affaire en trois points

Maxime Bilodeau

Lundi 31 octobre 2016

On apprend que Patrick Lagacé, journaliste et chroniqueur de La Presse, a été surveillé pendant six mois par le Service de police de la ville de Montréal (SPVM).

Mardi 1er novembre 2016

Des médias révèlent que Félix Séguin de TVA, Monic Néron, du 98,5 FM, et Fabrice de Pierrebourg, anciennement de La Presse, ont également fait l'objet d'espionnage de la part du SPVM.

Mercredi 2 novembre 2016

La Sûreté du Québec (SQ) confirme qu'elle a épié les journalistes de l'émission "Enquête" Marie-Maude Denis et Isabelle Richer, l'animateur Alain Gravel de Radio- Canada, le chef du bureau de La Presse à Québec, Denis Lessard, André Cédilot et Éric Thibault du Journal de Montréal.

La Presse+

L'ordre politique

Thursday, 03 November 2016

Byline: Yves Boisvert

Section: column

Chronique - Cette histoire illustre à merveille toute la trop grande proximité entre notre police « nationale » et le gouvernement du Québec, quel que soit le parti au pouvoir.
Il y avait quelque chose de grotesque à entendre Stéphane Bergeron, hier, jurer qu'il n'avait pas « autorisé l'espionnage de journalistes ».

Évidemment qu'il n'a pas autorisé ça. Il a cependant passé une commande politique au grand patron de la Sûreté du Québec. Et il a créé les conditions pour ce dérapage.

Ce matin de septembre 2013, M. Bergeron, ministre de la Sécurité publique du gouvernement Marois, reçoit une lettre du président de la FTQ, Michel Arsenault. Arsenault est furieux : les médias révèlent depuis un certain temps qu'il a été la cible d'une enquête criminelle de la Sûreté du Québec de 2007 à 2009 sur l'infiltration du crime organisé dans la construction ; ils révèlent aussi que la SQ a avisé le gouvernement Charest de cette enquête « sensible » ; et un membre du gouvernement libéral a averti Arsenault qu'il faisait l'objet d'une enquête. L'enquête a avorté. (Tout ceci sera confirmé en novembre 2013 à la commission Charbonneau.)

Ce jour de septembre 2013, donc, Michel Arsenault est furieux que des détails de cette enquête aient été divulgués dans les médias. Au lieu de se plaindre à la SQ, il écrit au ministre Bergeron.

Hier, M. Bergeron a affirmé qu'il n'était pas vraiment intéressé par « les états d'âme » de M. Arsenault. Ce qui l'intriguait, c'était plutôt la fuite de l'enquête au gouvernement libéral.

Il appelle immédiatement le chef de la SQ, Mario Laprise. C'est M. Bergeron lui-même qui a nommé M. Laprise, en écartant son prédécesseur Richard Deschênes.

Et que fait M. Laprise ? Enquête-t-il sur la personne du gouvernement Charest qui a fait une indiscrétion à Michel Arsenault ? Indiscrétion qui a apparemment fait capoter l'enquête ? Non, il déclenche une enquête sur la fuite d'information... dans les médias.

Autrement dit, ce qui était grave, ce n'était pas l'interruption d'une enquête majeure parce que le gouvernement libéral en avait avisé Michel Arsenault (ça pourrait ressembler, au pire, à une entrave à la justice...). Non, ce qui était grave, c'est que les médias révèlent l'histoire. Manifestement, la SQ en avait déjà assez des fuites dans les médias. Mais si en plus le ministre appelle...

Dans un tel état d'urgence, les vannes étaient ouvertes. Il devenait acceptable qu'un policier aille jusqu'à obtenir les relevés téléphoniques de six journalistes.

Je suis convaincu que M. Bergeron ne s'attendait pas à ce qu'on espionne les journalistes. Mais qu'il appelle ça « une question », qu'il appelle ça une demande de reddition de comptes, à la fin, c'est un ordre politique qu'il a passé à « son » chef de la SQ. Et cet ordre était clair : comment ça se fait qu'il y a des fuites chez vous ? Explique-moi donc ça...

***

Quand les ordres viennent de haut, la pression est forte. Et quand la pression est forte, on prend tous les moyens à sa disposition. Ce qu'il fallait découvrir ici, c'était « la taupe », ou « les taupes » de la SQ. Et quel moyen plus simple que de cibler tous les journalistes qui ont pu toucher à cette histoire ?

En ayant accès aux données des relevés téléphoniques, on retracera bien la foutue taupe...

Évidemment, en passant la gratte dans les données téléphoniques, en les épluchant une à une, on ramasse plein d'autres sources... Peut-être des sources policières, peut- être toutes sortes d'autres sources.

***

Une enquête inspirée par le ministre lui-même est suivie de près par le patron de la SQ. On est obligé de présumer que Mario Laprise était bien au courant des méthodes utilisées dans cette enquête de haute importance politique. Et qu'il les approuvait.

Ce matin, donc, Stéphane Bergeron devrait cesser d'occuper la fonction de porte-parole en matière de sécurité publique. Il fait partie de cette invraisemblable histoire et tant qu'elle n'est pas éclaircie, il ne peut remplir utilement ses fonctions. Or, on a besoin d'une opposition qui fasse un travail efficace dans cette affaire d'espionnage ahurissante.

L'ancien chef de la SQ devra nous dire ce qu'il savait, quand il l'a su, et par qui sont passés les ordres.

Les libéraux n'ont pas de leçons à donner, bien entendu : une enquête a avorté à cause d'indiscrétions policières en haut lieu.

La Coalition avenir Québec parle du triangle amoureux PQ-FTQ-SQ. La vérité, c'est que cette histoire illustre à merveille toute la trop grande proximité entre notre police « nationale » et le gouvernement du Québec, quel que soit le parti au pouvoir.

C'est pourquoi l'affaire est encore plus grave que l'espionnage de Patrick Lagacé : elle commence par un coup de téléphone ministériel.

Mince consolation : cette fois, c'est le corps de police lui-même qui a révélé l'espionnage, pas un hasard judiciaire.

Encore une fois, on remarque qu'un juge de paix quelque part n'a rien trouvé à redire à la saisie de relevés téléphoniques de journalistes d'enquête...

C'est tout ça qu'il faut exposer dans une enquête indépendante. On croyait naïvement que « ces choses-là » n'arrivent qu'ailleurs. On dirait que l'heure est venue de rappeler à ceux qui nous gouvernent, à ceux qui font des enquêtes et à ceux qui les surveillent que la liberté de la presse, c'est plus qu'une ou deux lignes dans les chartes.

Illustration(s) :

PHOTO IVANOH DEMERS, ARCHIVES LA PRESSE

Stéphane Bergeron, ancien ministre péquiste de la Sécurité publique

PHOTO IVANOH DEMERS, ARCHIVES LA PRESSE

L'ancien ministre de la Sécurité publique Stéphane Bergeron a nié hier toute responsabilité dans l'espionnage de journalistes par la Sûreté du Québec. Il a soutenu n'avoir jamais été informé que les policiers utiliseraient ce recours.

New York Times

Why Light Bulbs May Be the Next Hacker Target (Canada)

Thursday, 03 November 2016

Byline: John Markoff

Section: general

San Francisco - The so-called Internet of Things, its proponents argue, offers many benefits: energy efficiency, technology so convenient it can anticipate what you want, even reduced congestion on the roads.
Now here's the bad news: Putting a bunch of wirelessly connected devices in one area could prove irresistible to hackers. And it could allow them to spread malicious code through the air, like a flu virus on an airplane.

Researchers report in a paper to be made public on Thursday that they have uncovered a flaw in a wireless technology that is often included in smart home devices like lights, switches, locks, thermostats and many of the components of the much-ballyhooed "smart home" of the future.

The researchers focused on the Philips Hue smart light bulb and found that the wireless flaw could allow hackers to take control of the light bulbs, according to researchers at the Weizmann Institute of Science near Tel Aviv and Dalhousie University in Halifax, Canada.

That may not sound like a big deal. But imagine thousands or even hundreds of thousands of internet-connected devices in close proximity. Malware created by hackers could be spread like a pathogen among the devices by compromising just one of them.

And they wouldn't have to have direct access to the devices to infect them: The researchers were able to spread infection in a network inside a building by driving a car 229 feet away.

Just two weeks ago, hackers briefly denied access to whole chunks of the internet by creating a flood of traffic that overwhelmed the servers of a New Hampshire company called Dyn, which helps manage key components of the internet.

Security experts say they believe the hackers found the horsepower necessary for their attack by taking control of a range of internet-connected devices, but the hackers did not use the method detailed in the report being made public Thursday. One Chinese wireless camera manufacturer said weak passwords on some of its products were partly to blame for the attack.

Though it was not the first time hackers used the Internet of Things to power an attack, the scale of the effort against Dyn was a revelation to people who didn't realize that having internet-connected things knitted into daily life would come with new risks.

"Even the best internet defense technologies would not stop such an attack," said Adi Shamir, a widely respected cryptographer who helped pioneer modern encryption methods and is one of the authors of the report.

The new risk comes from a little-known radio protocol called ZigBee. Created in the 1990s, ZigBee is a wireless standard widely used in home consumer devices. While it is supposed to be secure, it hasn't been held up to the scrutiny of other security methods used around the internet.

[Video: A small drone wirelessly delivers a computer worm in Beer Sheva, Israel, causing lights to flicker. Watch on YouTube.]

The researchers found that the ZigBee standard can be used to create a so-called computer worm to spread malicious software among internet-connected devices.

Computer worms, which can keep replicating from one device to another, get less attention these days, but in the early years of the commercial internet, they were a menace. In 1988, one worm by some estimates brought down a tenth of the computers connected to the internet.

Since then, the number of internet-connected devices has spiraled into the billions, and with it the risks of a cleverly created worm.

So what could hackers do with the compromised devices? For one, they could create programs that help in attacks like the one that hit Dyn. Or they could be a springboard to steal information, or just send spam.

They could also set an LED light into a strobe pattern that could trigger epileptic seizures or just make people very uncomfortable. It may sound far-fetched, but that possibility has already been proved by the researchers.

The color and brightness of the Philips Hue smart light bulb can be controlled from a computer or a smartphone. The researchers showed that by compromising a single light bulb, it was possible to infect a large number of nearby lights within minutes. The worm program carried a malicious payload to each light - - even if they were not part of the same private network.

In creating a model of the infection process, they simulated the distribution of the lights in Paris over an area of about 40 square miles and noted that the attack would potentially spread when as few as 15,000 devices were in place over that area.

The researcher said they had notified Philips of the potential vulnerability and the company had asked the researchers not to go public with the research paper until it had been corrected. Philips fixed the vulnerability in a patch issued on Oct. 4 and recommended that customers install it through a smartphone application. Still, it played down the significance of the problem.

"We have assessed the security impact as low given that specialist hardware, unpublished software and close proximity to Philips Hue lights are required to perform a theoretical attack," Beth Brenner, a Philips spokeswoman, said in an emailed statement.

To perfect their attack, the researchers said they needed to overcome two separate technical challenges. They first found a "major bug" in the way the wireless communications system for the lights had been executed, which made it possible to "yank" already installed lamps from their existing networks.

The researchers then used what cryptographers describe as a "side channel" attack to purloin the key that Philips uses to authenticate new software. The term side channel refers to the clever use of information about how a particular encryption scheme is used.

"We used only readily available equipment costing a few hundred dollars, and managed to find this key without seeing any actual updates," the researchers wrote. "This demonstrates once again how difficult it is to get security right even for a large company that uses standard cryptographic techniques to protect a major product."

NBC News

Election Cyberattacks: Pro-Russia Hackers Have Been Accused in Past

Thursday, 03 November 2016

Byline: Gabe Joselow

Section: general

London - While Americans are just coming to terms with the prospect of political cyberattacks tied to Russia -- it isn't the first time Kremlin- linked hackers have been accused of trying to influence voters in other countries.
A torrent of stolen emails released by WikiLeaks -- most damaging to the Democrats and Hillary Clinton -- have marked the 2016 race in what U.S. intelligence officials say is an unprecedented attempt to by Vladimir Putin's government to undermine trust in the U.S. election process.

"We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities," the Department of Homeland Security and the Office of the Director of National Intelligence said in an extraordinary gloves-off statement on Oct. 7.

Russia has been accused of this before, notably when hackers attempted to hijack an election in neighboring Ukraine in 2014.

A few days before the vote, a sophisticated cyberattack shut down Ukraine's Central Election Commission's computer systems by disrupting the internal network. A pro- Russian hacktivist group called CyberBerkut claimed responsibility for the attack.

CEC administrators were able to restore the system in time for the vote, but on election day the website was compromised again when a photo was posted falsely showing a far-right candidate had won the vote. Russian state television went on to broadcast an image allegedly taken from the site to report what turned out to be a false story.

It is not clear whether CyberBerkut was responsible for the false photo, or if other hackers were involved.

But according to a Ukrainian official investigating the incident who spoke to NBC News on condition of anonymity as the investigation into the incident is ongoing, additional malware was found on the election commission's system. This was traced back to the group APT28, also known as Fancy Bear which has been linked to the recent hacks in the U.S.

While the 2014 incident did not alter the outcome of Ukraine's elections, the hackers accomplished their goal, according to NATO cyberdefense ambassador Kenneth Geers.

He believes the hack was a Russian attempt to discredit the election and "muddy the waters."

"Maybe the goal was just to disrupt the process and its integrity or credibility," he told NBC News, adding that the timing of the attack was critical.

Ukraine was electing a new leader to succeed pro-Russian Viktor Yanukovych, who had been forced out of office by the Euromaidan street protests that erupted in Kyiv in late 2013.

Russia had already annexed the Crimea region from Ukraine and a Russian-backed separatist movement was waging an armed insurgency in the east. And the battle on the ground was also being fought online.

"Anytime you have a geopolitical conflict now you see its reflection in cyberspace," Geers said.

At the time Russia said it had no role in the hack, just as it has rejected accusations that it is trying to meddle in the American presidential race.

"We deny it completely," the Kremlin's top spokesman Dmitry Peskov told NBC News when asked whether his government supported hackers trying to influence the outcome of the U.S. election.

But Christopher Porter, an analyst with the cybersecurity firm FireEye, says the attacks in Ukraine and in the United States fit a pattern.

"Something we've seen in [the U.S.] election is a close tie between APT28 activities and social media and broadcast news outlets in Russia," he said. "As soon as they release a new leak or at the same time or beforehand they will have a news story all ready to go."

The U.S. documents stolen in the recent attacks were released through WikiLeaks and pushed out almost simultaneously on Russian news sites.

FireEye researchers have linked APT28 to Russia in part by showing that some of the source code was written in Russian and that malware was compiled during Russian working hours.

Malware associated with APT28 has also reportedly been found on the computers of German lawmakers earlier this year in what investigators describe as an espionage campaign, according to an IT security researcher who investigated the attack on behalf of a political party there.

APT28 also claimed responsibility on its website for leaking athletes' health records from the World Anti-Doping Agency database in an apparent attempt to discredit the organization after it recommended Russian athletes be banned from this year's Rio Olympics.

While breaches in the U.S. have been more embarrassing for the Democrats and Clinton, the intent of Russia's alleged meddling was not to favor a particular candidate but to "undermine democracy in some vague way" and "sow discord," Porter said.

Donald Trump and his supporters have repeatedly claimed the election is rigged while pointing to documents published by WikiLeaks. This may be just the kind of "discord" the attackers had planned.

And there may be more to come.

U.S. intelligence officials are concerned that attackers with ties to Russia could try to post falsified documents to try to undermine confidence in the result and to stir fears of voter fraud.

U.S. officials already sent warnings to Illinois and Arizona in August after reports that hackers had infiltrated voter registration rolls in those two states, though it was unclear what, if any, information was obtained or altered.

A huge amount of data about U.S. voters is already being offered for sale online, experts warn.

"We saw 190 million national records for sale in October 2015 for $20,000," said Porter, the cybersecurity analyst.

The voter information appears to be a combination of public data that was easily acquired to other records that were more likely illegally obtained, according to Porter. It is not clear how attackers could use this information.

While senior U.S. officials maintain the Russian state is behind the slew of cyberattacks in the U.S., a leading Moscow-based cybersecurity expert said he doubted that the Kremlin was really responsible for the latest spate of hacks.

Oleg Demidov, a cybersecurity consultant with Moscow-based policy center PIR, told NBC News that he had not seen hard proof of Russian state involvement.

Concerning the possibility these hacked databases could be used to damage an election campaign he said: "I do not see it."

U.S. officials also have said it would be extremely difficult for anyone -- including state-backed hackers -- to alter the actual ballot count in the U.S. election, or to get into the actual voting machines.

Still, FireEye's Porter warned Russian hacking groups have shown they have firepower beyond just hacking databases and websites. He noted as an example the unprecedented cyberattack on a Ukrainian power distributor just before Christmas last year that temporarily knocked out electricity to 230,000 people.

"The Russian government-backed ... groups are limited by their will, not by technology," Porter says. "They can do a lot more damage than they've currently done."

USA Today

Microsoft to block Windows flaw used by Russian hackers

Thursday, 03 November 2016

Byline: Brett Molina

Section: general

Washington - Microsoft says it will release a patch next week to address vulnerabilities in its Windows operating system exploited by a group reportedly tied to the Russian government and linked to the theft of emails from the Democratic National Committee.
The group, called Strontium by Microsoft but Fancy Bear or APT 28 by other security researchers, has been tied to Russian state- sponsored hacking. U.S. intelligence agencies have said Russian groups were behind attempts to interfere with this year's U.S. presidential election.

Strontium has targeted "government agencies, diplomatic institutions, and military organizations, as well as affiliated private sector organizations such as defense contractors and public policy research institutes," Microsoft's executive vice president of Windows and devices group Terry Myerson said in a blog post Wednesday.

Myerson did not directly link Strontium to Russia, only that it has been used "to target a specific set of customers."

But according to CrowdStrike, an Irvine, Calif.-based computer security firm that published a detailed analysis of the attack on the DNC intrusion in June, Strontium is simply another name for the group CrowdStrike called Fancy Bear, a Russian intelligence- affiliated adversary.

The exploits used by Strontium involve versions of Windows going back to Vista as well as Adobe's Flash, according to Myserson. Microsoft says the group launched a campaign involving spear phishing, where users receive a malicious email disguised as a message from a friendly individual or business. If successful, hackers could gain access to a victim's computer. A patch is expected by Nov. 8.

The patch doesn't mean Strontium no longer will be able to launch attacks, merely that it will need to find new vulnerabilities. FancyBear/Strontium has a history of using so- called "zero day vulnerabilities." That means security holes in software that are unknown and therefore have not been patched, ones companies do not realize they must protect against.

The exploits were first discovered by Google's Threat Analysis Group, and shared publicly Monday.

La Presse+

Surveillance de journalistes : mutisme à la GRC et au SCRS

Wednesday, 02 November 2016

Byline: Vincent Brousseau-Pouliot

Section: general

Ottawa - Alors que la SQ et la Ville de Montréal ont confirmé avoir mis des journalistes sous surveillance, la GRC et le Service canadien du renseignement de sécurité (SCRS), les deux corps policiers fédéraux, ne veulent pas confirmer s'ils ont déjà adopté de telles pratiques, et le cas échéant à quelle fréquence. La GRC précise seulement que «les cas où des enquêtes de la GRC concernant des journalistes ont eu lieu sont extrêmement rares».
Le commissaire de la GRC Bob Paulson a dit mercredi «ne pas être au courant que nous avons des enquêtes actives ou de la surveillance à l'égard de journalistes», mais la GRC n'a pas voulu confirmer si des journalistes ont été surveillés dans le cadre de ses enquêtes. Un cas de filature avait été rendu public il y a un an, celui du journaliste de La Presse Joël-Denis Bellavance qui a été pris en filature en 2007.

Tout en précisant «reconnaître» et «respecter [...] l'importance de la liberté et de l'indépendance de la presse», la Gendarmerie royale du Canada (GRC) a indiqué ne pas pouvoir commenter «l'existence d'enquêtes en cours» ou «discuter des détails opérationnels» d'enquêtes passées. La GRC n'a pas précisé à La Presse si elle effectuait, comme l'a fait la Sûreté du Québec cette semaine, un examen de ses enquêtes pour déterminer si des journalistes ont été mis sous surveillance. La SQ a dévoilé aujourd'hui que six journalistes au Québec, dont Alain Gravel (Radio-Canada), Marie-Maude Denis (Radio-Canada), Isabelle Richer (Radio-Canada), Denis Lessard (La Presse) et Éric Thibault (Journal de Montréal).

Le Service canadien de renseignement de sécurité (SCRS) n'a pas répondu aux questions de La Presse à savoir si l'organisme fédéral responsable des enquêtes de sécurité nationale : 1) surveille actuellement des journalistes, 2) en a surveillé par le passé, 3) mène actuellement des démarches pour répondre à ces questions et a l'intention de rendre public le résultat de ces démarches.

De son côté, le gouvernement Trudeau n'a pas l'intention de demander à la GRC et au SCRS de divulguer de telles informations, estimant qu'il n'était «pas approprié de commenter sur les questions opérationnelles».

«Bob Paulson, commissaire de la GRC, a confirmé qu'aucun journaliste ne fait actuellement l'objet d'une surveillance par la GRC. Le ministre Goodale examine la Directive ministérielle sur les enquêtes dans les secteurs sensibles existante afin de s'assurer que les plus grands soins sont pris lorsque des enquêtes criminelles et du journalisme se recoupent et que la valeur canadienne fondamentale de la liberté de presse est protégée. Il est toujours ouvert à recevoir des représentations sur ce qu'il y a d'autre à faire pour protéger les libertés fondamentales de la presse», indique Scott Bardsley, attaché de presse du ministre fédéral de la Sécurité publique Ralph Goodale.

Le NPD demande une enquête publique sur la question de la surveillance des journalistes par les corps policiers. Les néo-démocrates sont «préoccupés» par le fait que la GRC et le SCRS ne veulent pas préciser s'ils ont mis des journalistes sous surveillance. «En ne répondant pas, ça affecte la confiance du public, dit le député Matthew Dubé. La réponse de la SQ de dévoiler [ces informations] démontre que le public a besoin d'être rassuré. Ce sont des questions auxquels ils doivent répondre. On continue de demander une enquête publique qui nous permettrait de constater les faits: est-ce une pratique répandue ou arbitraire?»

Après avoir vu les cas au SPVM et à la SQ, le chef par intérim du Bloc québécois Rhéal Fortin dit qu'il «ne tomberait pas en bas de ma chaise» s'il apprenait que des journalistes ont été surveillés par les corps policiers fédéraux. «Nous n'avons pas d'informations à cet effet-là, précise-t-il. Comme n'importe qui, je vois que si la SQ et le SVPM le font, je ne tomberais pas en bas de ma chaise [pour les corps policiers fédéraux]. Le ministre Goodale doit demander des comptes aux services policiers sous sa juridiction et rendre des comptes en Chambre aussi. Tout ça va peut-être nous permettre de découvrir qui est surveillé, mais ça ne règle pas le problème, ce qui rend encore plus pertinent et urgent que jamais notre projet de loi [sur la protection des sources journalistiques].»

Le Parti conservateur du Canada aimerait que le ministre Goodale fasse un examen de la situation et vienne en faire rapport en comité parlementaire.

L'Humanité

60 millions de fichés, émoi, émoi, émoi...

Thursday, 03 November 2016

Byline: Alexandre Fache

Section: general

Paris - La mise en place par décret, dimanche, d'un fichier compilant les données personnelles d'une grande partie des Français inquiète élus et associations. D'autant que la mesure n'a fait l'objet d'aucun débat public.

Ce n'est sans doute pas l'ensemble de nos libertés que le gouvernement a enterré dimanche, au coeur du week-end de la Toussaint. Mais la discrétion supposée que devait offrir au nouveau fichier TES (pour « titres électroniques sécurisés ») un simple décret paru le 30 octobre au Journal officiel peut à elle seule faire craindre le pire. De fait, aucun débat parlementaire, ni même aucune délibération citoyenne n'aura accompagné la création d'un gigantesque outil de recueil des données personnelles des quelque 60 millions de Français, ceux en tout cas qui ont un jour possédé un passeport ou une carte d'identité. Mis en place dans un souci de « simplification administrative », ce nouveau fichier TES, dont l'existence a été révélée par le site Next INpact lundi, réunit en effet dans une seule et même base les données relatives à l'ensemble de nos concitoyens âgés de 12 ans et plus : nom de famille, nom d'usage et prénoms, date et lieu de naissance, sexe, couleur des yeux, taille, domicile, noms, prénoms, date et lieu de naissance des parents, leur nationalité, ainsi qu'une adresse mail si celle-ci a été renseignée, ou encore une photographie, jusqu'aux empreintes digitales, prélevées depuis 2008 aux heureux possesseurs de passeports biométriques... En un mot comme en cent, « un monstre », selon la formule du député PS et membre de la Commission nationale de l'informatique et des libertés (Cnil), Gaëtan Gorce, qui a dit cette semaine toute son inquiétude quant à l'utilisation qui pourrait être faite d'un tel outil.

La crainte de modifier les finalités d'un tel fichier

Des inquiétudes qui ne datent pas de ce mois de novembre. En 2012, alors que la majorité de droite vivait ses dernières heures, une proposition de loi avait été adoptée, créant le même fichier géant, qualifié alors par le député UMP Christian Vanneste de « fichier des honnêtes gens », ceux qu'il fallait « protéger ». L'objectif était double : lutter contre l'usurpation d'identité d'une part, et permettre, d'autre part, l'identification d'une personne à partir de ses données biométriques, notamment à des fins judiciaires. Un deuxième point qui avait entraîné la censure de ce texte par le Conseil constitutionnel, saisi par des parlementaires socialistes, parmi lesquels Jean-Jacques Urvoas, devenu aujourd'hui ministre de la Justice...

Le gouvernement se défend d'avoir effectué un copier-coller du texte de 2012. « Le décret qui vient d'être pris ne comporte aucune fonctionnalité d'identification d'une personne à partir de ses seules données biométriques », fait ainsi valoir le ministère de l'Intérieur, assurant qu'il ne peut donc « être comparé à la proposition qui avait été censurée » il y quatre ans. Voire. « La finalité d'identification à partir des données a certes été écartée, mais dès lors que le fichier a été constitué, elle devient techniquement possible, s'inquiète Gaëtan Gorce. On peut craindre qu'un futur gouvernement ne modifie les finalités d'un tel fichier. » Un gouvernement de droite ou d'extrême droite, par exemple, qui voudrait durcir la législation au lendemain d'un nouvel attentat terroriste...

Des préoccupations partagées par la Ligue des droits de l'homme

Des préoccupations partagées par la Ligue des droits de l'homme et son président d'honneur Michel Tubiana. « Aujourd'hui, on n'a pas le droit de faire de tri dans ce fichier, suite à l'invalidation du texte de 2012 par le Conseil constitutionnel. Mais qui dit que demain ce dernier ne changera pas de position, dans un contexte différent ? » Pour l'avocat, le gouvernement aurait dû se ranger derrière l'avis de la Cnil, qui plaidait pour la mise en place d'un système de puce électronique dans la carte d'identité, permettant de « conserver les données biométriques sur un support individuel exclusivement détenu par la personne concernée ». « Là, on crée un fichier géant de 60 millions de personnes, inquiétant par nature, regrette Michel Tubiana, et ce d'autant plus qu'il va être consultable par pas moins de onze services de l'État, et même plus si la justice le demande. C'est énorme, et cela multiplie les risques de fuites ou de piratages. Sans régler par ailleurs le réel problème des usurpations d'identité, bien au contraire ! »

Stoïque malgré les critiques, Bernard Cazeneuve a rappelé, hier, à l'Assemblée, que ce nouveau fichier avait été « validé par le Conseil d'État et la Cnil ». Reste à demander leur avis aux 60 millions de fichés.

London Times

Hackers leak Putin plan to carve up Ukraine

Thursday, 03 November 2016

Byline: Maxim Tucker

Section: general

Kyiv - Leaked Kremlin emails reveal how Russian operatives botched an attempt last year to foment an uprising in Kharkiv, the second largest city in Ukraine.
The emails, obtained by The Times, were apparently hacked from the inbox of Maria Vinogradova, an adviser to Vladislav Surkov, President Putin's point man on Ukraine. The civilian intelligence analysis group Inform Napalm said that it had traced the adviser to an office in central Moscow used by the FSB spy agency.

Three of the Ukrainian hackers involved in the leak met The Times on condition of anonymity, carrying concealed weapons but rejecting suggesern tions that the hack had been carried out with the help of Ukrainian or US intelligence services. Last month NBC News reported that the CIA had vowed to retaliate against Russia for a series of intrusions targeting American political institutions.

The inbox that they shared contains 423 emails between government officials and separatist leaders between 2014 and 2016. Highlights include a proposal from a rebel leader to split Ukraine into three

parts under a federalised system, plans to replace unruly separatist officials who were then killed or arrested, and draft Ukrainian laws to be submitted by a pro-Russian party.

The presidential office was also sent emails asking for approval of a screenplay and a poem about the war in easting Ukraine. The email trove includes two maps sent in January this year by Denis Pushilin, a rebel leader who reports regularly to Mr Surkov, and suggests that Ukraine could be carved into three parts: an eastern third known as "New Russia", a central region, includ-Kiev, to be known as "Lesser Russia" and a smaller western area to take the historic name "Galicia".

An email sent in April last year to Mr Surkov from Mikhail Markelov, chairman of Russia's parliamentary committee for public associations, sets out a plan for stoking unrest in Kharkiv by creating a pro-Russian "resistance group" called the Civil Initiative.

"CI will develop and implement actions to mobilise protests, encourage criticism of Kiev policy, and promote ideas of regional 'autonomy'," the message reads.

By June, however, the committee chairman was reporting that the plan had run into problems. An email with the subject header "Problems and Mood" laments that the project "Kharkiv, rise up!" had not brought Ukrainians in the city on to the streets.

In the email Mr Markelov explains that Kharkiv had ignored the group's false warnings of "bloody attacks" on Russian speakers by Ukrainian nationalists. He also relays concerns that Ukrainian intelligence services had infiltrated the pro-Russian organisation. "So, instead of uniting and producing work aimed at the desired result, there is a 'debriefing' and 'a search for the traitors'," the parliamentarian writes.

In a third email two weeks later Mr Markelov appears to have abandoned hopes of an uprising, writing that many of the "resistance fighters" have been arrested or fled to Moscow or the breakaway Donetsk People's Republic.

Le Figaro avec Reuters

Montréal: des journalistes sur écoute

Thursday, 03 November 2016

Byline: Journaliste maison

Section: general

Montréal - Les téléphones mobiles de six journalistes québécois ont été surveillés en 2013, a rapporté mercredi Radio-Canada, deux jours après que le journal La Presse a révélé que l'un de ses chroniqueurs vedettes avait été espionné par la police de Montréal. Selon la radio, la Sûreté du Québec (SQ), la police provinciale, a obtenu des mandats lui permettant d'obtenir le registre des appels entrants et sortants des six journalistes mais n'a pas enregistré leurs conversations.
Guy Lapointe, porte-parole de la SQ, a expliqué mercredi soir à la radio 98,5 Montréal que la police avait cherché à déterminer l'origine de fuites ayant permis la divulgation dans la presse du contenu d'écoutes téléphoniques. Selon la presse canadienne ces fuites concernaient une affaire de fabrication de preuves par des policiers.

C'est dans le cadre de cette même enquête qu'un chroniqueur du journal La Presse, Patrick Lagacé, a été surveillé par la police de Montréal. Le premier ministre québécois Philippe Couillard a promis mardi de réformer la législation afin de mieux protéger la liberté de la presse au Québec après ces révélations.

Reuters

John Brennan's attempt to lead the CIA into the age of cyberwar

Wednesday, 02 November 2016

Byline: David Rhode

Section: general

Washington - When America goes to the polls on Nov. 8, according to current and former U.S. intelligence officials, it will likely experience the culmination of a new form of information war.
A months-long campaign backed by the Russian government to undermine the credibility of the U.S. presidential election - through hacking, cyber attacks and disinformation campaigns - is likely to peak on voting day, the officials said.

Russian officials deny any such effort. But current and former U.S. officials warn that hackers could post fictional evidence online of widespread voter fraud, slow the Internet to a crawl through cyber attacks and release a final tranche of hacked emails, including some that could be doctored.

"Don't underestimate what they can do or will do. We have to be prepared," said Leon Panetta, who served as CIA director and defense secretary in President Barack Obama's first term. "In some ways, they are succeeding at disrupting our process. Until they pay a price, they will keep doing it."

John Brennan, the current CIA director, declined to comment on the Russian efforts. But he said Russian intelligence operatives have a long history of marrying traditional espionage with advances in technology. More broadly, Brennan said, the digital age creates enormous opportunities for espionage. But it also creates vulnerabilities.

Citing an array of new cyber, conventional and terrorist threats, Brennan announced the most sweeping reforms of the CIA in its 69-year history 18 months ago.

Weakening the role of the Directorate of Operations, the agency's long-dominant arm responsible for gathering intelligence and conducting covert operations, Brennan created 10 new "mission centers" where CIA spies, analysts and hackers work together in teams focused on specific regions and issues. He also created a new Directorate for Digital Innovation to maximize the agency's use of technology, data analytics and online spying.

The information age "has totally transformed the way we are able to operate and need to operate," Brennan told Reuters in a series of interviews. "Most human interactions take place in that digital domain. So the intelligence profession needs to flourish in that domain. It cannot avoid it."

When a new American diplomat arrives for duty at the U.S. embassy in Moscow or Beijing, CIA official say, Russian and Chinese intelligence operatives run data analytics programs that check the "digital dust" associated with his or her name. If the newcomer's footprint in that dust - social media posts, cell phone calls, debit card payments - is too small, the "diplomat" is flagged as an undercover CIA officer.

The Russian-backed campaign to discredit the U.S. election is not isolated. Hackers believed to have links to Chinese intelligence began stealing the personal information of 22 million federal employees and job applicants in 2014, the worst known data breach in U.S. government history. Islamic State's online propagandists continue to inspire lone wolf attacks in the United States even as the group loses territory.

A senior official from the Directorate of Operations, who backs the shake-up, said the agency is experiencing its greatest test in decades.

THE DIGITAL DEBATE

"The amount of threats and challenges that are facing this organization and this nation are greater than at any time in the last 30 years," said the official, who declined to be named. "The days of a black passport, a fistful of dollars and a Browning pistol are over."

James Clapper, the Director of National Intelligence, praised Brennan and his efforts to retool the CIA for a new era in an interview. So did Lisa Monaco, Brennan's successor as the President Obama's Homeland Security and Counterterrorism adviser.

But some current and former officials question Brennan's strategy, arguing his reforms are too digitally focused and will create a more cautious, top-heavy spy agency. At a time when the agency needs to refocus its efforts on human espionage, they say, the concentration of power in the new mission centers weakens the ability of the Directorate of Operations to produce a new generation of elite American spies.

The reforms have hurt morale, created confusion and consumed time and attention at a time of myriad threats, according to interviews with ten former officials.

Glenn Carle, a former CIA covert officer, supports Brennan and his reforms but said they have sparked a mixed reaction among directorate of operations officials who believe human intelligence is getting short shrift.

"The value the CIA can fundamentally add is to steal secrets, and the ultimate secret is intention," the often inscrutable aims of foreign leaders, Carle said. "Obtaining that is a human endeavor."

At the same time, Brennan has stirred a different sort of criticism - that he has defied Congressional oversight. Liberal Democrats and libertarian Republicans in Congress say the Brennan- Obama tenure has been tarnished by a lack of transparency with congressional oversight committees and the public regarding surveillance, drone strikes and the agency's use of torture against terrorism suspects during the administration of George W. Bush.

"While I think John's overall legacy will be as a reformer, that legacy will suffer from his refusal to come to grips with the CIA's troubled torture program," said Senator Dianne Feinstein, D- Calif, vice chair of the Senate's intelligence committee. "I think the new president's CIA director must prioritize a high level of trust between the CIA and Congress to insure proper oversight is conducted."

It's unclear how closely the country's next president will hew to Brennan's strategy.

The front-runner, Democrat Hillary Clinton, has an incentive to beef up American cyber-espionage: U.S. intelligence officials blame the continuing leak of emails from her campaign on Russian-backed hacking. Clinton also expressed support for covert action in a transcript of a 2013 speech she gave to Goldman Sachs that was recently released by Wikileaks.

Republican Donald Trump, meanwhile, pledged to make cybersecurity a top priority in his administration in an October 3 speech. "For non-state terror actors, the United States must develop the ability - no matter how difficult - to track down and incapacitate those responsible and do it rapidly," Trump said. "We should turn cyber warfare into one of our greatest weapons against the terrorists."

In interviews at agency headquarters in Langley, Virginia, Brennan declined to comment on either candidate or discuss operational details of the CIA. But he and eight other senior CIA officials gave the

most detailed description yet of their rationale for the most radical revamp of the agency since its founding in 1947.

"I look out at the next 10, 20, 30 years, and I look at technology, I look at complexity, I look at the global environment," Brennan said. "I think CIA really needs to up its game."

JUST-WAR THEORIST

Brennan, a 61-year-old native of north New Jersey, looks like a linebacker but talks like a technocrat. He speaks excitedly about how the CIA and other government bureaucracies can be configured in "a way to ensure optimal outcomes."

The son of devout- Catholic Irish immigrants, Brennan speaks reverently of CIA officers as public servants who risk their lives without public accolades. He joined the agency in 1980, at the age of 24, after receiving a Master's Degree in government with a concentration in Middle Eastern studies from the University of Texas.

Educated in various Catholic schools, including Fordham University, Brennan says he is an adherent of just-war theory - a centuries-old Christian theological argument that war is justified when it is waged in self defense, as a last resort and minimizes civilian casualties. Those beliefs, he says, have guided him in one of the most controversial aspects of his tenure in the Obama administration.

As Obama's White House counter-terrorism adviser and CIA director, Brennan played a central role in carrying out 473 U.S. airstrikes outside conventional war zones between 2009 and 2015, primarily by drone. U.S. officials estimate the attacks have killed 2,372 to 2,581 people, including 64 to 116 civilians.

Human rights groups say the totals are vastly higher. Last year, for instance, a U.S. drone strike in Pakistan accidentally killed American aid worker Warren Weinstein and Italian aid worker Giovanni Lo Porto, who were both being held captive by al Qaeda.

Brennan declined to comment on specific strikes, but said, "I still can look myself in the mirror everyday and believe that I have tried to do what is morally right, what is necessary, and what is important to keep this country safe." He also acknowledged mistakes.

"You question yourself. You beat yourself up. You try to learn from it," Brennan said, in a rare display of emotions. "But you also recognize that if you're not prepared to make the tough decisions in the jobs that have been entrusted to you, you shouldn't be in those jobs."

Today, Brennan says the United States faces the most complex array of threats he has seen since joining the agency 36 years ago. As a CIA analyst, operative and executive, he has lived through the Cold War espionage duels of the 1980s; the disintegration of nation-states after the 1989 fall of the Berlin Wall;

the rise of non-state terrorist groups since 2001; and the current digital disruption. Now, he says, all four dynamics are converging at once.

BOLD AND INNOVATIVE RIVALS

CIA officials say their greatest state competitors are the Russian and Chinese intelligence services. While smaller countries or terrorist groups may want to strike at the United States, Russia and China are the only two adversaries with the combination of skills, resources and motivation needed to challenge Washington.

In recent years, Moscow's Federal Security Service, or FSB, has become adept at waging "gray zone" conflicts in Ukraine, Crimea and Syria, the officials said. In all three countries, Russian intelligence operatives have deftly shrouded protagonists, objectives and war crimes in ambiguity.

One target is America's increasingly politically polarized democracy. As Russian-backed hacking unfolded this summer, the Obama White House's response fueled frustration among law enforcement and intelligence officials, according to current and former officials. The administration, they said, seemed to have no clear policy for how to respond to a new form of information warfare with no rules, norms or, it seemed, limits.

White House officials said the administration is still considering various methods of responding, but the responses won't necessarily be made public.

China presents another challenge. Chinese businessmen and students continue trying to scoop up American state and economic secrets. In one bright spot, Beijing appears to be abiding by a 2015 pact signed by Obama and Chinese leader Xi Jinping that the two governments would not conduct economic espionage against one another. Chinese hacking appears to have slowed from the voracious rate of the past, which included hacking into the computers of the 2008 presidential campaigns of John McCain and Barack Obama but not releasing what was found.

"The question is whether or not it is due to greater care in terms of covering one's tracks," Brennan said of the apparent change. "Or whether or not they realize that they're brand is being tarnished by this very rapacious appetite for vacuuming up things."

Regional powers are also increasing their digital espionage efforts.

In 2014, the Obama administration blamed North Korea for the hacking of Sony Pictures' computer system. This spring, U.S. prosecutors indicted seven Iranian hackers for allegedly trying to shut down a New York dam and conducting a cyber attack on dozens of U.S. banks. They also indicted three Syrian members of the "Syrian Electronic Army," a pro-Syrian government group, who hacked into the websites of U.S. government agencies, corporations and news organizations.

In a 2015 case that U.S. officials said marks a worrying new trend, federal prosecutors indicted a 20-year-old hacker from Kosovo. With the help of a criminal hacker, Ardit Ferizi stole the home addresses of 1,300 members of the U.S. military, providing the information to Islamic State and posting it online, and calling for attacks on the individuals. Ferizi was arrested in Malaysia, where he was studying computer science. In September, he pleaded guilty in a U.S. federal court and was sentenced to 20 years in prison.

"This blend of the criminal actor, the nation-state actor and the terrorist actor, that's going to be the trend over the next five years," said John Carlin, who recently stepped down as head of the Justice Department division that monitors foreign espionage in the United States.

But some active clandestine officers argue that the intelligence community has grown too reliant on technology, a trend they trace back four decades to the directorship of Stansfield Turner. Satellite photography, remote sensors and communications intercepts have become more sophisticated, but so have encryption techniques and anti-satellite weapons.

More important, they argue, is that technology is no substitute for "penetrations" - planting or recruiting human spies in foreign halls of power. The CIA missed India's 1998 nuclear tests and misjudged Saddam Hussein's arsenal in 2003 because it lacked spies in the right places.

Today, these current and former CIA officials contend, American policymakers have little insight into the thinking of Vladimir Putin's inner circle. Presidents, kings and dictators often don't share their true intentions electronically, putting this valuable information largely beyond the scope of digital spying. The best sources are still people, and these officials believe the agency is not mounting the kind of bold human spying operations it did in the past.

Brennan and other CIA officials flatly denied downplaying human intelligence. They said aggressive, high-risk human spying is under way but they cannot go into operational detail.

One of Brennan's predecessors, Michael Hayden, former CIA chief under President George W. Bush, says the agency strayed from its core mission during the Bush years. After the Al Qaeda attacks of Sept. 11, 2001, Hayden said, the CIA had shift to become a paramilitary organization that devoted its most talented officers to tracking and killing terrorists. It now needs to reverse that trend by focusing on espionage against rival nations, he said.

"The constant combat of the last 15 years has pushed the expertise of the case officer in the direction of the battlefield and in the direction of collecting intelligence to create physical effects," said Hayden, using an intelligence euphemism for killing. "At the expense of what the old guys called long-range, country-on-country intelligence gathering."

'OPTIMIZING CAPABILITIES'

Brennan and the eight other senior CIA officials made the case that their modernization effort will address the needs and threats described by Hayden and others. Technological advances, they said, have leveled the intelligence playing field. The web's low cost of entry, creativity and speed benefits governments, hackers and terrorists alike.

A veteran covert operative who runs a new CIA mission center compared Brennan's reforms to the Goldwater-Nichols Act. The landmark 1986 legislation reorganized the U.S. military into a half dozen regional commands where the Army, Navy, Air Force and Marines work together. It was a response to inter-service rivalries that bedeviled the American military in Vietnam.

The CIA equivalent involves having the agency's five main directorates - Operations (covert spies), Analysis (trends and prediction), Science and Technology (listening devices and other gadgetry) and Digital Innovation (online sleuthing) and Support (logistics) - provide the personnel needed by each regional mission center.

Andrew Hallman, director of the new Directorate for Digital Innovation, said the CIA has embraced cloud computing as a way to better share intelligence. In a move that shocked insiders and outsiders, the CIA awarded an $600 million contract to Amazon in 2013 to build a secure cloud computing system where multiple CIA databases can be quickly accessed.

For decades, different directorates maintained their own separate databases as a security measure, said Hallman. Some of the applications the agency used were so old - up to 30 years - that the manufacturer was no longer in business.

Turning to Amazon was designed to immediately put private-sector computing advances at the fingertips of CIA operatives. It was also an admission that it was easier for the agency to buy innovation from the private sector than try to create it internally.

Several former CIA officials criticized the new team-focused system, saying it dilutes the cultures that made each agency directorate strong. The best analysts are deeply skeptical and need to be separated from covert operatives to avoid group-think, they said. And the best covert operatives are famously arrogant, a trait needed to carry out the extraordinarily difficult task of convincing foreigners to spy for America.

Richard Blee, a former CIA clandestine officer, said the agency needed reform but highlighted a separate problem created by technological change. Instant secure communications between CIA headquarters and officers in the field has centralized decision-making in Washington, Blee said. And regardless of administration, senior officials in Washington are less willing to take a risk than field officers - virtually all of whom complain about headquarters' excessive caution.

"The mentality across the board in Washington is to take the lowest common denominator, the easiest option, the risk-free option," Blee said. "The Chinese are taking tough decisions, the Russians are taking

tough decisions and we are taking risk-averse decisions. And we are going to pay a price for that down the road."

Brennan says his reforms will empower CIA officers: The integrated teams in each new mission center will improve speed, adaptability and effectiveness.

"To me, that's going to be the secret of success in the future, not just for CIA but for other organizational structures," Brennan said. "Taking full advantage of the tools, capabilities, people and expertise that you have."

The old ways of spycraft, Brennan argues, are no longer tenable. Asked what worries him most, he gave a technocratic answer: Twentieth century American government management practices are being rendered obsolete in the digital age.

"U.S. decision making processes need to be streamlined and accelerated," he said. "Because the problems are not going to wait for traditional discussions."

Globe and Mail
In scathing ruling, Federal Court says CSIS bulk data collection illegal
Friday, 04 November 2016
Byline: Colin Freeze

Ottawa - The Federal Court of Canada faulted Canada's domestic spy agency Thursday for unlawfully amassing data, for misusing its surveillance warrants and for not being forthright with judges who authorize its intelligence programs. The court is also revealing that CSIS no longer needs warrants to collect Canadians' tax records because of changes wrought by Bill C-51.
The matter was said to involve the decade-long collection of volumes of data within the Canadian Security Intelligence Service's little- known Operational Data Analysis Centre, which the judges who scrutinize CSIS are characterizing as a hidden and unlawful repository of data amassed by the spy agency.

The centre and the data within it are so secret that the Federal Court - which authorizes CSIS wiretapping bids - had no idea they existed.

"The Court had never before been fully informed of the existence of the program. The Court, during the hearings, learned that the program had been in existence since 2006 yet it had never heard nor seen any evidence on the matter," reads a partly redacted new ruling from Federal Court Judge Simon Noël.

These judges took the rare step of meeting collectively several times in 2016 to grill CSIS officials about their wiretap warrants and whether the service was being forthright enough in making them.

This is a scathing ruling on several levels. It is basically the second time in three years that senior Federal Court judges who approve CSIS programs have publicly said they cannot keep tabs on what the spy agency is doing because its intelligence officers are breaching their "duty of candour" with the court. The judges further reveal that controversial 2015 Conservative legislation, Bill C-51's Security of Canada Information Sharing Act, eased information flow between government departments to the point that "CSIS no longer needs a warrant to obtain information from the Canada Revenue Agency."

Public Safety Minister Ralph Goodale is currently consulting with Canadians on whether he needs to change the laws under which CSIS operates. He is also pitching Parliament on a new committee of MPs who could be given powers to investigate intelligence agencies.

CSIS exists to advise the Prime Minister about threats to national security. It can potentially collect much greater amounts of data, about more people and more entities, than any police agency can, given it works under lower legal thresholds of intelligence investigations that are never intended to be discussed publicly. Its relationships with Canadian telecommunications companies and other Canadian government departments have always been murky.

Elsewhere, however, spy agencies are also falling under fire for collecting data in bulk quantities, and for gathering information about everyone in hopes of deducing patterns that speak to where terrorists could be. For example, the U.S. and British counterparts of CSIS have lately been faulted by their own watchdog agencies for indiscriminately amassing material relating to citizens' phone logs, taxation records and passports, in hopes that such records might be useful to intelligence analysts.

The Federal Court of Canada documents released Thursday say CSIS has been unlawfully amassing "associated data" - a term that appears to refer to telecommunications metadata such as phone logs and e-mail trails. Under its foundational legislation passed in 1984, CSIS is entitled to collect only information that is "strictly necessary" to collect, but Federal Court judges who sign off on warrants now say the spy agency is not living up to this law.

"CSIS had an obligation, beginning in 2006, to fully inform the Court of the existence of its collection and retention of associated data program. The CSIS also had the duty to accurately describe this program to the Court," reads the Federal Court statement. It added that "the Court concluded that the retention of associated data ... falls outside the CSIS's legislatively defined jurisdiction" and "that therefore this retention of associated data is illegal."

Some of these criticisms align with ones previously made by a federal watchdog agency, which had already publicly complained that CSIS rarely lets go of any phone logs and Internet-transaction data it collects.

This fall, the Security Intelligence Review Committee criticized CSIS for going beyond its "strictly necessary" collection mandate by "ingesting bulk data sets" in bids to predict patterns of terrorism. The previous year, SIRC faulted CSIS for indefinitely holding on to telecommunications metadata it gathers in the course of wiretapping investigations, alleging CSIS was likely legally obliged to destroy such material.

SIRC has recommended that CSIS reconsider these practices or at least tell the Federal Court about them. But CSIS's written response was that it did not need to tell the Federal Court what it was doing.

"The Service did not agree with SIRC's recommendation to advise the Federal Court of activities relating to metadata collected under warrant. CSIS's position is that ... the CSIS Act does not confer any general supervisory authority to Federal Court judges, therefore, it believes that SIRC's recommendation was both inappropriate and unwarranted," was the spy service's position at the time, according to the report.

The Federal Court has now signalled it disagrees with this assessment. In recent years, CSIS's collection capabilities are thought to have been vastly increased by co-operation warrants that exist with the Communications Security Establishment, a federal spy agency that dredges global telecommunications data in bulk. CSE's headquarters are now located beside CSIS's headquarters.

CTV.CA
5 things to know about the CSIS metadata ruling
Friday, 04 November 2016
Byline: Graham Slaughter

Analysis: In a scathing ruling released Thursday, a Federal Court judge said the Canadian Security Intelligence Service illegally held on to potentially revealing electronic data about people over a 10-year timeframe.
We break down the ramifications of the major decision and what it means for the future of Canada's spy agency:

What do we know?

Justice Simon Noel said CSIS held on to metadata that was not directly linked to threats to Canadian security. Keeping the information was a breach of the agency's duty to inform the courts, the judge ruled, since the information was obtained through judicial warrants.

According to court documents, the information was crunched beginning in 2006 and includes data trails linked to family and friends of people under CSIS surveillance, but who were not under investigation themselves.

What is metadata?

Metadata is information associated with a communication, such as an email address or telephone number. Metadata does not include contents of the correspondence. However, it can reveal a person's movement, communication patterns or other identifying details.

In this case, it is difficult to pinpoint the exact type of metadata CSIS held because the 126-page ruling was heavily redacted.

You can see it for yourself here.

What has CSIS said?

CSIS director Michel Coulombe said Thursday that the agency has stopped allowing access and analysis of the metadata until it has time to fully assess the judge's decision. He added that he regrets "the court's serious concerns with respect to meeting our duty of candour."

What happens next?

The decision immediately sets new rules on how metadata can be used by CSIS. Only metadata that relates to a specific security threat, investigation, prosecution, national defence or foreign affairs can be kept and used.

The judge also suggested that the federal government should seriously take a fresh look at the CSIS Act of 1984, which he said is "showing its age" thanks to modern technology.

How has the government reacted?

Public Safety Minister Ralph Goodale said the government won't appeal the decision and said he will follow up with CSIS top brass about the ruling. He added that "Canadians need to have confidence" about all federal departments and agencies.

CTV.CA
Feds hold Twitter consultation on national security
Friday, 04 November 2016
Byline: Laura Payton

Ottawa - Public Safety Canada held a Twitter chat Thursday night to hear what Canadians think about national security and its responsibility to Canadians.
The department in charge of the RCMP, the Canadian Security Intelligence Service and its oversight body, and the Canada Border Services Agency asked people to tweet them using the hashtag #YourNatlSec starting at 8 p.m. ET to discuss accountability in national security.

The social media discussion comes the same week the House public safety committee is starting its review of bill C-22, which will amend some of the laws changed under the Conservatives' highly contentious C-51.

The review also comes hours after a shocking revelation that CSIS held on to 10 years of electronic data it wasn't allowed to have. The metadata, which includes information like a telephone number or email address but not the content of a communication, wasn't directly related to national security threats. The Federal Court released a decision Thursday rebuking CSIS for keeping the information.

Public Safety Minister Ralph Goodale didn't participate in the Twitter chat.

New Democrat justice critic Murray Rankin says he wanted as many people as possible to participate.

"Any effort to get Canadians engaged is great," he said.

The department is holding national security townhalls across the country until Dec. 15. It's also is accepting input on its website too.

Rankin, who once served as a lawyer to the Security Intelligence Review Committee, says he'd like to see changes to C-22. The bill would set up a parliamentary committee to review spy agency activity after the fact, but no oversight during operations.

Goodale has promised more changes to C-51 are still to come, but Rankin says he wants to know when.

"It's been more than a year. I haven't seen a single comma change in C-51, which is an odious bill that deserves to be, we say, repealed," he said.

Toronto Star
CSIS collected data on citizens for past 10 years
Friday, 04 November 2016
Byline: Alex Boutilier

Ottawa - Canada's spies for almost a decade illegally kept and analyzed data on people who posed no threat to national security, a federal court judge has ruled.
In a scathing ruling, Justice Simon Noël said the Canadian Security Intelligence Service had illegally retained an unknown amount of data on "third party" and "non-threat" individuals since 2006.

CSIS fed that data into a powerful database that allowed the agency to draw out "specific, intimate insights into the lifestyle and personal choices of individuals," read the heavily censored court ruling, circulated to journalists on Thursday.

Moreover, CSIS failed to inform the court, which acts as one of the only checks against the agency's investigative powers, about the program for almost a decade.

"(Judges) serve as the gatekeepers of intrusive powers, ensuring a balance between private interest and the state's need to intrude upon that privacy for the collective good," Noël wrote.

"If the CSIS unduly limits the flow of information the court needs to make proper determinations, then the CSIS can be seen as manipulating the judicial decision-making process."

According to the court documents, CSIS created the Operational Data Analysis Centre (ODAC) in 2006 to be a "centre of excellence for the exploitation and analysis" of different data sets.

One source of ODAC's data was gathered through legally approved surveillance of CSIS targets. Anyone who communicated with the target - family, friends, employers - would be considered "third party" or "non-threat" individuals.

Information about those people, who are not suspected threats or targeted by the agency, was scraped into the ODAC. CSIS wanted to retain that information - metadata like telephone numbers and Internet protocol addresses - indefinitely.

Although the information seems innocuous in isolation, the court documents make clear it was collected to give the agency highly detailed intelligence. And while collecting the data was legal, retaining it indefinitely was not.

In the wake of Noël's ruling, CSIS has halted all access and analysis of the data.

The revelations prompted an unprecedented snap press conference by CSIS director Michel Coulombe. Coulombe told journalists the agency believed its actions were legal, from 2006 until October's ruling, but accepts Noël's findings.

Coulombe could not, however, explain why CSIS believed it needed to inform the court of ODAC's existence in 2006, but failed to do so for almost 10 years.

"I'll be honest, we went through our records and we really can't find a good explanation of why the court was not informed," Coulombe told reporters Thursday evening.

Coulombe was clear that CSIS believed the program was useful and effective, and said he would like to keep it in operation.

"That is something I will discuss with officials, (Public Safety Minister Ralph Goodale) and it is a public policy decision that the government and parliamentarians will have to make," the director said.

In a statement, Goodale said the government will not appeal Noël's decision.

But the minister did leave open the possibility of changing the CSIS Act to allow for such techniques in the future. Goodale noted the court ruling found the legislation governing CSIS was beginning to "show its age" after 30 years, and threats and investigative techniques have changed over that time.

Goodale said he would be discussing CSIS's failure to tell the court the full truth, however, with the agency's senior management.

"In matters of security and intelligence, Canadians need to have confidence that all the departments and agencies of the (government) are being effective at keeping Canadians safe, and equally, that they are safeguarding our rights and freedoms," Goodale wrote.

Noël noted this was the second time in three years that the Federal Court has found that CSIS failed to provide key information judges needed to properly authorize the agency's activities.

"I wonder what it will take to ensure that such findings are taken seriously," Noël wrote. "Must a contempt of court proceeding, with all its related consequences, be necessary in the future?"

Postmedia News
Hillary Clinton was warned in 2010 that U.S.-Canada intelligence sharing 'may be controversial for Canadians'
Friday, 04 November 2016
Byline: Zane Schwartz

Ottawa - Huma Abedin warned Hillary Clinton in 2010 that cables from the U.S. Embassy in Ottawa could cause problems for Stephen Harper's government, emails released Thursday show.
"Two cables set for release contain especially sensitive information on counterterrorism and intelligence sharing. The depth of bilateral cooperation detailed in the cables may be controversial for Canadians," said longtime Clinton-advisor Abedin.

The email between Abedin and the then-U.S. Secretary of State is one of 357 released Thursday by the State Department in response to a lawsuit. More emails are scheduled for release Friday.

Abedin's email was sent on Nov. 27 2010. On Nov. 29 the New York Times published a story detailing a 2008 conversation between the former head of the Canadian Security Intelligence Service Jim Judd and senior State Department counsellor Eliot Cohen.

The story details a conversation where Judd told Cohen that Canada received warning the Taliban was planning an explosion at Sarpoza Prison in Kandahar but was unable to "get a handle on the timing."

Ralph Goodale: Bill C-22 is designed to protect Canadians' rights, and defend their security

'Everything we do is reviewed': Canadian security agency defends activities amid spying allegations

This seemed to contradict a statement made by former chief of defence staff General Rick Hillier that: "Obviously we would have liked to have known so we could have pre-empted or helped, more accurately, the Afghans pre-empt that kind of thing."

The New York Times story was based on documents leaked to WikiLeaks detailing correspondence from U.S. diplomatic officials around the world, including staff from the embassy in Ottawa.

One of the most significant revelations was the Canadian government's concern in 2004 that they were being locked out of the Five Eyes network as punishment for not joining the U.S.-led war in Iraq. One leaked document said the Canadian government had: "expressed concern at multiple levels that their exclusion from a traditional 'four- eyes' construct is 'punishment' for Canada's nonparticipation in Iraq

and they fear that the Iraq-related channel may evolve into a more permanent 'three-eyes' only structure."

The Five Eyes network is an alliance between the signals intelligence agencies of Canada, the United States, Australia, the United Kingdom and New Zealand. Signals intelligence agencies focus on monitoring people via telephone and computer instead of by relying on human agents to monitor them in person. The five countries divided the world during the Cold War with each spying on certain regions and all sharing the information they intercepted. The United States temporarily restricted Canada and New Zealand's access within the Five Eyes network following both countries reluctance to join the 2003 war in Iraq.

Abedin was concerned the revelations might cause problems for the Harper government. "Canadian press coverage of the issue may put additional pressure on the Harper government," said Abedin.

Abedin need not have worried. Canadian coverage at the time largely focused on a comment from Judd that Canada had an "Alice in Wonderland" attitude on terrorism and a cable prepared prior to Barack Obama's visit to Ottawa in 2009 claiming that Canada had an "inherent inferiority complex" when it came to the United States.

The emails released Thursday demonstrate how the United States and Canada worked behind the scenes to downplay the importance of the 2010 revelations.

"Ambassador Jacobson saw Foreign Minister Cannon the evening of November 24 and reviewed the substance of the cables in The New York Times' cache," said Abedin, adding: "Cannon said he did not see any serious problems for the government."

The significance of Canada's role in the Five Eyes alliance became clearer in 2013 when leaked information from whistle blower Edward Snowden showed that Canada's Communications Security Establishment set up covert spy posts in about twenty countries on behalf of the United State's National Security Agency .

Those revelations sparked a debate in Canada about whether there is sufficient oversight over Canada's security agencies. In response, Stephen Harper's government passed Bill C-51, which granted significant new powers to the security agencies. Justin Trudeau promised to alter Bill C-51 to include more oversight provisions during the 2015 federal election campaign but has yet to do so.

On Thursday a Federal Court judge ruled that the Canadian Security Intelligence Service broke the law by keeping potentially revealing data about Canadians over a 10-year period.

Journal de Montréal
Pas de journalistes épiés par l'UPAC ou la GRC
Friday, 04 November 2016
Byline: Journaliste maison

Ottawa - Le grand patron de l'Unité permanente anticorruption, Robert Lafrenière, assure qu'aucun journaliste n'a fait l'objet d'une enquête ou de quelque surveillance de l'UPAC depuis sa création en 2011.
Le premier ministre Justin Trudeau a lui aussi indiqué que les agences fédérales de sécurité ne surveillent pas les journalistes comme l'ont fait la Sûreté du Québec et le Service de police de la Ville de Montréal.

Hier, il a dit s'être entretenu à ce sujet avec les dirigeants de la Gendarmerie royale du Canada (GRC) et de l'agence d'espionnage canadienne, le Service canadien du renseignement de sécurité (SCRS), et avoir reçu la confirmation que le fédéral n'a pas cette «préoccupation».

ABC (Australia)
Australia exposed to $16 billion cyber-attack risk, insurance giant Lloyd's warns
Friday, 04 November 2016

Canberra - The growing risk of cyber attacks leaves the Australian economy exposed to a potential $16 billion damage bill over the next decade, according to one of the world's biggest insurance companies.
In a joint study with Cambridge University, the Lloyd's insurance giant has found out of 301 global cities, Sydney ranks 12th in terms cyber attack exposure with $4.86 billion of economic growth at risk.

Lloyd's global chief executive Inga Beale told The World Today dealing with the constant threat of cyber attacks was now critical for businesses of all sizes.

"It's not just for banks to worry about -- it impacts retailers, travel and hospitality firms, education and healthcare providers, and any business with proprietary information worth protecting," Ms Beale said.

"Where a decade ago people would talk about preventing a cyber-attack, the reality is firms will be subjected to attacks.

"The issue is how you mitigate against that."

The Australian Cyber Security Centre recently said systems in government agencies had been hit with 1,095 cyber security incidents considered serious enough to trigger an operational response.

The Lloyd's study points to a report from the accounting firm PWC which highlights a 109 per cent increase in detected security incidents in Australian companies, compared to a 38 per cent global average.

Under proposed legislation before the Australian Parliament, hacked companies that lose personal details, tax file numbers, medical records or credit card information will be required to report the incident and alert customers.

'High-profile data breaches just the beginning': Beale

But Ms Beale warns that while big business and government agencies are at most risk, private individuals are at risk from personal information stored in smartphones and personal computers.

"We are living in a world where people carry a globally-connected supercomputer in their pocket and almost every important work document is stored in the cloud, on servers or online," Ms Beale said.

"The result is an explosion in the potential for cyber risk. The latest series of high-profile data breaches is just the beginning.

"With the emergence of the Internet of Things the potential for cyber risk is enormous."

As one of the world's major insurers and reinsurers, Lloyd's is now seeing demand for cyber attack cover form a major part of its traditional business of insuring for global natural disasters and catastrophes.

Lloyd's says demand for cyber insurance in Australia has increased by 16,828 per cent in the past two years as businesses seek protection from current and emerging threats.

The Lloyd's index points to a range of other risks including power outages, terrorism, sovereign default, oil price shock, heatwave, drought and floods.

Journal de Montréal
Un deuxième journaliste surveillé par le SPVM
Friday, 04 November 2016
Byline: Benoît Philie

Montréal - Les communications du reporter ont été épiées en 2014
Les communications d'au moins un autre journaliste ont été espionnées par la police de Montréal, a confirmé hier l'assistant-directeur du SPVM, lors d'un point de presse où le chef Philippe Pichet brillait par son absence.

L'assistant-directeur du SPVM, Patrick Lalonde, a confirmé hier en conférence de presse qu'un second reporter a été épié par le service de police en 2014.

«Des vérifications nous ont permis de trouver un autre cas d'enquête à l'intérieur de laquelle une autorisation judiciaire a été donnée à l'endroit d'un journaliste», a déclaré Patrick Lalonde, au quartier général du SPVM.

Les registres de communications de ce journaliste ont été épiés en décembre 2014 dans le cadre d'une enquête interne sur un policier. Selon la police, le reporter aurait été ciblé par le même genre d'enquête que le chroniqueur de La Presse Patrick Lagacé.

M. Lalonde a refusé de nommer le journaliste et l'agent concernés puisque l'enquête «est actuellement entre les mains de la Direction des poursuites criminelles et pénales [DPCP]».

Un mandat DNR (Dial Number Recorder) aurait été autorisé dans ce cas aussi, ce qui permet d'obtenir les numéros entrants et sortants d'un téléphone cellulaire, à partir du moment où l'autorisation judiciaire est obtenue d'un juge.

D'AUTRES CAS

Le Journal révélait mardi que trois journalistes, dont Félix Séguin du Bureau d'enquête, ont également fait l'objet d'une forme de surveillance par le SPVM. Ce sont toutefois les registres d'appels de certains policiers qui ont été fouillés pour y trouver les numéros de téléphone des reporters.

D'autres cas d'espionnage pourraient bien être dévoilés d'ici à vendredi prochain, moment où le SPVM prévoit avoir terminé la vérification de l'ensemble de ses dossiers concernant des personnes à statut particulier, comme les juges, les avocats, les élus et les journalistes.

Le service de police s'est engagé à informer et rencontrer toute personne à statut particulier impliquée de près ou de loin dans ce genre de dossier.

PHILIPPE PICHET ABSENT

Questionné à propos de l'absence du directeur Philippe Pichet au point de presse, M. Lalonde a offert une réponse laconique. «M. Pichet est toujours chef de police. [...] Il vaque à d'autres occupations présentement, vous comprendrez qu'il en a beaucoup», a-t-il répondu.

Times of Israel
Israel Aerospace wins $15m Asian cyber deal
Friday, 04 November 2016

Jerusalem - Israel Aerospace Industries Ltd. (IAI) (TASE: ARSP.B1) has announced that it has signed a contract worth $15 million for a cyber- intelligence system with a customer in Asia. The contract is for an advanced, national level, strategic cyber solution, which combines cellular systems and cyber and includes establishing an intelligence center and infrastructure and providing unique sensors. The contract will be executed by one of ELTA/IAI's cyber subsidiaries and development centers.
IAI's Director of Cyber Programs Esti Peshin said, "This new contract is an example of the 'ecosystem' created by IAI's cyber subsidiaries and R&D centers and the parent company. Our worldwide innovation centers benefit from IAI's size and experience while simultaneously having the flexibility of a start-up company. The proximity to the customers combined with innovation, white-hat hacking and engineering capabilities enables us to effectively deal with the many challenges of the cyber world. We intend to continue developing the strategy in the coming months by to additional cyber subsidiaries & R&D centers."

Cyber security is a strategic sector and core competency for IAI. The company is developing unique cyber solutions for intelligence, protection, monitoring, identification and accessibility. These advanced capabilities are possible due to the innovative technologies developed by IAI's research, development and excellence centers, offering IAI's customers a wide range of capabilities for dealing with evolving and ever growing cyber threats. IAI operates four cyber development centers - one in Singapore, one in Switzerland, and two in Israel - the most recent of which was opened in Beersheva.

IAI also leads the Israel Cyber Company Consortium (IC3) which offers end-to-end solutions for national cyber systems and is comprised of leading Israel cyber companies.

Gulf News
IoT pulls out the welcoming mat to cyber threats
Friday, 04 November 2016
Byline: Harshul Joshi

Dubai - The massive distributed denial of service (DDoS) attack on Dynamic Network Services Inc, (Dyn), a US-based Domain Name Server (DNS) provider on October 21, 2016, again exposes the vulnerabilities being made visible by the advance of the internet of Things into every aspect of modern life.
DDoS attacks are especially disruptive, utilising hacking networks known as botnets, which are compromised computers that actors bring under their control. There are many way hackers gain the initial control but most commonly it is achieved by making users inadvertently download software by following a link in an email or by making users agree to download a corrupted file.

Once the initial infection has occurred the malware looks to spread across the network, and even smart home gadgets may be compromised in this way. These botnets are then used to bombard servers with simple requests for information that when carried out simultaneously overwhelm and block legitimate access.

Given the relentless rise of the internet of Things (IoT), and the fact that the very devices that were hacked to orchestrate this incident are the same ones finding their way into our lives at an ever-expanding pace, the cascading effects of this latest attack have implications at every level of digital transformation, right the way through to smart city developments.

The rise of IoT will prompt similar attacks in the future as inadequately secured IoT devices will continue to be an engine to facilitating such breaches.

The internet and its ubiquitous connectivity has developed to become a crucial component of national critical infrastructure. As such it is essential that we understand how the internet is used to support our businesses and governments, and to look to find answers to burning questions including:

. What are the fundamental infrastructure and services supporting this central component of the critical infrastructure puzzle?

. What are the primary objectives or the key assets that need to be managed or mitigated, and do we have preventive, detective, responsive and recovery controls in place ensuring the system is resilient?

. What are the attack vectors and who are the attack actors? What are their capabilities, techniques and objectives?

. How can technological and regulatory stacks be fine-tuned and galvanised for this type of attack?

. What emerging technologies, methodologies and ideas could be used to mitigate these threats in the near, mid and long term and what will it take to increase preparedness?

The cyber security community needs to work closely with key national entities, whether they be telecom or DNS providers, or key websites that may be at risk. All IoT stakeholders need to understand the interconnected parameters of their operations as well as the correlation between them if a similar attack is launched.

In our estimation, the risk of such breaches happening in the future can be limited if entities follow the Cyber Security Life-Cycle, which incorporates planning, detection, protection, and recovery of digital information.

In order to adhere to the Life-Cycle, organisations need to understand their risk profile before initiating a cyber security management and mitigation exercise, which would provide them with an understanding of all their digital assets, the full range of threats they may face and the vulnerabilities, and how best to protect themselves from such.

This is an area we believe the UAE can take a lead in given the relative lack of legacy, and progressive legislation such as Dubai's Open Data Laws, which place the country in a better position to predict and/or react to massive cyberattacks.

Radio-Canada Nouvelles (web)
Espionnage de journalistes : Trudeau ouvert à revoir le Code criminel
Thursday, 03 November 2016
Byline: Journaliste maison

Ottawa - Le gouvernement fédéral doit s'interroger sur ce qu'il peut faire pour mieux protéger les sources journalistiques, affirme le premier ministre canadien Justin Trudeau, dans la foulée des nouvelles révélations d'espionnage de journalistes de la part de la Sûreté du Québec (SQ).
M. Trudeau affirme cependant que les Canadiens peuvent être rassurés quant aux pratiques en vigueur à la Gendarmerie royale du Canada (GRC) et au Service canadien du renseignement de sécurité (SCRS).

En conférence de presse jeudi midi, M. Trudeau a été interrogé sur la possibilité que son gouvernement revoit l'article 193 du Code criminel, évoqué par la SQ mercredi pour justifier l'espionnage des communications de six journalistes québécois en 2013.

Je pense qu'avec ces nouvelles, on va certainement avoir des réflexions sur comment, en tant que société, nous nous devons d'assurer la protection des journalistes et de leurs sources confidentielles.

Justin Trudeau

« Je sais que dans un monde où il y a quand même des dangers, nous nous devons d'être responsables dans notre fonctionnement », a-t-il ajouté. « Mais c'est fondamental à nos valeurs, à notre identité, en tant que pays libre et juste, que les journalistes puissent faire leur travail d'informer les Canadiens et donc de protéger leurs sources confidentielles. »

Trudeau « rassuré » par la GRC et le SCRS

M. Trudeau a par ailleurs révélé qu'il avait communiqué avec le commissaire de la GRC et les responsables du Service canadien du renseignement de sécurité (SCRS) dans la foulée de cette affaire pour s'assurer qu'« aucune activité de ce type [ne] se passe au niveau fédéral ».

On a des balises, des règles et des paramètres très stricts en place, et j'ai été rassuré qu'ils sont tous en train d'être suivis. On peut être rassuré qu'au niveau fédéral, on n'a pas cette préoccupation.

Justin Trudeau

En mai dernier, CBC avait révélé que deux journalistes de La Presse, Joël-Denis Bellavance et Gilles Toupin, avaient bel bel et bien été espionnés pendant neuf jours, en 2007, par des agents de la GRC.

Les deux hommes avaient fait l'objet d'une surveillance physique de la part d'enquêteurs, qui souhaitaient ainsi découvrir la source qui leur avait dévoilé des détails d'une conversation impliquant Adil Charkaoui et un plan pour détourner un avion.

Après neuf jours, les enquêteurs avaient demandé une autorisation formelle au quartier général de la GRC, mais cela leur avait été refusé. La direction avait alors ordonné que les journalistes ne soient pas considérés comme des suspects. Elle précisait qu'aucune autre démarche ne devait être entreprise sans le consentement de la direction.

Vice
L'affaire Lagacé : « Une attaque radicale à la liberté de presse », dit Edward Snowden
Thursday, 03 November 2016
Byline: Justine de l'Église

Montréal - Les agissements de la Sûreté du Québec (SQ) et de la police montréalaise sont une « menace au modèle traditionnel de démocratie », a martelé mercredi Edward Snowden à un public de quelque 600 personnes. La conférence a débuté avec plus d'une heure de retard, en raison d'une manifestation étudiante en soutien aux employés de l'Université McGill, qui demandaient de meilleures conditions de travail.
Sur écran géant, en direct de la Russie où il a trouvé asile, le célèbre lanceur d'alerte responsable de la plus importante fuite d'informations sur la sécurité de l'histoire des États-Unis a été très sévère envers les corps policiers québécois.

Cette conférence était prévue il y a longtemps, mais elle tombait étrangement à point : La Presse nous apprenait la journée même que six journalistes avait été surveillés par la SQ, deux jours après qu'il a été révélé au grand jour que le chroniqueur Patrick Lagacé avait été espionné par le Service de police de la ville de Montréal (SPVM).

Si l'ex-agent de la CIA et ancien contractant de la NSA avait déjà réagi sur Twitter en début de semaine, il a consacré une bonne partie de la conférence à souligner la gravité de l'action des policiers dans l'affaire Lagacé. « Désormais, la police locale peut décider qu'elle n'aime pas le travail d'un journaliste, aller voir un juge de paix [...] qui va dire : "Merveilleux! Regarde le GPS sur son téléphone, découvre où il est allé, avec qui il a communiqué. Non, tu ne peux pas lire ses courriels ou écouter ses appels, mais tu peux voir qui il a rencontré, qui il a appelé et pour combien de temps, et ainsi obtenir de l'information extraordinaire sur la façon dont cet individu travaille." »

Selon le célèbre lanceur d'alerte américain, il s'agit d'une « attaque radicale à la liberté de presse ». Snowden a appelé le directeur du SPVM, Philippe Pichet, à donner sa démission et il a critiqué le maire de Montréal Denis Coderre, ainsi que le premier ministre Philippe Couillard de ne pas l'avoir exigée.

Il est même allé plus loin en suggérant qu'il est possible que le système de justice lui-même fasse défaut. « Le gouvernement a érigé des mécanismes pour contourner ces choses, ces restrictions, a-t-il souligné. Peut-on reconnaître une idée radicale, ou au moins en débattre raisonnablement : la loi commence à échouer à protéger nos droits? »

Attention aux lois adoptées pour contrer de fausses menaces

Snowden a à nouveau mis les citoyens en garde contre les dérives autoritaires des gouvernement actuels, qui demandent plus de pouvoir pour faire face à des terroristes soi-disant capables de mettre à mal nos États. « Il n'y a aucune preuve que ce soit le cas, mais les politiques de la peur ont modifié la façon dont nos lois sont adoptées. »

Il a cité au passage la Loi antiterroriste (C-51), dont l'adoption en 2015 avait suscité un lot de critiques d'experts et de citoyens s'inquiétant de la protection de la vie privée et des droits individuels. Cette loi donne aux autorités des pouvoirs élargis pour identifier les terroristes et contrer leurs plans, et autorise le partage d'information sur les citoyens canadiens entre 128 institutions fédérales, dont les agences, les ministères et la GRC.

Justin Trudeau avait promis en campagne électorale qu'il allait modifier cette loi, en retirer les « éléments problématiques » et « les définitions trop vagues comme "propagande terroriste" », et garantir que « tous les mandats du Service canadien des renseignements et de la sécurité respectent la Charte canadienne des droits et libertés ». Mais il ne l'a toujours pas fait.

La seule modification prévue pour l'instant, le projet de loi C-22, permettrait la formation d'un comité parlementaire chargé de surveiller les actions des agences de sécurité. Pour le reste, le gouvernement canadien procède depuis le 8 septembre à des consultations à l'échelle du pays avant de proposer de nouvelles modifications. Comme la session prend fin en décembre, il est fort probable qu'aucun changement ne soit apporté avant l'an prochain.

En vidéo- conférence à Toronto le mois dernier Snowden avait avancé que Justin Trudeau était réticent à faire de telles modifications. D'après Snowden, le premier ministre « craint que son gouvernement soit accusé de laxisme sur le terrorisme, peu importe si cette loi est inefficace pour prévenir la moindre attaque terroriste ».

China Daily
New vision for big data: Safe cities
Friday, 04 November 2016

Byline: Edith Mutethya

Security and technology experts are calling on African governments to embrace safe-city concepts in an effort to address the increasing incidence of crime and extremism.
Combating crime, according to the experts, has become the hardest activity for police and security organizations, as available video security systems are faced with blind spots, unclear images, difficult video retrieval and data damage or loss.

To solve these challenges, the experts are recommending a safe-city technology solution provided by Huawei Technologies Co, a Chinese multinational IT company headquartered in Shenzhen, Guangdong province.

The solution is an integral network of sensors and communication platforms that enable public-safety, law-enforcement and related agencies to access context-specific intelligence for managing real-time events and providing seamless service delivery to the public.

Experts who spoke during the Huawei Safe City Africa Summit in Nairobi on Oct 14 and 15, applauded the country's safe-city project and its three-way partnership between Huawei, Safaricom (Kenya's leading mobile phone operator) and the Ministry of Internal Security.

The first phase of the project, which involved the installation of surveillance cameras in densely populated Nairobi and Mombasa, coincided with a 46 percent drop in crime from 2014 to 2015.

The number of international visitors to Kenya also increased by 14 percent in the first four months of this year to 263,284, compared with 231,038 in 2015, according to Shaka Kwach, special projects head at Safaricom.

Eng Koh Hong, the global chief public safety expert at Huawei, says that while intelligent video surveillance, broadband-trunked radio and computer-aided dispatch are crucial, they are not enough to create a safe city.

"There is a need for a policing cloud to link up the silos of different public safety agencies for better information sharing and user experience," he says.

The one-stop ICT solutions provided by Huawei in the safe-city market are now deployed in more than 100 cities in some 30 countries, and serve more than 400 million people.

Huawei not only offers safety to Kenyan citizens and visitors but also brings beautiful rhythms to the ears of music lovers in South Africa.

On Oct 27, Huawei signed cooperation contracts with global and local music vendors in Johannesburg to accelerate digitalization of African music. At the Huawei Southern Africa Partner Summit held in Johannesburg, Huawei inked contracts with Spice Music, Mtech, CCA and other local music vendors.

Africa has great demand for digital services, like music, games and videos, according to Huawei's analysis. In five years, digital services' year-on-year growth in Kenya will be about 40 percent, the company says. However, there remains a big gap between the growing demand and actual production.

The summit, aimed at creating a sharing platform to promote digital collaboration in Africa, has attracted more than 40 industry partners.

Wilson Feng, president of Huawei's carrier business in the southern Africa region, said at the summit that the company is willing to work hand-in-hand with African partners to create a better industry ecosystem.

"We will leverage our innovative technologies in digital services, and our global resources, to improve African consumers' digital experience and accelerate Africa's digital economy development," Feng said.

Through the cooperation, Huawei's digital business cloud will also help its partners in monetization, which means it's a win-win solution for all parties in the ecosystem, he said.

The cooperation with content providers means Huawei will hold the copyrights of millions of music titles from international and local vendors. This is Huawei's first breakthrough into the global music space.

Huawei will then be able to provide music to telecom operators in South Africa, such as Vodacom, MTN, Cell C, etc, which offer music to end users through their music apps.

The summit also showed off Huawei's efforts to leverage its Digital inCloud, a software platform, to integrate content across music, video, gaming and other digital service genres.

Siphumelele Zondi, senior producer and anchor of South African Broadcasting Corporation, said there would be a great need for artists in southern Africa to venture into the digital space.

Often local content is in demand but not available on digital platforms, which then promotes piracy, he said.

"Africa is a mobile-device-intensive environment, and platforms such as Huawei's Digital inCloud can aid the availability of local content to Africa," Zondi said.

Huawei, although a nonpublic company and not on the list, spent 59.6 billion yuan ($8.8 billion; 7.9 billion euros; 7.14 billion) on R&D in 2015, making it the highest spender in China, according to the 2016 Global Innovation 1000 Study report, released on Wednesday by PricewaterhouseCoopers.

Reuters
China internet authority formalises regulations for live- streaming industry
Friday, 04 November 2016
Byline: Staff reporter

Beijing - Chinese internet authorities have formalised controversial rules regulating the country's fast-growing live-streaming video industry, in a move that strips out smaller competitors and places hard-line surveillance measures on leading firms.
In an announcement posted on their website on Friday, the Cyberspace Administration of China grouped a handful of earlier restrictions under a final 24-point regulation that will come into effect on Dec. 1.

The rules require streaming services to log user data and content for 60 days, and work with regulators to provide information on users who stream content that the government deems threatening to national security or social order. Both users and providers are punishable under the regulations.

The law also codifies rules that ban online news broadcasting services from original reporting, requiring them to identify sources and non-selectively reproduce state-sanctioned information.

China's live video streaming industry has experienced booming growth in the past two years as dozens of video and social media sites scrambled to add the updated capabilities to their existing services.

Credit Suisse Group analysts estimate the industry could top $5 billion by the end of 2017, driven by cheap bandwidth and a growing population of young mobile users.

The industry's exponential growth attracted increased scrutiny from government authorities in 2016. In April, Chinese authorities called on 20 of the country's top firms to join a self- criticism coalition, saying the industry was damaging China's youth by proliferating content including pornography, fraud and terrorism.

On June 1 companies including Baidu Inc, Sina Corp , Sohu.com Inc and Youku Tudou, acknowledged new rules as part of the group, including requirements for real-name authentication.

While the latest move places wide-reaching restrictions on the sites, it also signals an official sanctioning of the industry and its top players by Chinese officials.

Much like China's earlier online video and music industries, the regulations put pressure on smaller competitors and bring larger firms into line with regulators, offering more growth opportunities for a smaller number of controllable companies.

"One of the things the government always wants to do is narrow the playing field to a smaller number of higher profile known entities, ideally ones that have a better track record of cooperating with the government," says Mark Natkin, Managing Director at Marbridge Consulting.

"In the long run it's actually relatively beneficial to the large companies."

In May the government handed down 588 licenses for prominent media outlets and live-streaming sites, effectively banning all unapproved services.

China Daily
Information sharing key to capturing corrupt officials (Canada)
Friday, 04 November 2016
Byline: Zhou Wenting

Shanghai - Information sharing has played a key role in bringing back corrupt officials who fled abroad to avoid trial, Ding Guping, director of the anti-corruption bureau at the Shanghai People's Procuratorate, said on Thursday.
Anti-graft officers have analyzed big data collected from various sources to learn about the movements of suspects, Ding said during a media briefing on the hunt for such fugitives since the launch of operation "Sky Net" in March last year.

Sky Net was launched by the Chinese government, aimed at tracking down corrupt officials hiding abroad and confiscating their ill-gotten assets.

A total of eight corrupt officials have been brought back to face trial from six countries - the United States, Canada, Australia, Thailand, Japan and Singapore - and more than 15 million yuan ($2.22 million) in illegal funds has been seized, according to the bureau.

Ding said it cooperated with the police department, the state security bureau and the immigration inspection authority to obtain information, such as conversation and transaction records from popular messaging app WeChat and mobile payment service Alipay.

Cai Guozhen, deputy director of the bureau's central office, said people always leave traces of their daily lives, which are recorded on surveillance cameras in buildings, on roads and in convenient stores, and through purchases they make. "The key is how to integrate the information," he said.

Ding said anti-graft officers formulated a specific plan for each case after analyzing such information.

For example, Sun Jin, former general manager of the sales department of a futures commission company in Shanghai, who fled to the US in the 1990s after being suspected of embezzlement of public funds, became a US citizen and changed his name and identity. However, through big data investigation

and tracking, anti-graft officers determined his identity and captured him when he checked in at a Shanghai hotel using his US passport.

Big data analysis also helped officers to track down Liang Kaifeng, a high-ranking official at a Shanghai-based State-owned enterprise specializing in papermaking. Liang was suspected of taking bribes and fled to the US, but was identified on a flight from the US to Shanghai in May.

Cai said 21 corrupt officials from Shanghai who fled the country have not been captured, and most of them are in hiding in the US, Canada and Australia.

He said it is difficult to bring them back from such countries due to a lack of bilateral extradition treaties and differences in laws, but added that it will become less difficult with increased international cooperation.

"Consensus was reached on anti-corruption cooperation to help bring fugitives back to their home country during the G20 Leaders Summit in Hangzhou, capital of Zhejiang province, in September. The group's first anti-graft research center was set up in Beijing recently," he added.

Reuters
Canada court deals blow to spy agency, says it kept data illegally
Friday, 04 November 2016
Byline: David Ljunggren

Ottawa - A court dealt Canada's spy agency a blow on Thursday, declaring it had illegally kept data collected during investigations over the past decade and threatening sanctions if the issue occurred again.
Although judges have previously criticized the Canadian Security Intelligence Service, or CSIS, for a lack of openness about its operations, the ruling was particularly uncompromising.

Federal Court Judge Simon Noel said CSIS secretly set up a special data analysis center in 2006 to help track potential terrorism suspects. The agency stored electronic information from people not linked to particular threats, which is referred to as associated data.

"CSIS has a limited mandate which does not permit the retention of associated data ... as it has done so since 2006. Therefore this retention of associated data is illegal," Noel said in the judgment.

CSIS Director Michel Coulombe told a news conference shortly after the ruling that the agency would immediately stop sharing and analyzing associated data until it could "assess potential operational and legal impacts."

Canada belongs to the so-called Five Eyes intelligence- sharing network, along with Britain, the United States, Australia and New Zealand.

Critics said the ruling reinforced their belief that CSIS was largely unaccountable.

"The fact that CSIS could go 10 years retaining large quantities of our sensitive private information, yet we're only finding out about this now, and only as a result of a court judgment, is deeply concerning," said David Christopher of OpenMedia, an advocacy group.

The case came to light in early 2016 after CSIS applied for amendments to the court warrants it needs to launch probes. At the same time, the court learned independently about the data center and launched an investigation.

Noel said CSIS broke its duty of candor toward the court by not disclosing the existence of the data analysis center.

Noting that judges had twice previously concluded the agency improperly obscured details of its operations, Noel suggested CSIS could be charged with contempt of court.

Federal Public Safety Minister Ralph Goodale, who has overall responsibility for law enforcement agencies, welcomed the ruling and said the government would not appeal it.

"I also take very seriously the explicit finding by Justice Noel that CSIS had failed in its duty to be candid with the court. I will be pursuing this criticism with the executive management of the Service," Goodale said in a statement.

Most Canadian security agencies have small individual review bodies, which OpenMedia and others complain are impotent and can only look at old cases.

Oversight is more robust in other nations such as Britain and the United States, where special legislative committees monitor the work of security and intelligence agencies.

Goodale, acting amid global concerns about the reach of security agencies, promised in June to create a similar oversight committee as part of a comprehensive probe into how national security is handled.

A scandal erupted this week in the province of Quebec when it emerged that police had secretly tracked phone calls received and made by six reporters.

Prime Minister Justin Trudeau said on Thursday he found the case troubling and had contacted CSIS to make sure the agency was not carrying out similar operations.

Globe and Mail
Quebec to probe surveillance of media
Friday, 04 November 2016
Byline: Ingrid Peritz

Quebec has announced a public inquiry into press freedom and police surveillance amid fresh disclosures that the monitoring of some journalists' cellphones lasted as long as five years and targeted an ever-growing list of reporters.
On Thursday, new evidence added to growing concerns about the scope of the police spying.

Three of Quebec's most respected investigative journalists said they were told by the provincial Surete du Quebec that their phone data had been tracked from 2008 to 2013 - the very years police were unearthing and exposing corruption in Quebec's construction industry.

The disclosures suggest police would have been able to access logs of calls that included those from whistle-blowers dealing with highly sensitive matters.

"During this whole period - I feel sick about it - the police had their noses in our phones," Alain Gravel, an award-winning RadioCanada journalist, said on the public broadcaster on Thursday.

Two other Radio-Canada television journalists, Marie-Maude Denis and Isabelle Richer, say they too were told they were under scrutiny for five years. All three had been identified on Wednesday as part of a group of six journalists targeted for surveillance by the provincial police.

As each day delivers more startling admissions from police about surreptitious monitoring, one opposition MNA said the situation in Quebec was reminiscent of the former Soviet bloc.

The week began with the bombshell report that La Presse columnist Patrick Lagace had had his cellphone data tracked for months this year; since then, the list of reporters targeted by police has not stopped growing.

Late in the afternoon on Thursday, Montreal's police department said their own investigation found a second journalist was the object of a surveillance warrant, this one in 2014; police did not identify the reporter, but said the tracking operation was part of a probe into one of its own officers, as was the case for Mr. Lagace.

The latest case brings to 11 the number of journalists in Quebec whose phones were reportedly monitored by either the Montreal or provincial police - the two largest forces in Quebec.

Montreal police obtained court warrants to monitor two journalists; Quebec provincial police got court orders against six journalists, according to facts confirmed by both services. And in the case of three

others, police scrutinized the call logs of its officers to find out who had been speaking to the reporters, according to a media report.

The Liberal government of Philippe Couillard, which has tried to manage the controversy since it began to unfurl on Monday, announced on Thursday it would set up a commission of inquiry. Earlier this week, the government had set up a panel of experts to study the revelations; that panel will now be upgraded.

"Because the principle of press freedom, the principle of the protection of sources, is extremely important, well that is what's at the heart of the affair," said Quebec Public Security Minister Martin Coiteux. "But the confidence of our population is also, we believe, shaken."

"We want to shed light on the question, and we'll do it in a transparent way," he said.

The commission's mandate has not been specified; however, Quebec Justice Minister Stephanie Vallee stressed the importance of journalistic sources and freedom of the media.

It would likely mean Quebec would stage months of hearings to probe the activities of police and possibly their ties to politicians. The Quebec provincial police launched their probe of the six journalists in 2013 the same day they received a call from a Parti Quebecois cabinet minister, Stephane Bergeron. Mr. Bergeron admitted he called the head of the SQ at the time to ask him to look into it, but he says he never ordered the journalist surveillance. Mr. Bergeron stepped aside on Thursday as PQ public-security critic. In Ottawa, Prime Minister Justin Trudeau said reports about the media surveillance were "troubling."

"Like all Canadians, I am following this story coming out of my city, my province, with concern," Mr. Trudeau said. He said he obtained assurances from the RCMP and CSIS that "there has been nothing of this sort happening at the federal level."

"We have actually very strong safeguards and protections in place to protect freedom of the press in the course of the business conducted by CSIS and the RCMP," he said. "Not only is freedom of the press important, it's one of the foundational safeguards of a free democracy, of a free society."

Reuters
FBI examining fake documents targeting Clinton campaign: sources
Friday, 04 November 2016
Byline: Staff report

Washington - The FBI and U.S. intelligence agencies are examining faked documents aimed at discrediting the Hillary Clinton campaign as part of a broader investigation into what U.S. officials believe has been an attempt by Russia to disrupt the presidential election, people with knowledge of the matter said.

U.S. Senator Tom Carper, a Democrat on the Senate Homeland Security Committee, has referred one of the documents to the FBI for investigation on the grounds that his name and stationery were forged to appear authentic, some of the sources who had knowledge of that discussion said.

In the letter identified as fake, Carper is quoted as writing to Clinton, "We will not let you lose this election," a person who saw the document told Reuters.

The fake Carper letter, which was described to Reuters, is one of several documents presented to the Federal Bureau of Investigation and the U.S. Department of Justice for review in recent weeks, the sources said.

A spokeswoman for Carper declined to comment.

As part of an investigation into suspected Russian hacking, FBI investigators have also asked Democratic Party officials to provide copies of other suspected faked documents that have been circulating along with emails and other legitimate documents taken in the hack, people involved in those conversations said.

A spokesman for the FBI confirmed the agency was "in receipt of a complaint about an alleged fake letter" related to the election but declined further comment. Others with knowledge of the matter said the FBI was also examining other fake documents that recently surfaced.

U.S. intelligence officials have warned privately that a campaign they believe is backed by the Russian government to undermine the credibility of the U.S. presidential election could move beyond the hacking of Democratic Party email systems. That could include posting fictional evidence of voter fraud or other disinformation in the run-up to voting on Nov. 8, U.S. officials have said.

Russian officials deny any such effort.

In addition to the Carper letter, the FBI has also reviewed a seven-page electronic document that carries the logos of Democratic pollster Joel Benenson's firm, the Benenson Strategy Group, and the Clinton Foundation, a person with knowledge of the matter said.

The document, identified as a fake by the Clinton campaign, claims poll ratings had plunged for Clinton and called for "severe strategy changes for November" that could include "staged civil unrest" and "radiological attack" with dirty bombs to disrupt the vote.

Like the Carper letter, it was not immediately clear where the fraudulent document had originated or how it had begun to circulate.

On Oct. 20, Roger Stone, a former Trump aide and Republican operative, linked to a copy of the document on Twitter with the tag, "If this is real: OMG!!"

Benenson's firm had no immediate comment. Craig Minassian, a spokesman for the Clinton Foundation, said the document was "fake." He said he did not know if the FBI had examined it.

Stone did not respond to emails requesting comment.

A spokesman for the Clinton campaign, Glen Caplin, said the document was a fake and part of a "desperate stunt" to capitalize on the leak of Democratic emails by Wikileaks.

The developments highlight the unusually prominent role U.S. law enforcement and intelligence agencies have played in a contentious election and an ongoing debate about how public they can or should be about their inquiries.

FBI Director James Comey, a Republican appointed by President Obama, touched off an outcry from Democrats last week when he alerted Congress that agents had found other emails that could be linked to an inquiry into Clinton's use of a private email server when she was Secretary of State, effectively re-opening an investigation he had closed in July.

Associated Press
Court says Canada spy agency illegally kept data
Friday, 04 November 2016
Byline: Rob Gillies

Toronto - A Canadian court ruled Thursday that Canada's spy agency illegally kept phone numbers and email addresses of people they were not directly investigating over a 10-year period and wasn't forthright with judges who authorized the intelligence gathering.
Federal Court Justice Simon Noel said the Canadian Security Intelligence Service should not have kept the information since it was not directly related to threats to Canada's security. The data involves the phone numbers, email address or IP addresses of family members or friends of those the spy agency investigates. The spy agency called it "associated data."

CSIS said it used metadata -- information associated with a communication, such as a telephone number or email address -- but not the message itself. It said the program has been in place since 2006.

Spy Service director Michel Coulombe said they have halted logging, storing, and analyzing the data in question and said he "deeply" regretted the judge's findings about breach of "duty of candor." Coulombe stressed all data collection was done under warrant. He noted the issue is the retention of non-threat related data.

Canadian Public Safety Minster Ralph Goodale said he takes it seriously the spy agency was not forthright with the courts and said he would talk to senior executives of the spy agency. Goodale noted

the laws that govern the spy agency are 30 years old and need to be updated to reflect new technologies.

"Justice Noel did not dispute the potential value of "associated data" to the important work CSIS does in this challenging world, but he could not find existing legislative authority permitting its retention and use," Goodale said in a statement.

News of the spy agency program comes as the provincial Quebec government announced they are calling a public inquiry into police surveillance of journalists amid revelations various forces in the province monitored reporters' phones. The province's two largest police forces said earlier this week that they had monitored the phones of six prominent journalists in 2013.

The Local (Switzerland)
Malware used to spy on Iran talks in Geneva
Friday, 04 November 2016
Byline: Staff report

Geneva - A large number of computers at a Geneva hotel that hosted delicate Iranian nuclear talks last year were infected with malware used for espionage, Swiss prosecutors said on Thursday.
The Swiss Attorney General's office (OAG) however said it had closed its investigation, since it had failed to determine who was behind the spying.

Swiss investigators launched a probe in May last year based on "suspicion of illegal intelligence services operating in Switzerland," searching a hotel that hosted the nuclear talks and seizing computer equipment.

Those talks, which were held at a range of luxury hotels in Switzerland and Austria, concluded on July 14th 2015 with a landmark deal to rein in Iran's nuclear programme in exchange for the lifting of international sanctions.

The agreement between Tehran, Washington and five other major powers came into force in January.

Israel, which was vehemently opposed to the nuclear deal, was accused of espionage after a Russian-based security firm said a computer worm widely linked to the Jewish State was used to spy on the negotiations.

Israel flatly denied the accusations.

"Investigations revealed that a significant number of computers (servers and clients) at a hotel in Geneva had been infected with a form of malware," the OAG said in a statement Thursday, without divulging the name of the hotel.

"This malware was developed for the purposes of espionage, and is basically used to gather data from the computers infected," it said.

Investigators had however turned up "no evidence as to the identity of the perpetrators," it said.

"Accordingly, although there is evidence of criminal activity, it cannot be attributed to specific persons," OAG said, explaining why it had decided to close the case.

NBC News
White House Readies to Fight Election Day Cyber Mayhem
Friday, 04 November 2016
Byline: Multiple reporters

New York - The U.S. government believes hackers from Russia or elsewhere may try to undermine next week's presidential election and is mounting an unprecedented effort to counter their cyber meddling, American officials told NBC News.
The effort is being coordinated by the White House and the Department of Homeland Security, but reaches across the government to include the CIA, the National Security Agency and other elements of the Defense Department, current and former officials say.

Russia has been warned that any effort to manipulate the actual voting or vote counting would be viewed as a serious breach, intelligence officials say.

"The Russians are in an offensive mode and [the U.S. is] working on strategies to respond to that, and at the highest levels," said Michael McFaul, the U.S. ambassador to Russia from 2012 to 2014.

Officials are alert for any attempts to create Election Day chaos, and say steps are being taken to prepare for worst-case scenarios, including a cyber-attack that shuts down part of the power grid or the internet.

But what is more likely, multiple U.S. officials say, is a lower-level effort by hackers from Russia or elsewhere to peddle misinformation by manipulating Twitter, Facebook and other social media platforms.

For example, officials fear an 11th hour release of fake documents implicating one of the candidates in an explosive scandal without time for the news media to fact check it. So far, document dumps attributed to the Russians have damaged Democrats and favored Trump.

The Russians "want to sow as much confusion as possible and undermine our process in ways they've done elsewhere," said a senior Obama administration official. "So this is to make sure that we have all the tools at our disposal and that we're prepared to respond to whatever it is that they do."

"We need to be prepared on every front, not just technical but messaging, and so on," the official added, saying the details were classified. "Because any reporting irregularity could be incredibly disruptive. ... They can cause tremendous chaos, and by the time we are able to attribute, the damage may have already been done."

Officials were reluctant to discuss how they might be respond to such "influence operations," other than to say they will make efforts to counter misinformation and keep open communication nodes.

The U.S. intelligence community and the Department of Homeland Security assess that it would be extremely difficult for even a nation-state actor to alter actual ballot counts or election results by cyber-attack, a second senior administration official told NBC News.

"This assessment is based on the decentralized nature of our election system in this country and the number of protections state and local election officials have in place," the official said. "States ensure that voting machines are not connected to the Internet, and there are numerous checks and balances as well as extensive oversight at multiple levels built into our election process."

However, a Department of Homeland Security official said, other possible hacks pose "the potential for causing confusion and misperception" around the election.

For example, "Somebody could tamper with voter registration information or unofficial election night reporting."

While multiple intelligence officials told NBC that they have no specific warning about an Election Day attack, they also say they consider the massive and sophisticated internet disruption of Friday, Oct. 21, a potential dry run.

The "distributed denial of service" attack on equipment provided by the company DYN, which took down popular internet sites like PayPal and Amazon for hours, "had all the signs of what would be considered a drill," said Ann Barron-DiCamillo, former director of Homeland Security's computer emergency readiness team.

If a similar attack began unfolding on Election Day, DHS would work with big internet providers such as Comcast (owner of NBC Universal) and Verizon to try to mitigate it, Barron-DiCamillo said. Since most of the internet is owned by private companies, the government relies on the private sector to help stop attacks, she said.

As is standard for major national events, all six federal cyber centers will be up and running, closely monitoring network traffic and hunting for malware.

"Given (the Russians') past behavior in other contexts, we understand the way they like to go about potentially causing confusion and so we want to make sure that we are mitigating that potential," the DHS official said.

A current Obama administration national security official said that a White House working group has been watching Russia's apparent intervention in other foreign elections with growing concern.

A recent case study, the official said, was the October 16 parliamentary election in Montenegro, a small Balkan nation straddling East and West.

The incumbent Democratic Party of Socialists narrowly won, but fell short of an absolute majority after facing stiff and well-financed opposition from a pro-Russian coalition that opposes the country's proposed membership in NATO -- a position also held by Putin.

In the run-up to the election, U.S. officials believe Russia secretly funneled money to opposition parties and either set up or co-opted friendly media outlets and "influencers" to undermine the pro-West party and highlight the risks of joining NATO, the official said.

During the election, Russia launched a coordinated disinformation campaign using traditional and social media to allege widespread voting irregularities, including that dead people had been registered to vote, according to the Obama national security official. Social media networks were so bombarded with complaints and accusations that Montenegro ordered telecom operators to temporarily shut down WhatsApp, Viper and similar messaging apps, creating even more questions about the election, the official said.

A network of anti-censorship bloggers also reported that the website of Montenegro's top election observation NGO, the Center for Democratic Transitions (CDT), was knocked out for part of Election Day, raising concerns among U.S. officials about Russian interference.

Montenegro's state election commission released the final results Oct. 29 -- and certified the pro-NATO party's win -- despite protests by the pro-Russian opposition party, which cited the very irregularities the U.S. blames on Russia as reason to doubt the vote totals.

"It's the kind of thing that we are anticipating that they will try here," the official said. "But they will target whatever they can -- voting infrastructure, putting out false stories about the Democratic Party intentionally manipulating the results. That's what they do."

Montenegro's leaders publicly accused Russia of meddling in the election. Russian officials and opposition party members denied any interference, but Russia's foreign minister said NATO was being "irresponsible" for supporting admission for Montenegro, which could come as soon as Spring 2017.

Russia has also denied any involvement in recent hacks of U.S. political groups and operatives.

Vice News Canada
There's A Secret Canadian Spy Database That We Just Found Out About
Friday, 04 November 2016
Byline: Justin Ling

Ottawa - The Canadian Security Intelligence Service, better known as CSIS, has found itself in trouble with the legal system once again after a federal court discovered the existence of an "illegal" database full of information on Canadians, held at a secret data centre.
The information came to light in a federal court judgement, released Thursday, that takes aim at the previously-unknown Operational Data Analysis Centre and a program whereby CSIS was storing large amounts of data that had nothing to do with its investigations.

The judgement is heavily redacted so it is difficult to determine the exact nature of the investigation, the warrants, or the data collected.

But Justice Simon Noël is unequivocal: "this retention of associated data is illegal."

His ruling outlines how the collection of the data, its storage, and the data centre itself were all part of a large program that CSIS kept under wraps.

Over the course of a normal investigation, CSIS may obtain information, intelligence, and data pertaining to an individual. The agency has the power to run through that information to determine if the person is a national security threat, relevant to an investigation, or has something to do with international affairs.

If that data--such as an email between two law-abiding individuals--isn't useful in any of those respects, CSIS is required to delete it.

Except, according to Justice Noël's ruling, that's not exactly what they were doing.

While CSIS was deleting the data, they were saving and storing the metadata from the information, but renaming it "associated data," mostly in an effort to skirt rules around data collection, and keeping it for as long as they want. This data, the court adds, was "non- threat, third-party information."

The information would be stored in the secretive Operational Data Analysis Centre, whose purpose is to "retain all data collected from investigations and warrants in order to exploit that information in ongoing and future investigations."

Metadata could include everything from your phone number and email address to your search history and GPS location.

This is big data analysis is the job of CSIS' signals intelligence sister, the Communication Security Establishment, but not in CSIS itself.

There has been virtually no reporting on the Operation Data Analysis Centre since its inception in 2006. The only online mentions of the centre come from a now-deleted job post on the CSIS website, and a LinkedIn page for a former manager of the centre.

The LinkedIn page refers to it as "the CSIS centre of excellence for big data exploitation."

"The end product [of this program] is intelligence which reveals specific, intimate details on the life and environment of the persons the CSIS investigates," Noël writes. "The program is capable of drawing links between various sources and enormous amounts of data that no human being would be capable of..." the rest is redacted.

Later in his ruling, Noël underscores that this data had active uses, writing that "evidence was produced establishing that the processing and analysis of associated data has yielded some useful intelligence results. In some cases, analysis of retained data in past cases indeed contributed to new investigative leads and other useful pertinent information."

That's the process that Noël said was illegal.

The ruling added that information was still scant on the entire program, and that even the court remained in the dark about aspects of the surveillance activities.

"The court, during the hearings, learned that the program had been existence since 2006 yet it had never heard nor seen any evidence on the matter prior to the recent hearings," Noël writes.

CSIS informed the Public Safety Minister but never told the court. They kept it secret until 2011, when a lawyer for the agency made an "indirect allusion" to the data centre.

The judge concluded that "CSIS had an elevated obligation to inform the Court of the use it was making of non-threat-related information collected through the operation of warrants; it failed to do so."

The only official reference to the centre comes from a 2010 CSIS report which reads that the "Operational Data Analysis Centre (ODAC) provides support to the Service's operational branches by performing advanced analysis of data that is collected on subjects of investigation."

There is still much fog around exactly how CSIS goes about collecting digital information, as it does have legal authority to intercept and monitor communications--usually with a warrant--and can cooperate and deputize Canada's main signals intelligence agency, the Communication Security Establishment (CSE), to do bulk data collection.

This ruling adds context to documents obtained under access to information laws by VICE News in 2015. In those documents, which contain memoranda of understanding between CSIS and CSE, there is a 2007 agreement between the two agencies that "provide[s] for the disclosure and safeguarding of information shared between the parties." That agreement sets out a host of conditions for how to share and store information, data, and intelligence.

This isn't the first time that CSIS has gotten in trouble for pulling the wool over the court's eyes. In 2013, another federal court judge chided CSIS' efforts to get around its own domestic mandate by contracting out to CSE and the American NSA to conduct foreign surveillance. That problem was resolved after the federal government authorized international CSIS operations.

Washington Post
U.S. officials warn of Russian mischief in election and beyond
Friday, 04 November 2016
Byline: Greg Miller, Adam Entous

Washington - U.S. intelligence agencies do not see Russia as capable of using cyberespionage to alter the outcome of Tuesday's presidential election, but they have warned that Moscow may continue meddling after the voting has ended to sow doubts about the legitimacy of the result, U.S. officials said.
The assessment reflects widespread concern among U.S. spy agencies that a months-long campaign by Russia to rattle the mechanisms of American democracy will probably continue after polls close on one of the most polarizing races in recent history, extending and amplifying the political turbulence.

U.S. security officials have not ruled out Russian- sponsored disruption on Election Day. In recent weeks, officials at the Department of Homeland Security have collected evidence of apparent Russian "scanning" of state-run databases and computer voting systems. "Whether they were really trying hard to get in, it's not clear," a U.S. official said.

Still, the decentralized nature of U.S. polling would make it extraordinarily difficult to subvert a nationwide race. Instead, U.S. officials said it is more likely that Russia would use hacking tools to expose or fabricate signs of vote-rigging, aiming to delegitimize an election outcome that Republican candidate Donald Trump has said he may refuse to accept if he does not win.

"I think it's correct to say the Russians don't think they can dictate the outcome," said Rep. Adam B. Schiff (Calif.), the top Democrat on the House Intelligence Committee. But even as votes are being tallied Tuesday, Schiff said, Russian intelligence services are likely to be "looking through their troves of hacked documents and seeing what they can release."

Whether Trump or Democratic nominee Hillary Clinton prevails, Schiff said, the United States "can expect a lot more of the same in terms of cyber-malevolence and influence" from Moscow.

U.S. officials said there is still time for last-minute disruptions, even if the overall election appears relatively secure. Several officials said they fear that even an isolated operation that forces a voting system offline could erode confidence. Schiff and others said they remain worried that Moscow could dump doctored documents over the weekend that appear to expose illegality by the Clinton or Trump campaigns -- disclosures designed to create confusion among voters and be difficult to disprove before citizens cast their votes.

No forgeries have so far been identified among the thousands of files that U.S. officials believe were stolen by Russia and essentially laundered to the U.S. public and media through the WikiLeaks website.

The fact that Russia has so far refrained from altering documents or planting forgeries among the leaked emails is seen by some U.S. officials as potentially setting the stage for a more sinister plot. The media and public have come to see the WikiLeaks stockpiles as authentic, increasing the potential impact if Russia were to insert a deliberate but compelling falsehood.

Russian President Vladi-mir Putin has repeatedly denied any Russian involvement in the -election-related hacks. But those assertions have been dismissed by U.S. intelligence agencies and cybersecurity experts, with some saying that Russia engaged in sloppy tradecraft or seemed not terribly concerned about covering its tracks.

Anxiety about late-election vulnerabilities has factored into the Obama administration's reluctance so far to retaliate against Russia.

The White House has opted against authorizing any countermeasures despite high confidence across U.S. spy agencies that Russia alone orchestrated the digital theft of thousands of sensitive documents posted online in recent months by WikiLeaks. The releases have included hacked files of the Democratic National Committee and emails of Clinton campaign chairman John Podesta, among others.

The White House has been weighing countermeasures for months but worried that retaliating before the election would give Moscow time to inflict more direct damage in the waning days of the campaign.

"Escalation in the cyber- realm can happen quickly," a senior U.S. official said. Those urging restraint say they believe the Russian threat would be diminished after Election Day. Officials said the White House is

also reluctant to take decisions on an escalation that could have profound implications for the next president.

U.S. officials said the options under consideration include kicking more suspected Russian intelligence officers out of the United States, imposing new economic sanctions against Russian entities tied to the alleged hacking and potentially launching cyberattacks on Russian computer systems. Obama used cyberweapons to hobble Iran's nuclear program early in his first term but has been reluctant to go down that road again, aides say.

The administration's decision could depend on what the Russians do in the coming days. An election-disrupting attack would probably trigger a more aggressive U.S. response, according to officials. U.S. officials say the stakes have been made clear to Moscow.

The election-related tensions are part of a broader escalation in the level of antagonism between the United States and its former Cold War adversary. The two countries are fighting a proxy war against each other in Syria, are competing for influence elsewhere in the Middle East and are at odds over Russian intervention in Ukraine.

The hack of the DNC was blamed on Russia by cybersecurity experts and U.S. officials the moment it was publicly disclosed in June. The administration formally went public with its case last month, issuing a statement from Director of National Intelligence James R. Clapper Jr. and Homeland Security Director Jeh Johnson concluding that intrusions were authorized by "Russia's senior most officials."

Even so, there is still disagreement among some agencies and analysts over Moscow's objectives. The White House has maintained that it does not believe Russia's operations have been aimed at delivering an election win for Trump, who has praised Putin and argued there is no evidence of Russian involvement in the hacks -- a position at odds with what he has been told in classified briefings. The operations could be a more general effort to embarrass the United States and disrupt democratic institutions.

Clinton has said that Russia is seeking to ensure her defeat, a contention some U.S. intelligence officials say they believe is supported by the one-sided nature of the leaks. U.S. officials have speculated that Putin harbors personal animosity toward Clinton, believing that while serving as secretary of state she helped incite mass protests in Moscow that embarrassed the former KGB operative.

Even if there are no further election-related disruptions and Clinton emerges victorious, some U.S. officials believe that Russia has already accomplished many of its goals.

"They've weakened Secretary Clinton by dumping information from her campaign manager and others," Schiff said. The leaks have exposed infighting between Clinton and her former Democratic opponent, Sen. Bernie Sanders of Vermont, forced the resignation of the DNC chief and -- perhaps most

importantly -- cast Russia and its capacity to inflict damage as an ominous figure looming over the 2016 campaign.

"They enjoy being the subject of discussion in an American election," Schiff said. "It enhances their prestige in a bizarre way that they're considered a player. This is also their way of payback, and I think they are delighting in that."

CNN.com
State Department releases new batch of Hillary Clinton emails (Canada)
Friday, 04 November 2016
Byline: Laura Koran, Tom LoBianco

Washington - The State Department released its latest batch of emails from the FBI's investigation of Hillary Clinton's private email server Thursday, with just five days until the election.
The 1,280 pages of emails that were produced under court order include mostly administrative correspondence and duplicates of previously released material. But the batch also includes new correspondence from Clinton's 2010 clean-up tour amid the stunning WikiLeaks release of diplomatic cables.

A series of largely redacted emails from 2010 include Clinton's discussions of how she will approach world leaders, as well as how hard she should go after WikiLeaks founder Julian Assange. The newest emails from Clinton were released by the State Department while Assange continued his extended bombardment of the Clinton campaign with regular releases from campaign chairman John Podesta's hacked emails.

In a Dec. 2, 2010, top aide Huma Abedin wrote to Clinton that an ally had suggested Clinton say, "We view this not as a 'clever game' of wiki leaks but rather as a 'criminal act' against the United States of America. He might think this is a clever game today but when he is prosecuted and if convicted he will move from being a clever cyber thief to a convicted criminal -- and will find out that's a whole different kind of game."

Assange has been in asylum at the Ecuadorean Embassy in London for four years, and has blamed Clinton in part for his seeking asylum. Democrats have accused Assange and the Donald Trump campaign of coordinating the release of the Podesta emails with Russia, but Assange told Russia Today that the Russian government was not the source of the emails.

WikiLeaks' release of more than 250,000 diplomatic cables in 2010 -- with stark and cutting assessments of foreign leaders -- created a massive problem for Clinton as she played clean-up in her role as secretary of state. Emails released by the State Department Thursday detail some of the behind-the-scenes scramble inside her office.

A Nov. 26, 2010 email about her planned call with French Foreign Minister Michele Aliot-Marie is largely redacted, but includes some background, including bracing for "the first of several articles" that Le Monde was set to publish from the WikiLeaks cables.

A Nov. 27, 2010 from Huma Abedin to Clinton shows them bracing for the impact from the New York Times' publication of WikiLeaks material dealing with the U.S. relationship with Canada.

"Two cables set for release contain especially sensitive information on counterterrorism and intelligence sharing. The depth of bilateral cooperation detailed in the cables may be controversial for Canadians," Abedin wrote in the email.

The latest release follows a compromise agreement reached this September in a Freedom of Information Act lawsuit. The agreement paved the way for at least 2,900 pages of Clinton's emails to be reviewed ahead of November 8.

None of the new emails contained information marked as classified or newly upgraded to classified, but 18 were near duplicates that included a previously-released email that had been upgraded when originally released.

The State Department was initially tasked with processing 1,050 pages out of about 5,600 work- related emails before the election as part of an order in a separate FOIA lawsuit. But attorneys for the State Department and VICE News reporter Jason Leopold agreed to an accelerated release before the election.

After an initial review of the documents turned over by the FBI, the State Department concluded a "significant number" of the 5,600 work-related emails were duplicates or near-duplicates of emails already released to the public, and therefore will not be subject to re-release.

Clinton turned over approximately 55,000 pages of her emails in early 2015. Those were processed and produced to the public, with redactions, between May 2015 and March 2016.

An additional 350 pages are scheduled to be released Friday.

Reuters
FBI fear of leaks drove decision on emails linked to Clinton: sources
Friday, 04 November 2016
Byline: Staff report

Washington - FBI Director James Comey was driven in part by a fear of leaks from within his agency when he decided to tell Congress the FBI was investigating newly discovered emails related to Hillary Clinton, law enforcement sources said on Thursday.

The examination of the email traffic is now being carried out under the tightest secrecy by a team at Federal Bureau of Investigations headquarters in Washington, the sources said, requesting anonymity because of the inquiry's sensitivity.

Several sources said it was unclear whether the FBI would make any further public disclosures about its latest review before Tuesday's presidential and congressional elections. Two sources said such disclosures were unlikely.

Another source, recently in contact with top investigators, said: "It depends on how it goes and what they find." The source said that, as of Thursday, "nobody really knows" whether the FBI will have anything further to say before the election.

Dropping like a bombshell on the U.S. presidential campaign, Comey's disclosure last Friday in a letter to senior lawmakers just days before the elections raised questions about his motives and drew criticism from some over his timing.

Comey disclosed that the FBI was looking at emails as part of a probe into Clinton's use of a private email system while secretary of state, without describing the emails' content or how long the inquiry might take. The FBI normally does not comment on ongoing inquiries.

The latest emails examination was moving forward "expeditiously," said one source close to the review.

The new emails turned up as FBI investigators were examining electronic devices used by former Democratic Representative Anthony Weiner in connection with an alleged "sexting" scandal. Weiner's estranged wife, Huma Abedin, is a Clinton confidante.

Two law enforcement sources familiar with the FBI's New York Field Office, which initially discovered the emails, said a faction of investigators based in the office is known to be hostile to Hillary Clinton. A spokeswoman for the FBI's New York office said she had no knowledge about this.

Democratic Party sources said such a faction was likely responsible for a recent surge in media leaks on alleged details of an ongoing FBI investigation of the Clinton Foundation.

The FBI has made preliminary inquiries into Clinton Foundation activities and alleged contacts between Trump and associates with parties in Russia, according to law enforcement sources. But these inquiries were shifted into low gear weeks ago because the FBI wanted to avoid any impact on the election.

The FBI previously had spent about a year investigating Clinton's use of the unauthorized server at her home in Chappaqua, New York, instead of the State Department system after classified government secrets were found in some of her emails.

Comey had said in July that while there was "evidence of potential violations of the statutes regarding the handling of classified information, our judgment is that no reasonable prosecutor would bring such a case."

The Guardian (London)
Edward Snowden calls Canada police spying a 'radical attack' on journalists
Friday, 04 November 2016
Byline: Ashifa Kassam

Toronto - Edward Snowden is calling for the resignation of Montreal's police chief, amid allegations that police forces in the Canadian province secretly monitored the phones of at least seven journalists. Snowden spoke at Montreal's McGill University, after news broke that police in the city had spent five months tracking the phone of a prominent journalist in order to identify his sources.

The scandal deepened on Wednesday after Québec provincial police admitted they had obtained warrants in 2013 to spy on another six journalists with the aim of ferreting out media leaks within the police force.

Speaking via video link to a packed auditorium, the NSA whistleblower described the police actions as a "radical attack on the operations of the free press" and wondered whether the law was beginning to fail in its role as a guarantor of rights.

Montreal police have defended their actions, claiming that it was an exceptional situation. The surveillance was part of an investigation into allegations that police officers in the drugs and street gangs unit had fabricated evidence. Five officers were arrested over the allegations this summer.

After police detected contact between one of the officers under investigation and La Presse journalist Patrick Lagacé, they obtained warrants to track Lagacé's iPhone. Police actions were aimed at investigating police officers, not Lagacé, Montreal police chief Philippe Pichet said on Monday.

"We are very aware of the importance of freedom of the press," said Pichet. "But on the other hand, there were criminal allegations against a police officer ... and we have a job to do."

Echoing a call by some Montreal city councillors, Snowden suggested the police chief should resign. "Rather than the police chief saying 'all right this was clearly something that went too far and regardless of whether or not I authorised this operation, I recognise that to restore trust I need to re- establish the basis of accountability ... for that reason I have chosen to resign.' We don't see the mayor calling for that, we don't see the local premier calling for that."

The story, said Snowden, fits a broader narrative of governments masking their own actions as they peer into the lives of private citizens. "This inverts the traditional dynamic of private citizen and public officials into this brave new world we're facing of private officials and public citizens," he said.

On Thursday, the Québec government said it would launch a full public inquiry into the affair. "We consider that it's important for the public of Québec to trust their public institutions," Stéphanie Vallée, the province's justice minister, told reporters.

Her comments came after Philippe Couillard, Québec's premier, announced that the government would look into procedures at the province's three major police forces and seek to make it harder for police to obtain a search warrant to monitor journalists.

The scandal was put to Justin Trudeau, the country's prime minister, at a news conference on Thursday. "Obviously I think that the troubling stories - troubling for all Canadians - coming out of Québec and of this situation will lead to reflection on how we must and can continue to ensure protection of the press and their rights," he said.

His government had reached out to the Royal Canadian Mounted Police and the Canadian Security Intelligence Service this week to confirm that nothing of the sort was taking place at the federal level. "We have actually strong safeguards and protections in place to protect the freedom of the press in the course of business conducted by CSIS and the RCMP," he said. "And I can confirm those safeguards are still very much in place and consistent with the values and concerns this government has and that Canadians have."

Speaking to the Guardian earlier this week, the Canadian Journalists for Free Expression noted that police had said they had not broken any laws in tracking journalists. "That's the worst part of this thing. You can't even make the argument that this is just a few bad apples because it was authorised by a justice of the peace. This is the system as it's supposed to work," said Tom Henheffer of the organisation. "Which just goes to show that the whole system is broken."

The Guardian (London)
'The FBI is Trumpland': anti-Clinton atmosphere spurred leaks, sources say
Thursday, 03 November 2016
Byline: Spencer Ackerman

New York - Deep antipathy to Hillary Clinton exists within the FBI, multiple bureau sources have told the Guardian, spurring a rapid series of leaks damaging to her campaign just days before the election. Current and former FBI officials, none of whom were willing or cleared to speak on the record, have described a chaotic internal climate that resulted from outrage over director James Comey's July decision not to recommend an indictment over Clinton's maintenance of a private email server on which classified information transited.

"The FBI is Trumpland," said one current agent.

This atmosphere raises major questions about how Comey and the bureau he is slated to run for the next seven years can work with Clinton should she win the White House.

The currently serving FBI agent said Clinton is "the antichrist personified to a large swath of FBI personnel," and that "the reason why they're leaking is they're pro-Trump."

The agent called the bureau "Trumplandia," with some colleagues openly discussing voting for a GOP nominee who has garnered unprecedented condemnation from the party's national security wing and who has pledged to jail Clinton if elected.

At the same time, other sources dispute the depth of support for Trump within the bureau, though they uniformly stated that Clinton is viewed highly unfavorably.

"There are lots of people who don't think Trump is qualified, but also believe Clinton is corrupt. What you hear a lot is that it's a bad choice, between an incompetent and a corrupt politician," said a former FBI official.

Sources who disputed the depth of Trump's internal support agreed that the FBI is now in parlous political territory. Justice department officials - another current target of FBI dissatisfaction - have said the bureau disregarded longstanding rules against perceived or actual electoral interference when Comey wrote to Congress to say it was reviewing newly discovered emails relating to Clinton's personal server.

Comey's vague letter to Congress, promptly leaked by Republican congressman Jason Chaffetz, said the bureau would evaluate communications - subsequently identified as coming from a device used by disgraced ex-congressman Anthony Weiner, whose estranged wife Huma Abedin is a Clinton aide - for connections to the Clinton server. Comey's allies say he was placed in an impossible position after previously testifying to Congress it would take an extraordinary development for him to revisit the Clinton issue. Throughout the summer and fall, Trump has attacked the FBI as corrupt for not effectively ending Clinton's political career.

A political firestorm erupted, with Comey and the bureau coming under withering criticism, including a rebuke on Wednesday from Barack Obama. Even some congressional Republicans, no friends to Clinton, have expressed discomfort with Comey's last-minute insertion of the bureau into the election.

The relevance of the communications to the Clinton inquiry has yet to be established, as Comey issued his letter before obtaining a warrant to evaluate them. Clinton surrogates contend that Comey has issued innuendo rather than evidence, preventing them from mounting a public defense.

Some feel Comey needs to address the criticism and provide reassurance that the bureau, with its wide-ranging investigative and surveillance powers, will comport itself in an apolitical manner. Yet since Friday, Comey has maintained his silence, even as both Clinton and Trump have called for the bureau to disclose more of what it knows.

Leaks, however, have continued. Fox News reported on Wednesday that the FBI is intensifying an investigation into the Clinton Foundation over allegations - which both the foundation and the Clinton camp deny - it traded donations for access to Hillary Clinton when she was secretary of state. The Wall Street Journal reported that justice department officials, who have been considering FBI investigation of the issue since 2015, considered the allegations flimsy.

The leaks have not exclusively cast aspersions on Clinton. Paul Manafort, Trump's former campaign manager, is the subject of what is said to be a preliminary FBI inquiry into his business dealings in Russia. Manafort has denied any wrongdoing.

The Daily Beast reported on Thursday on ties between Trump surrogate Rudy Giuliani, the former New York mayor, and the FBI's New York field office, which reportedly pressed the FBI to revisit the Clinton server investigation after beginning an inquiry into Weiner's alleged sexual texting with a minor. The website reported that a former New York field office chief, highly critical of the non-indictment, runs a military charity that has received significant financial donations from Trump.

Comey's decision to tell the public in July that he was effectively dropping the Clinton server issue angered some within the bureau, particularly given the background of tensions with the justice department over the Clinton issue. A significant complication is the appearance of a conflict of interest regarding Loretta Lynch, the attorney general, who met with Bill Clinton this summer ahead of Comey's announcement, which she acknowledged had "cast a shadow" over the inquiry.

"Many FBI agents were upset at the director, not because he didn't [recommend to] indict, but they believe he threw the FBI under the bus by taking the heat away from DOJ [Department of Justice]," the former bureau official said.

All this has compounded pressure on Comey, with little end in sight.

Jim Wedick, who retired from the bureau in 2004 after 35 years, said that if Clinton is elected, she and Comey would likely to find a way to work together out of a sense of pragmatism. He recalled both his own occasional clashes with federal prosecutors and Bill Clinton's uneasy relationship with his choice for FBI director, Louis Freeh.

"Each one will find a way to pick at the other. It's not going to be good and it's not going to be pretty. But they'll both have to work with each other," he said.

The FBI would not comment for this story.

Radio Free Europe
Hackers Release More E-Mails They Say Tie Putin Aide To Ukraine Crisis
Thursday, 03 November 2016
Byline: Staff report

Kyiv - Ukrainian hackers claim to have broken into a second e-mail account linked to Vladislav Surkov, a senior aide to Russian President Vladimir Putin, releasing documents they say add to mounting evidence of the Kremlin meddling in Kyiv's affairs.
The new e-mails were obtained by RFE/RL from the hackers in advance of their public release on November 3. If authentic, they provide detail about the extent to which Surkov's office worked to set up separatist enclaves in eastern Ukraine in 2014.

The e- mails include plans that ostensibly show how associates of Surkov plotted to destabilize Ukraine's eastern Kharkiv region, researched Ukrainian politicians who openly supported weakening central power in a bid to exploit the country's political divisions, and helped establish the leadership of separatist groups in the Donetsk and Luhansk regions.

They indicate that, in one case, a draft law on an economic zone in eastern Ukraine purportedly written by Surkov himself was sent to the office of an opposition lawmaker and later introduced in the Ukrainian parliament.

The new release comes one week after an initial batch of e-mails from an inbox allegedly associated with Surkov, a longtime Putin aide who is the point man for Ukraine in his administration.

Analysts say they demonstrate careful planning by Russia ahead of the forcible annexation of Crimea in March 2014 and a direct Russian role in fomenting anti-Kyiv actions in the Donetsk and Luhansk regions, which led to a war that has killed more than 9,600 people since that April and persists despite Western-brokered cease-fire deals.

In both cases, the e-mails were released by a group of Ukrainian "hacktivists" who call themselves the Cyber Alliance.

On November 3, the Cyber Alliance posted a video on YouTube in which a character in a trademark mask of the hacker group Anonymous takes credit for hacking accounts in Surkov's office and warns, "This is just the beginning."

Independent international analysts and Ukraine's domestic Security Service, the SBU, have said many of the e-mails in the first group appear authentic, but there were doubts about some of the documents. Several people whose correspondence with Surkov was included in the leak have confirmed they sent the messages to Surkov released by the hackers.

The Kremlin has not explicitly called the e-mails or attached material fraudulent but has sought to cast doubt on their authenticity. Putin's spokesman, Dmitry Peskov, said of one unspecified text that Surkov "doesn't use electronic mail...so someone must have sweated quite a bit to compose this document."

Surkov himself has not commented on the matter.

The e-mails released on November 3 were hacked from pochta_mg@mail.ru, a private e-mail account that uses the digital signature "Ivan Ivanov" but appears to have been managed by Surkov assistants Maria Vinogradova and Yevgenia Kudryavtseva, to whom many of the letters are directly addressed.

Vinogradova and Kudryavtseva also handled the e-mail account from the first leak. Contacted by RFE/RL's Russian Service, both declined to comment.

The pochta_mg@mail.ru account, reviewed by RFE/RL, includes 340 megabytes of data from 336 incoming messages, many addressed to Surkov himself, and 87 outgoing messages, including some that appear to have been signed by Surkov, between November 28, 2014, and September 21, 2016.

The authenticity of the newly released e-mails and documents has not yet been fully established, but Aric Toler of the open-source investigation unit Bellingcat and the Atlantic Council's Digital Forensic Lab told RFE/RL that the metadata and other aspects of the e-mails appeared genuine.

An e- mail sent to Surkov's office on April 29, 2015, by Anna Makharinskaya, an assistant to Mikhail Markelov, a State Duma member from the ruling United Russia party at the time, included a detailed plan to destabilize Kharkiv, Ukraine's second-largest city, with 1.4 million people. Neither Makharinskaya nor Markelov, who the document indicates authored the plan, could be reached for comment.

The plan -- titled Package Of Measures X -- says that "the majority of the population of the Kharkiv region adheres to opposition views toward Kyiv" and includes a proposal to create an organization called Civil Initiative that would "develop and implement a set of...actions in order to mobilize dissent [and] criticism of Kyiv authorities," as well as promoting "autonomy" for the region and establishing "a dialogue in this regard between Kharkiv and Kyiv."

But the plan appears to have fizzled if it ever got under way, according to a June 4 e-mail identified as being from Markelov. "'The Kharkov, rise up!' movement and 'destabilization rallies and actions' have become "irrelevant," the author wrote, using the Russian spelling for the city name.

Among Kharkiv's youth there is growing support for the ideas "'Ukraine is Europe,' 'Russia invaded Ukraine,' 'Kharkiv is Ukraine,' etc.," the author continued, adding that among pro-Russian activists it is believed that "Russia has abandoned us."

The developments described in those e-mails seems to align with events and attitudes in Kharkiv in 2015. In the months following the pro-Western Euromaidan protests in Kyiv, which drove Russia-friendly President Viktor Yanukovych from power in February 2014, Russia-backed separatists rallied for a "Kharkiv People's Republic," storming government offices like their counterparts in Donetsk and Luhansk, and a group calling itself Kharkiv Partisans targeted pro-Kyiv groups in a bombing campaign that killed several people, according to Ukrainian authorities.

Ultimately, the uprising in Kharkiv failed and the city remains under Ukrainian control today -- while Donetsk and Luhansk are held by the Russia-backed separatists.

Other e- mails included in the November 3 release indicate that Surkov's associates devoted time to researching Ukrainian federalization -- a process for granting more power to the regions, weakening the central government in Kyiv. Many of the e-mails in the account contain what appear to be briefings from his assistants on legislation in Ukraine's parliament, the Verkhovna Rada, and news reports about the conflict in eastern Ukraine.

The e-mails suggest Vinogradova and Kudryavtseva were used to pass correspondence between Surkov and leaders of the separatists in Donetsk and Luhansk. Russian Aleksandr Kazakov, an aide to Donetsk separatist leader Aleksandr Zakharchenko, features prominently in the e-mails, writing to Vinogradova with several requests to pass on messages to Surkov. In one, addressed directly to Surkov, an author identified as Kazakov begs for a meeting to ask about Surkov placing him on "unpaid leave."

On December 15, 2015, an unidentified sender sent a list with proposed replacements for the heads of so-called "ministries" in what separatists describe as the "Luhansk People's Republic." It included the names and resumes of possible candidates to replace 13 officials but not the the self-declared "prime minister," Igor Plotnitsky.

There is also correspondence apparently involving European officials.

In a series of e-mails that appear to have been sent from official government e-mail accounts in April and May 2015, an author identified as Steffen Thomas, who is listed on the official German Bundestag website as state secretary at the Federal Ministry of Finance, discusses with Russian Deputy Finance Minister Aleksei Moiseyev the possible resumption of banking services in the separatist-controlled areas of Donetsk and Luhansk.

Banking services in those parts of the Donetsk and Luhansk regions remain cut off today.

Times of Israel
Israeli hackers show light bulbs can take down the internet
Friday, 04 November 2016
Byline: Gavin Rabinowitz

Jerusalem - A team of researchers at Israel's Weizmann Institute of Science has shown how hackers can use the simplest of household devices, like light bulbs, to potentially take down sections of the internet or launch a full-scale attack on a country's infrastructure.
The researchers focused on hacking into ordinary devices which are connected to the internet, the so-called "Internet of Things," to show how easy it is to take control of the devices and employ them for the kind of distributed denial of service (DDoS) attack that took down wide swathes of the internet last month for several hours.

The experiment, carried out by four researchers, Eyal Ronen, Colin O'Flynn, Adi Shamir and Achi-Or Weingarten, focused on simple Philips Hue wifi-connected smart bulbs and showed how the bulbs can "infect each other with a worm that will spread explosively over large areas in a kind of nuclear chain reaction."

"The attack can start by plugging in a single infected bulb anywhere in the city, and then catastrophically spread everywhere within minutes," the researchers' paper said.

The team managed to remotely infect the first light bulb by exploiting a weakness in the ZigBee Light Link protocol, the wireless language that everyday devices use to connect to one another.

In one experiment they flew a drone up to an office building that houses several well-known Israeli security companies and managed to transmit an infected key to a light bulb. Soon dozens of light bulbs were "kidnapped" and "crying for help" flashing SOS.

In another experiment the team drove by a building in the Weizmann Institute and managed to take control of the lights from a distance of 70 meters.

"We used only readily available equipment costing a few hundred dollars, and managed to find this key without seeing any actual updates," they wrote.

By only taking control of the light bulbs, they warn that hackers could permanently disable, or "brick," these devices, jam wireless networks, attack and overload an electric grid or even possibly cause epileptic seizures on a large scale by "repeatedly flashing the lights at the right frequency."

And they warn that this is only the beginning of the problem. "Within the next few years, billions of IoT devices will densely populate our cities."

The researchers said that they had been in contact with Philips and provided technical details and suggestions for a fix. "They have already confirmed and fixed the takeover vulnerability," they wrote.

Associated Press
Swiss Prosecutors Shelve Probe Into Spying at Iran Talks
Friday, 04 November 2016
Byline: Staff report

Geneva - Swiss authorities have suspended an 18-month investigation into suspected cyber-spying during international talks on Iran's nuclear program last year, saying they have turned up criminal wrongdoing but haven't found out who was behind it.
The office of Attorney General Michael Lauber says the investigation prompted by a report from Swiss intelligence authorities turned up malware "developed for the purposes of espionage" to scoop up data on many computers at a Geneva hotel. The talks in question took place at the President Wilson hotel.

Thursday's statement from Lauber's office cited evidence of criminal activity but said "it cannot be attributed to specific persons."

Kaspersky, a cybersecurity firm, announced at the time that it had uncovered the campaign, saying the malware was so sophisticated that a government must have created it.

CBC.CA
CSIS chief argues data was collected legally, but accepts court ruling
Sunday, 06 November 2016

Ottawa - The head of the Canadian Security Intelligence Service says he wants to "make it clear" the spy service was "not knowingly exceeding the scope" of its legal authority when it kept potentially revealing electronic data about people who posed no security threat over a 10-year period.
On Thursday, a Federal Court judge said the spy service was acting illegally and breached its duty to inform the court of its data-collection program, since the information was gathered using judicial warrants.

CSIS director Michel Coulombe took the unusual step of issuing an additional statement on Sunday to defend the program, saying the spy service had been collecting the data using legal warrants and retaining it based on its interpretation of the law, but that it accepted the decision of the court.

Coulombe also says that the agency briefed former public safety ministers Stockwell Day and Vic Toews about the program, and shared information with the Security Intelligence Review Committee and other government stakeholders.

But Coulombe also says those briefings might not have dealt specifically with retaining the subset of associated data that is the subject of the ruling by the court.

Coulombe said last Friday that the spy service had halted all access to, and analysis of, the data in question while it reviews the court decision.

Presse canadienne
Larouche et Lagacé n'auraient pas été mis sur écoute, dit le SPVM
Sunday, 06 November 2016
Byline: Emilie Bergeson & Louis Cloutier

Montréal - Le Service de police de la Ville de Montréal (SPVM) a réagi aux informations parues dans La Presse, samedi, en réitérant que le chroniqueur Patrick Lagacé et le journaliste Vincent Larouche n'avaient jamais été mis sur écoute.
La Presse rapportait que le SPVM a demandé et obtenu un mandat pour placer sur écoute MM. Lagacé et Larouche. Le service de police ne se serait donc pas contenté d'obtenir le droit de fouiller les relevés téléphoniques et de géolocaliser les journalistes. Le quotidien ignore cependant si ce mandat d'écoute électronique a été utilisé.

Par voie de communiqué samedi, le directeur du SPVM a maintenu que seuls les policiers faisant l'objet d'une enquête ont été sur écoute électronique. Philippe Pichet a cependant précisé que toute personne ayant communiqué avec les policiers en question a pu être entendue dans le contexte de ces

conversations. Le communiqué affublé du titre «Le SPVM dément les informations parues dans La Presse ce matin [samedi]» ne semble toutefois ni confirmer ni infirmer l'existence d'un mandat ciblant directement les journalistes.

M. Pichet, qui assure avoir agi en toute légalité, a dit vouloir demander à la cour une levée rapide des scellés sur les données concernant Patrick Lagacé, par souci de transparence.

Plus tôt samedi, le chef du Parti québécois a réclamé sa suspension, le temps que la lumière soit faite sur les deux cas de surveillance policière révélés dans la dernière semaine.

Jean-François Lisée a fait valoir que, dans la foulée des informations rapportées par La Presse, la suspension de M. Pichet, «l'un des acteurs principaux de ce qui est un manque de jugement, sinon un abus de pouvoir», devient d'autant plus nécessaire.

«À chaque jour qui passe et lorsqu'on en apprend davantage, on voit que l'une des personnes que la commission d'enquête voudra le plus voir et interroger, c'est bien le directeur Pichet et donc il faudrait l'extraire de son travail immédiatement pour ne pas entacher la preuve d'aucune façon [...] Il faut prendre cette précaution», a-t-il lancé, en entrevue avec La Presse canadienne.

Le chef péquiste a précisé qu'il demandait déjà qu'un tel geste soit posé depuis le début de la semaine. Il n'exige toutefois pas la démission du directeur du SPVM pour l'instant.

Les problèmes du SPVM

«Les problèmes du SPVM sont plus profonds que la seule identité de la personne qui le dirige présentement», a soutenu pour sa part Patrick Lagacé.

«Il y a une culture qui fait en sorte que dans le haut commandement, on se moque de la liberté de presse, on méprise les journalistes», a-t-il dénoncé, en entrevue avec La Presse canadienne.

Selon la lecture d'une déclaration sous serment et d'une autorisation judiciaire obtenues par La Presse, la police aurait eu l'autorisation de mener des écoutes électroniques auprès de M. Lagacé, de même que de Vincent Larouche.

Leurs communications privées pouvaient être interceptées, aurait écrit le juge Marc Bisson, de la Cour du Québec, dans un mandat d'écoute signé en mai dernier et valide pour 60 jours - toujours selon les informations de La Presse.

La Presse ignore cependant si les deux journalistes ont finalement été écoutés. Ils n'ont pas reçu un avis de 90 jours les prévenant qu'ils avaient été écoutés, comme le prévoit la loi.

Cette semaine, le directeur du SPVM avait déclaré devant les médias qu'il n'avait jamais été question d'écoute électronique de Patrick Lagacé dans ce dossier.

Aux yeux du chroniqueur, il est impératif de mettre en lumière le fonctionnement du SPVM au-delà «des versions roses et édulcorées des communiqués de presse».

«La seule solution à laquelle je peux penser à mon niveau, c'est de continuer à faire du journalisme», a-t-il lancé.

De son côté, Jean-François Lisée affirme qu'il revient «légalement» au premier ministre, Philippe Couillard, de suspendre Philippe Pichet - et non au maire de Montréal, Denis Coderre.

Le ministre de la Sécurité publique Martin Coiteux a écrit sur sa page Facebook en fin d'après-midi qu'il était en contact avec le maire Coderre «depuis tôt [samedi] matin».

«Tout au long de la journée, nous avons échangé sur cette situation qui me préoccupe au plus haut point. Devant les nouveaux éléments rapportés par le journal La Presse ce matin, les autorités du Service de police de la Ville de Montréal et la Ville de Montréal doivent faire preuve de la plus grande transparence dans ce dossier et poser des gestes afin de restaurer la confiance des Montréalais envers leurs institutions», a-t-il soutenu.

Commission d'enquête

Quant à Denis Coderre, il n'a pas formulé de commentaires samedi.

Le gouvernement a annoncé jeudi qu'une commission d'enquête sera mandatée pour se pencher sur la surveillance policière des sources journalistiques, après que de nouveaux cas, concernant six journalistes, eurent été révélés.

La création éventuelle d'un comité d'experts formé d'un juge, d'un membre des forces policières et d'un représentant des médias avait déjà été lancée. Ce dernier recevra tous les pouvoirs relatifs à la loi sur les commissions d'enquête, qui incluent notamment le pouvoir de contraindre les témoins.

Me Christian Leblanc a été choisi à l'unanimité par une douzaine de chefs des principales salles de nouvelles du Québec pour siéger au comité.

M. Lisée a rappelé samedi qu'il avait demandé au premier ministre que les chefs des partis de l'opposition soient consultés sur la nature du mandat et sur la période qui sera couverte par la commission, se disant déçu de ne pas avoir encore été approché en ce sens.

CBC Radio The House

Spy agency broke the law, so who should be held accountable?
Saturday, 05 November 2016

Ottawa - Public Safety Minister Ralph Goodale hasn't ruled out firing those responsible at the Canadian Security and Intelligence for illegally keeping potentially revealing electronic data it collected over a 10-year period.
"There are circumstances that would certainly go to that extreme," he told The House.

On Thursday the Federal Court ruled that CSIS illegally kept potentially revealing electronic data, breaching its duty to inform the court, since the information was gathered using judicial warrants.

Because the metadata -- which can include information like email addresses and telephone numbers contacted at a specific date or time, but not the content of the messages or calls themselves -- was not related to a security threat, it should have been destroyed.

Goodale said he's tasked the Security Intelligence Review Committee, also known as SIRC, to continue to monitor CSIS.

"The first identification here of a problem actually came from SIRC, came from their review process," Goodale said.

"They are the eyes and the ears of the Canadian public. They get full disclosure of all the details. What I am asking them to do is make sure that the information here, that court has criticized, make sure that that information is properly handled."

He also said the creation of a parliamentary oversight committee could also offer a future safeguard.

Sputnik News Service
Canadian Federal Court Exposes, Rules Illegal Database on Innocent Citizens
Saturday, 05 November 2016

Washignton - "The court concluded that the retention of associated data falls outside the CSIS's legislatively defined jurisdiction... therefore the retention of associated data is illegal," a court-issued summary of the ruling stated. The CSIS, Canada's equivalent of the US Central Intelligence Agency, has maintained a database since 2006 containing information from everyone contacted during the course of a security-related investigation, regardless of whether the information was related to the probe, according to the court. At a press conference in the nation's capital of Ottawa on Thursday afternoon, CSIS Director Michel Coulombe said the agency accepted the court's decision and had "taken immediate actions to respond," according to follow up reports in Canadian media. By issuing the ruling, the public was informed for the first time of a program that had operated in secret for the past decade.

National Post
After trust has eroded, CSIS might get left out in the cold by ministers
Saturday, 05 November 2016
Byline: John Ivison

Column: "Trust, but verify."
Academics Craig Forcese and Kent Roach argue that this should be the maxim in the security sector when dealing with powerful state agencies like the Canadian Security Intelligence Service and the RCMP.

But trust in Canada's security services is thin on the ground, after the news Thursday that a CSIS unit illegally kept data deemed unrelated to national security threats.

Public Safety Minister Ralph Goodale said Friday that a Federal Court decision by Justice Simon Noel, who found CSIS has "breached, again, the duty of candour it owes the court," is timely because the Liberals are in the midst of reviewing Canada's national security laws.

The latest hit to the spy agency's reputation is unlikely to endear it to this government, and makes it more likely the Liberals will roll back what Forcese and Roach call the "outer limits" of C-51, the anti-terror legislation introduced last year by the Conservatives.

The Federal Court ruling found CSIS illegally kept electronic data, breaching its duty to inform the court -- a duty it had since the information was gathered using judicial warrants. The metadata -- information like email addresses and telephone numbers, though not the contents of actual emails and telephone calls -- was unrelated to national security threats, the judge concluded, and should have been discarded.

As Noel indicated, it was not the first time CSIS has fallen foul of the courts.

In 2013, another Federal Court justice, Richard Mosley, hammered CSIS for deliberately keeping the court in the dark about outsourcing its spying on Canadians abroad to foreign agencies. On that occasion, he said CSIS purposely misled him when he granted it numerous warrants to intercept the electronic communications of Canadians suspected as domestic security threats.

Even before that, both Mosley and Noel had lambasted CSIS for providing inaccurate information to the court. In the Mohamed Harkat case, Noel criticized the lack of candour coming from CSIS.

Judicial opinion is particularly pertinent since the new anti-terror legislation gave CSIS the power to ask judges to approve warrants, even if preventative measures breached rights or freedoms otherwise protected by law.

CSIS chief Michel Coulombe said last March that the agency has used its new threat disruption powers (previously the agency could gather information about suspected terror plots but not disrupt them). However, he said CSIS had not sought judicial approval in any of those instances.

Critics of C-51 suggest the Liberals should roll back the provision, removing the ability to seek judicial warrants.

Given the fact that the country's foremost jurists on national security law have repeatedly censured the spy agency for deliberately misleading them, it seems a good bet that the government will decide to shorten CSIS's leash.

Yet Goodale did not rule out a change to the law to allow CSIS to keep the information ruled offside by the court. "This is an issue that I think needs to be examined in the context of our national security review," he said. "I want to hear the professional advice on both sides ... Our security agencies to be effective in keeping Canadians safe. At the same time, what the agencies do needs to be in accord with the law and with the Constitution."

Phil Gurski, a former CSIS analyst, said the metadata was retained for a reason - - namely to identify people involved with, or sympathetic to, terror groups. "It was a legal opinion that this was illegal because the service is only allowed to retain information that is strictly necessary. I'm saying that it is strictly necessary and the data would inform future investigations."

Gurski suggested the three-decade-old CSIS Act be updated to reflect the new threat environment, allowing the spy agency to retain metadata.

But he conceded public opinion could push the Liberals in the opposite direction. "The perception is that CSIS acted illegally and the public might say, 'Why give these guys more powers if they can't legally use the ones they have?' I hope that's not the case."

But that hope may prove forlorn. The Liberals are in the process of beefing up oversight and verification, in the form of the new parliamentary committee that will monitor CSIS's activities.

Now trust has broken down, both with the judges who issue the warrants CSIS needs and with the minister to whom it answers.

When consultations with Canadians over national security end, and the government reports back, the spies could find themselves left out in the cold.

CBC.CA
What you need to know about the CSIS metadata ruling
Saturday, 05 November 2016
Byline: John Paul Tasker

Ottawa - A Federal Court judge's ruling this week that CSIS has been illegally storing Canadians' communications data for more than a decade has shed new light on the agency's secretive data analysis program.
In his redacted ruling, Justice Simon Noël found the domestic spy agency held on to what it calls "associated data," vast amounts of data about private electronic communications obtained under warrant, long after it had decided the information was not related to a security threat.

CSIS has been storing that information for an indefinite period in an Operational Data Analysis Centre (ODAC), a shadowy part of the agency that essentially maintains a database of metadata, which includes phone numbers, email addresses and geographic coordinates.

Noël found that when it came to the ODAC, the intelligence agency did not fulfil its "duty of candour," which obligates the agency to be forthcoming with the Federal Court about its investigatory practices when seeking warrants.

The judge found that CSIS was concealing these efforts -- to collect and store vast amounts of data -- from the court, something the agency director now says is "regrettable."

Media placeholder

Is CSIS keeping the content of my communications?

At issue in this landmark ruling is not the actual content of a "communication event," which can largely be defined as a phone call or an email, but rather associated information like phone numbers, call times, date stamps and GPS data.

But that doesn't mean it's useless information, Noël writes in his judgment. Far from it.

"Metadata, on its own and processed through aggregation and analysis, can provide intimate insights into the lifestyle and personal choices of individuals; it is not an innocuous kernel of information."

What is the Operational Data Analysis Centre?

It's hard to say, exactly, because Noël, who had been issuing warrants to CSIS to allow them to collect this data through "intrusive methods," had no idea there was such a thing.

CSIS set up this centre in 2006 to house "non-threat, third- party information," that it obtained from service providers (largely mobile carriers and internet companies).

This, Noël ruled, is hugely problematic because warrants stipulated that information unrelated to a threat must be destroyed.

Despite those legal limits, the agency felt that information it collected was "under-utilized," because it was not sufficiently analyzed. Internally, the ODAC was billed as a "centre for excellence for the exploitation and analysis" of databases.

Most of the judge's description of the ODAC in his ruling is blacked out, but he discovered that the centre processes metadata and spits out an "end product of intelligence which reveals specific, intimate details on the life and environment of the persons CSIS investigates."

CSIS Data Privacy 20161103

This practice, Noël wrote, goes beyond CSIS's limited mandate, which restricts its activities to those that are "strictly necessary for the purpose of protecting the security of Canada."

CSIS legally acquired the data and thought it was allowed to retain it, the agency's director, Michel Coulombe, said in a press conference Thursday.

"It is now clear that the Federal Court disagrees with this interpretation."

He did concede Thursday that existing data collection practices "have proven to be an effective tool."

Coulombe also said its policies had the full backing of lawyers in the Department of Justice

"We've heard the court loud and clear," Robert Frater, chief general counsel for the Department of Justice, who attended the press conference with Coulombe, said. "We are taking steps to improve our practices and we will meet that standard."

Who knew about this operation?

CSIS told the court that it had informed Stockwell Day, who was serving minister of public safety, about the associated data collection program.

But Day refuted that claim in an interview with CBC News Network's Power & Politics. "If he is suggesting, or anybody, that they thought they told me something inappropriate was going on, yeah, I would suggest they did not."

Media placeholder

The current public safety minister, Ralph Goodale, said Friday the Security Intelligence Review Committee (SIRC) initially flagged possible problems with the collection and storage of associated data in a report tabled earlier this year.

Goodale said he only became aware of the full extent of the problem recently, when Noël filed a preliminary report "a couple of weeks ago."

"I took the immediate step of informing SIRC of the issue and asking SIRC to intervene in the situation to supervise the management of the data and to make sure that there was full compliance with the federal court's judgment," Goodale told reporters.

CSIS does not need a warrant to review Revenue Canada files

In addition to collecting and storing metadata for years, Noël also documents in his ruling how the spy agency can now obtain information from the taxman without a warrant.

"The Court no longer adjudicates applications for warrants to obtain information from the Canada Revenue Agency," he wrote.

This is part of a new trend, expanded in the former Harper government's anti-terrorism legislation, Bill C-51, which dramatically expanded information sharing among government departments. It allows CSIS to operate internationally and gives it the ability to take action to actually prevent a threat.

What happens now?

Coulombe said CSIS has halted all access to, and analysis of, the data in order to assess the "operational" impact of the ruling and to determine the way forward.

"We are working closely with the Department of Justice to make sure that we meet our obligations with the court," he added. "The trust of Canadians is essential in the fulfillment of our mandate."

Goodale said the Federal Court ruling is "timely" as it comes in the midst of the government's public consultations over the future of national security.

He has already promised to launch a parliamentary oversight committee of CSIS, a promise the Liberals made after it tacitly endorsed parts of the controversial Bill C-51.

Noël said, in the context of this ruling, "it may be time for Canadians to renew a debate regarding the mandate and functions of our domestic intelligence agency.

"It is my opinion that the CSIS Act is showing its age," the judge said of the 30-year-old legislation.

Daniel Therrien, the country's privacy commissioner, told CBC News Friday that CSIS has already reached out to his agency to propose next steps.

"At this point I can tell you that we welcome discussions on changes to CSIS policies required by the judgement. We also welcome a proposal from CSIS to meet to discuss their Privacy Impact Assessment for the Operational Data Analysis Centre and how it should be updated following the Court's decision."

CBC.CA
CSIS metadata: Ralph Goodale 'pursuing criticism' with spy agency management
Saturday, 05 November 2016
Byline: Janyce McGregor

Ottawa - Public Safety Minister Ralph Goodale suggested today that there may be consequences for the senior management of Canada's spy agency after a Federal Court decision found CSIS broke the law in failing to destroy potentially sensitive personal information.
"I take very seriously the explicit finding by [Federal Court] Justice Noel that CSIS had failed in its duty to be candid with the court," he told reporters before entering question period.

"I will be pursuing that criticism with the executive management of the service," he said.

The ruling Thursday found that the Canadian Security and Intelligence Service illegally kept potentially revealing electronic data it collected over a 10-year period, breaching its duty to inform the court, since the information was gathered using judicial warrants.

Because the metadata -- which can include information like email addresses or telephone numbers contacted at a specific date or time, but not the content of the messages or calls themselves -- was not related to a security threat, it should have been destroyed.

"Canadians need to have confidence that all the departments and agencies of the government of Canada are being effective at keeping Canadians safe, and equally that they are safeguarding our rights and freedoms, including privacy and the rule of law," the minister said.

"From the service and from the department of justice, a strong and timely remedial plan is required to reassure the Federal Court about the issue of candour."

Media placeholder

The federal government is not appealing the Federal Court ruling. Goodale said Friday he welcomed the decision.

"The court's insight and guidance are timely, coming in the midst of the public consultations on Canada's national security framework," he said, pointing out later that Canadians haven't been given a chance to be heard on privacy concerns like this until now.

SIRC will monitor compliance

The spy agency can legally intercept communications and collect third-party data associated with those communications when it's required for an investigation. But data can't be studied or kept unless it relates to a specific threat.

CSIS has blocked all access to and analysis of this data as a result of the ruling, Goodale said.

"I am asking the SIRC (Security Intelligence Review Committee) to monitor the situation carefully to ensure compliance."

The minister said this privacy breach was first raised in SIRC's 2014-15 report, which was delayed because of the election. He eventually tabled it last January.

The minister said he became fully aware of the issue when the Federal Court judgment was made available to him in preliminary form a few weeks ago.

"The law is the law and all government agencies must comply with the law of the government of Canada," he said.

CSIS Info Sharing

When asked whether anyone could be fired over this, the minister said he would discuss with CSIS executives how they might plan to respond.

"(CSIS) director (Michel) Coulombe is abundantly aware of my expectations in this matter," he said, adding later that this ruling has exposed a "serious defect" in records management that needs to be fixed.

At a hastily called news conference late Thursday to respond to the ruling, Coulombe said he deeply regrets the court's "serious concerns." The agency accepted the court's decision, he told reporters, and has "taken immediate actions to respond."

Future committee could review use

The future use and analysis of metadata are part of the ongoing national security review. While it could be useful to keep Canada safe from threats, "privacy is a fundamental Canadian value," Goodale said.

The parliamentary oversight committee the Liberals are setting up -- legislation to implement it, Bill C-22, is currently before the House -- could offer a future safeguard.

It will have "extraordinary authority," Goodale said, and unlike SIRC, could review not just past activities of security agencies but also ongoing operations.

"Timeliness is a critical concern here," the minister said.

But at an earlier press conference, two NDP MPs suggested the the new committee won't be independent enough.

The prime minister and cabinet would appoint its members and hand-pick its chair, justice critic Murray Rankin said, while controlling the information it receives and potentially blocking investigations into certain areas. Reports could be revised without notifying the public, he warned.

"Surely that's not good enough for Canada in the 21st century," Rankin said, especially with the cyber-security concerns noted by the judge in this case.

"Metadata is the new frontier for privacy protection," he said.

Media placeholder

New Democrats are proposing amendments they say would give the intended watchdog more teeth and claws.

Thursday's judgement shows that the parliamentary oversight committee needs the power to summon witnesses, compel testimony under oath and require the production of documents, Rankin said.

Public safety critic Matthew Dubé said that despite what former minister Stockwell Day said on CBC News Network's Power & Politics Thursday, the Federal Court ruling said that in 2006, the former Conservative minister was made aware of this data collection.

We have to imagine that Goodale was briefed too, Dubé said. "We want to know: what did the minister know?"

"The Liberals were elected realizing ... that there were problems with C-51, with how this was all taking place, and promised more oversight and promised more accountability," he said.

"If the minister was aware of this, and continued under the status quo that had been put in place under the previous government, that in and of itself is a problem, given what they promised."

CTV.CA
Former Ontario privacy commissioner wants CSIS metadata deleted
Saturday, 05 November 2016

Byline: Graham Slaughter

Ottawa - Information illegally held by Canada's spy agency over the course of a decade should be deleted from CSIS servers, according to Ontario's former information and privacy commissioner. Ann Cavoukian said metadata - the information included in a communication, such as a telephone number or email address - never should have been gathered because it included details on Canadians who didn't pose a security threat.

"As Justice (Simon) Noel made perfectly clear, there was no authorization whatsoever to collect that type of unrelated metadata. That was completely unanticipated, unauthorized and should never have happened," she told CTV's Power Play on Friday.

The Federal Court judge ruled that CSIS should not have kept metadata regarding people who didn't pose a direct threat to national security, and said the agency breached its duty to inform the courts of the data-collection program because the information was gathered under judicial warrants.

The ruling was made public Thursday.

Cavoukian said a major concern about metadata is that it could be crunched by sophisticated algorithms to form data profiles and help track people.

"What machine learning algorithms excel at are predictive analytics - predicting future behaviour based on the data collected, and it can paint a very, very deep, involved picture of these individuals," she said.

"That was never authorized, and that's (why) we have to ensure this information is deleted."

CSIS has not said whether it plans to destroy the information. CSIS director Michel Coulombe said Thursday that the agency had stopped all access to, and analysis of, the metadata in question as it fully assesses the court decision.

Cavoukian said the spy agency's response on Thursday "didn't address the major concerns" of the scathing ruling.

"They said, 'OK, we're not going to do it anymore.' But they didn't say we're going to destroy the 10 years of metadata that we collected, contrary to having any legal authority to do so," she said.

In his ruling, Justice Noel suggested that's it time for the federal government to revisit the CSIS Act of 1984, which he wrote is "showing its age."

A former director for Canada's CSIS watchdog echoed that call for reassessment.

"The Act is now more than 35 years old," said Jacques Shore, former director of research and investigation for the Security Intelligence Review Committee (SIRC), who now works as partner with Gowling WLG.

"Clearly with new technologies, we have to address it."

Public Safety Minister Ralph Goodale said Friday he was taking the finding "very seriously" and following up with CSIS top brass.

"(CSIS) has confirmed to me that it is taking immediate steps to address the court's decision," Goodale said. "It has blocked all access to, and analysis of, any associated data while it considers its next steps to comply."

Globe and Mail Online
Where is the review of intelligence analysis in CSIS?
Saturday, 05 November 2016
Byline: Stephanie Carvin

OpEd: Stephanie Carvin is an assistant professor of international relations at the Norman Paterson School of International Affairs at Carleton University, and a former national security analyst with the federal government
In a week dominated by headlines alleging the FBI meddling in the U.S. presidential election, and police surveillance of journalists in Quebec, Thursday's Federal Court ruling on CSIS's Operational Data Analysis Centre (ODAC) likely heightened the uncertainty many Canadians feel over the actions of our national security services.

While much of the ruling refers to data collection and retention, it also speaks to the role of intelligence analysis within the government of Canada - a topic that has thus far not received much attention in discussions surrounding the national security review process, but should.

As both the ruling and the CSIS director Michel Coulombe noted on Thursday, part of the issue surrounds the CSIS Act - a product of the early 1980s. Both the Federal Court and Coulombe noted that technology has moved on since this time. However, the issue goes further than this, especially when it comes to intelligence analysis.

Although the Macdonald Commission desired to create a civilian intelligence agency, the character of CSIS continues to reflect the organization from which it was born - the 1970s RCMP. While the focus in the Act is rightly on stopping the "bad guys," other intelligence functions of national security organizations, especially analysis, are secondary considerations.

Indeed, other than noting in Section 12(1) that the Service "shall report to and advise the Government of Canada" on national security threats, the role of intelligence analysis is barely given any consideration. There is no guidance as to how this role should be done, how intelligence should support operations or in what way advice is to be given.

Moreover, there is no formal or consistent intelligence analysis oversight - or more correctly, efficacy review. One can only speculate that had there been some form of regular review of CSIS's analytical functions, it is unlikely that ODAC's existence and activities would have been such a surprise to the Federal Court.

But this situation has led to other problems as well. For example, there is no accountability within the CSIS Executive as to the delivery of intelligence products, how those products are produced or whether those products are delivered in a timely manner.

Additionally, there is no way of knowing how intelligence products are used or if they adequately support internal operations or policy making. Furthermore, there is no way of knowing if analysts have the proper tools and training.

In fact, it is not even clear what kind of analysis CSIS should be producing. ODAC's role appears to be that of supporting operations, but there is no reason that the broader trends it uncovers cannot be used to support intelligence analysis that supports policy making.

But complicating matters is the largely haphazard structure of the Canadian intelligence community's (IC) analytical branches. There is considerable overlap between several, including the Privy Council Office's Intelligence Assessment Secretariat, the Integrated Terrorism Assessment Centre (ITAC), and CSIS's analytical branches.

While having competing perspectives can provide a plurality of views for the government to choose, the lack of review means that we do not know how well the IC manages these relationships and/or collaborates. As such, the government should take two steps as it undergoes its national security review.

First, it should support CSIS's development of innovative intelligence analysis techniques, such as data analytics. In an era of budgetary constraints and rapidly evolving threats, such techniques can help provide direction and focus of scarce resources. Even in noting its concern with ODAC's analytical activities, the Federal Court saw their value in supporting the Service's work.

This change, however, will be difficult. CSIS is an organization led by intelligence officers, many of whom are more comfortable "knocking on doors" than statistically driven trends. Although some might speculate that CSIS is anxious to jump on the "big data" wagon, this change will come as a culture shock to a largely traditional organization still governed by its Cold War mandate.

This brings us to the second step - analytical modernization must be done with appropriate oversight and efficacy review. This, as well as ensuring the quality and timeliness of analysis, should be key functions of the Parliamentary committee that the Liberal government is creating.

On Thursday, Public Safety Minister Ralph Goodale stated that he was taking seriously the concerns about CSIS's bulk data collection activities. He must also take the time to consider what CSIS's analytical role should be and ensure there is appropriate oversight and review of its activities.

After all, there are many excellent analysts in the government. Review will ensure their work helps Canada to be a safer place.

Ottawa Citizen
Clean up spy agency
Saturday, 05 November 2016

Editorial: So, Canada's spy agency has gobs of people's metadata in a secret database. Well, it's just numbers, isn't it? You know, telephone numbers and Internet IP addresses and so forth. Who cares? The justice system, to begin with. On Thursday, the Federal Court released a ruling saying that the Canadian Security Intelligence Service's retention and analysis of wide swaths of data, which had been going on for 10 years, was illegal. And CSIS hadn't bothered to inform the court of what it was doing.

This duplicity is unacceptable; keeping data you're not entitled to is a scandal that concerns all Canadians. And it's happening as a related mess unfolds in Quebec, where police have been spying on journalists, collecting their metadata, too.

The word "metadata" sounds bland. But the information CSIS kept could be pieced together to create, said Justice Simon Noël, "intimate insights into the lifestyle and personal choices of individuals; it is not an innocuous kernel of information."

Let's say your information, being scooped up by spies, shows a telephone call from your boss. Next, you telephone your mother. Then, you phone a number associated with a suicide hotline. What could be happening? It doesn't take a highly trained intelligence analyst to figure it out.

Further, CSIS has been retaining such information about people who aren't the target of an investigation -- "third-parties" like you and me. Let's say there's a legal surveillance operation underway. If the person being watched calls their second cousin, say, the cousin's data is collected, too, creating a network of information even about an innocent distant relative. (Redactions in the court ruling leave a bit murky what CSIS is actually hoarding.)

Public Safety Minister Ralph Goodale was shifty on Friday when asked if the Liberals' planned security oversight committee would have stopped this sort of spying; instead he repeated talking points. He also

refused to say how many Canadians had their data captured. Reassuringly, though, the government won't appeal the court ruling.

But here are some questions CSIS and the minister still must answer: . How many Canadians had their privacy violated in this way? . Will their data be destroyed? If not, why not? . It's claimed this data analysis has yielded valuable intelligence information. What sort of information? . Will Canada's new oversight infrastructure ever be able to stop this sort of activity? . Is anyone going to be fired for this fiasco?

It's a bad day for our intelligence services. Shame on our spies. And on our lackadaisical oversight system.

Le Devoir
Surveillance - La confiance ébranlée
Saturday, 05 November 2016
Byline: Manon Cornellier

Editorial - Pendant dix ans, le Service canadien du renseignement de sécurité (SCRS) a conservé et analysé des données associées à des personnes qui n'étaient soupçonnées de rien, mais qui avaient eu le malheur de communiquer avec des personnes légalement surveillées. Et le service l'a fait sans en informer la Cour fédérale, un des rares garde-fous contre d'éventuels abus de nos espions. Le gouvernement doit serrer la vis et vite ; la confiance des citoyens et la protection de leur vie privée en dépendent.\r\nLa nouvelle est tombée comme une tonne de briques en fin de journée jeudi. Dans un jugement catégorique, le juge Simon Noël, de la Cour fédérale, a conclu que le SCRS avait illégalement conservé certaines données personnelles et avait failli à son devoir d'en informer le Tribunal au moment d'obtenir les mandats nécessaires à la collecte d'information sur des personnes pouvant représenter une menace à la sécurité nationale.
La préservation de ces données dites connexes (ou métadonnées, comme des numéros de téléphone, adresses IP et de courriel) était illégale, parce que les personnes touchées n'étaient pas visées par les mandats, mais avaient seulement communiqué avec la personne sous surveillance. Plutôt que de détruire ces renseignements après une période déterminée, le SCRS les a versés dans une banque de données sophistiquée capable de les recouper et de dresser le portrait de leurs habitudes et de leurs réseaux.

Le Tribunal rappelle que le SCRS doit, en vertu de la loi, conserver les données uniquement " dans la mesure strictement nécessaire ", ce qui n'était pas le cas. Lors d'une conférence de presse convoquée en toute hâte, le directeur du SCRS, Michel Coulombe, a dit que le service avait cessé toute analyse et verrouillé l'accès aux données en question. Le ministre de la Sécurité publique, Ralph Goodale, a précisé que le gouvernement n'interjetterait pas appel et a déploré le manque de franchise du SCRS devant la Cour.

Mais ensuite ? La Cour n'a pas demandé de détruire ces données et personne ne sait trop ce qu'on en fera. Le plus préoccupant est que M. Coulombe espère pouvoir les conserver et que le ministre de la Sécurité publique, Ralph Goodale, n'a pas fermé la porte.

Il a noté que cette question serait mieux débattue lors des consultations publiques en cours sur " le cadre de sécurité nationale ". Le ministre a d'ailleurs relevé que le juge Noël avait suggéré de revoir la loi sur le SCRS et de l'adapter à la réalité des nouvelles technologies.

Ces consultations doivent aussi guider la révision de la Loi antiterroriste, le fameux projet C-51 adopté sous les conservateurs. Les libéraux l'avaient appuyé en promettant d'y apporter des amendements. Pourrait-on en profiter pour jeter du lest en ce qui a trait à la conservation de données connexes ? Ce serait inquiétant, car C-51 permet déjà, pour des raisons de sécurité, de vastes échanges de données au sein de l'appareil fédéral. Le SCRS n'a ainsi plus besoin de mandat pour obtenir une foule de renseignements, dont des données fiscales.

Toutes les agences de renseignement fédérales se servent de plus en plus des technologies de collecte et d'analyse de métadonnées, mais l'encadrement n'a pas suivi. Le SCRS a demandé des mandats à répétition au fil des ans sans jamais informer la Cour de ses méthodes. Pire, il a agi avec la bénédiction du ministère de la Justice, qui partageait l'interprétation qu'avait le service de ses obligations en matière de conservation de données.

C'est la deuxième fois en trois ans que le SCRS est surpris à cacher des faits à la Cour fédérale, au point où le juge Noël se demande s'il faudra l'accuser d'outrage au tribunal pour qu'il comprenne. " Dans le présent dossier,écrit-il, [le SCRS] n'a certes pas favorisé la confiance de la Cour. " Imaginez celle des citoyens !

Il revient au gouvernement d'établir des balises et les mécanismes de surveillance adéquats pour protéger la vie privée et les droits des Canadiens. Parmi les gestes à poser, il doit établir que rien ne justifie de conserver les données des gens ne posant aucune menace à la sécurité. Il doit aussi mettre à niveau la Loi sur la protection des renseignements personnels et, idéalement, modifier le projet de loi C-22 créant le futur comité de parlementaires chargé de surveiller toutes les activités de sécurité. Ce comité doit pouvoir faire enquête et rapport sans craindre l'obstruction éventuelle de ministres ou la censure du premier ministre.

Reuters
Canada's spy agency may be hobbled by ruling on data collection
Saturday, 05 November 2016

Ottawa - Canada's spy agency will not be able conduct normal operations until it assesses the effects of a court ruling that curtailed its ability to gather data and could make it less useful to key allies, say sources and officials.

A federal court judge on Thursday said the Canadian Security Intelligence Service (CSIS) had secretly operated a data analysis center for 10 years and illegally retained electronic information from people in Canada who were not linked to particular security threats.

The agency, which says the data is useful, said late on Thursday it would suspend analysis of the information until it reviews what the ruling means for its domestic and foreign intelligence gathering.

That looks set to negatively affect its relations with sister spy agencies abroad as critics at home complain CSIS needs closer supervision.

To seek electronic data from a suspect in an investigation CSIS needs a warrant from the federal court, which has now ordered the agency not to hold onto data collected from third parties.

A senior security source said that unless the law was changed to allow CSIS to retain the data in question, "everyone should be clear what this means to the ability of CSIS to discharge its responsibilities."

CSIS could now also have trouble working with its allies in the so-called Five Eyes intelligence-sharing network, which also includes Britain, the United States, Australia and New Zealand, said a leading security expert.

"The implications are major because the new constraints are now part of every warrant going forward," Christian Leuprecht, politics professor at the Royal Military College of Canada.

The ruling, he said, meant CSIS would not be able to gather as much information as it wanted about suspects.

"That depreciates its value as a partner to allies because it means CSIS has less intelligence to share," he said by e-mail.

If CSIS finds its ability to act is crimped it could in theory turn to the Royal Canadian Mounted Police, which shares responsibility for national security. Two sources with knowledge of the matter say relations between the agencies have deteriorated.

Counterintelligence was originally handled by the RCMP's security service, but this was disbanded after a scandal and folded into the new CSIS in 1984 along with a new generation of civilian employees, a move that generated friction.

The sources said the two agencies had agreed last year to try to work towards a rapprochement but had little success.

Neither the RCMP nor CSIS were immediately available for comment.

CSIS officials said they retained the data in question because of its value. Public Safety Minister Ralph Goodale, who publicly criticized CSIS on Friday, said all intelligence and security agencies had to follow the law.

Both agencies ultimately report to Goodale, who said CSIS director Michel Coulombe understood the need for immediate action in the wake of the court ruling.

"A serious error has been made ... this situation needs to be remedied, it has to be remedied quickly," Goodale told reporters. He declined to answer directly when asked whether he still had confidence in Coulombe, who has been in his position since May 2013.

(Reporting by David Ljunggren and Allison Lampert; Editing by Alden Bentley)

Globe and Mail
Public safety minister vows action after CSIS data collection finding
Saturday, 05 November 2016
Byline: Colin Freeze and Laura Stone

Toronto - Public Safety Minister Ralph Goodale says he will make sure Canada's spy agency takes action after a Federal Court found that its officials have misled justices and unlawfully amassed data about people not suspected of being threats.
The Canadian Security Intelligence Service was found this week by Justice Simon Noël to have made chronic omissions in wiretap applications.

Suggesting at one point that CSIS's behaviour verged on contempt of court, he wrote that the spy agency had tried to keep its intelligence programs hidden.

For at least 10 years starting in 2006, CSIS has been skimming telecommunications data, such as phone logs and Internet trails, from the conversations it has intercepted after receiving authorization from the Federal Court.

The spy agency is required to destroy the records of some conversations it captures, including those of people who were in contact with CSIS targets but were not suspected of being a threat to security.

However, the spy agency has been holding onto the data related to these people, and had not disclosed this in wiretap applications.

Federal Court judges, who are on the front lines of making sure CSIS surveillance is lawful, were outraged to learn of such retention in a watchdog's report earlier this year.

They convened court hearings on the matter, and ruled this was always fundamentally unlawful under the CSIS Act.

During the 1980s, the spy agency's first director resigned after taking personal responsibility for a subordinate's inclusion of false information in a wiretapping warrant.

On Friday, Mr. Goodale said he intends to ensure that CSIS follows the Federal Court's directive to stop the controversial practices.

Toronto Star
Civilian watchdog defends CSIS and embattled director over 'metadata'
Saturday, 05 November 2016
Byline: Tonda MacCharles and Alex Boutilier

Ottawa - Michel Coulombe, Canada's top spy, is in deep trouble with the courts and his political boss, Public Safety Minister Ralph Goodale, over revelations CSIS kept a decade's worth of data on Canadians who are no threat to national security.
But Pierre Blais, head of the civilian watchdog agency over CSIS, says Coulombe "acted in good faith" and should not lose his job over the affair.

"He's doing a good job. And that's a difficult issue, that we have to act as big girls and big boys and we look at this and we should do the best for the future," said Blais, chair of the Security Intelligence Review Committee (SIRC).

Blais came to Coulombe's defence Friday, saying CSIS and its director did not deliberately lie to the court about a practice that SIRC red-flagged in an annual report tabled in January.

That was the first time the Federal Court learned that CSIS had created an Operational Data Analysis Centre in 2006. CSIS and its lawyers were hauled before a panel of all Federal Court judges who handle national security warrants and cases last spring to explain.

On Thursday, Justice Simon Noël released a scathing ruling that said the agency wrongly kept and analyzed "metadata" of an untold number of Canadians in violation of its legal mandate to retain only "strictly necessary" information on threats. CSIS downplayed the type of data scooped up in its probes as simply email addresses, cell numbers and IP addresses, but not the content of communications.

Still, the judge said CSIS breached its "duty of candour" when it failed to reveal what it was up to. Goodale said Friday he first learned of it was two weeks ago when an unredacted copy of the pending judgment reached his desk.

Asked if he still has confidence in Coulombe, the minister would say only that he has made his expectations to the director abundantly clear.

"A serious error has been made. (Coulombe) maintains that in his view, and in the view of the advice he got from the Department of Justice over the course of the last number of years, that the course of conduct by CSIS was within the parameters of law," Goodale told reporters.

"The court has now said very clearly and unequivocally that it was not. This situation needs to be remedied. It has to be remedied quickly . . . CSIS must be forthcoming and candid with the court. That will happen."

Blais said Coulombe, who rose through the ranks of CSIS to become its head, should not resign or be fired, and expressed total confidence that he "is a very efficient person and he will make the correction that has to be done for the future no question about that."

Asked if he was concerned CSIS had lied by omission to the courts, Blais said "lying, it's a very strong word."

"As far as I'm concerned -- I cannot say that; they never lied to the judge. They maybe (didn't) put everything that should have been presented to the judge," but he repeated "I'm sure that everybody's acting in good faith."

A former chief justice of the Federal Court of Appeal who heard national security cases before taking the top job at SIRC, Blais was also once a Progressive Conservative solicitor general and justice minister, and said: "It's not that black and white all the time, particularly in this area. . . . It's never black and white, it's always grey, and we try to make sure that we do the best job possible in respecting the law."

But Goodale was adamant Friday that innocent people should not have their information tracked and stored by Canada's spies.

"That's a fundamental principle of Canadian privacy," Goodale said.

La Presse
Surveillance de journalistes
Saturday, 05 November 2016
Byline: Vincent Brousseau-Pouliot

Ottawa - S'il a obtenu l'assurance qu'aucune surveillance de journalistes ne se produit «actuellement» au niveau fédéral, le gouvernement Trudeau n'a pas demandé à la Gendarmerie royale du Canada (GRC) et au Service canadien du renseignement de sécurité (SCRS) s'ils ont mis des journalistes sous surveillance au cours des cinq dernières années. «L'enjeu, c'est ce qui se passe maintenant et nous

pouvons offrir l'assurance que ce genre d'activités ne se produit pas actuellement. Je n'ai pas connaissance de choses qui se sont produites quand nous ne formions pas le gouvernement du Canada», a dit le ministre Ralph Goodale, qui n'a pas l'intention de demander à la GRC ou au SCRS si des mandats de surveillance ont été lancés à l'égard de journalistes au cours des cinq dernières années. «La réponse, autant de la GRC que du SCRS, est que rien de la sorte ne se produit actuellement. [...] C'est la responsabilité du directeur du SCRS de répondre aux questions opérationnelles. Vous allez sur une pente très dangereuse quand vous invitez les politiciens à aller dans ce domaine», dit le ministre Goodale.

Canadian Press
Federal security review to examine CSIS powers in the digital age, Goodale says
Saturday, 05 November 2016
Byline: Jim Bronskill

Ottawa - A federal review of national security will consider whether Canada's spy service should be able to sift through the kind of personal data it kept illegally for years, says Public Safety Minister Ralph Goodale.
Goodale said Friday the notion that the Canadian Security Intelligence Service should avoid stashing away information about innocent people is a ``fundamental principle of Canadian privacy.''

But the minister appeared to leave the door open to one day giving CSIS the legal authority to keep and analyze electronic data about individuals who do not pose a security threat.

He indicated the federal security review already under way would be a good forum to explore the matter.

``I want to hear the professional advice on both sides,'' Goodale told a news conference in the foyer of the House of Commons. ``I'm not pre-empting the consultation.''

A Federal Court judge says CSIS violated the law over a 10-year period by keeping potentially revealing electronic data about people who were not targets of investigation.

In a pointed ruling made public Thursday, Justice Simon Noel said CSIS breached its duty to inform the court of its data-collection program, since the information was gathered using judicial warrants.

CSIS processed the data beginning in 2006 using a powerful program known as the Operational Data Analysis Centre to produce intelligence that can reveal specific, intimate details about people, the judge said.

The improperly retained material was metadata _ information associated with a communication, such as a telephone number or email address, but not the message itself. It is believed to have included data

trails related to people such as friends or family members who knew the targets of surveillance but were not themselves under investigation.

The ruling means metadata can now be kept and used by CSIS only if it relates to a specific threat to Canadian security or if it is of use to an investigation, prosecution, national defence or foreign affairs.

In a hastily assembled news conference Thursday after the decision become public, CSIS director Michel Coulombe said the spy service had halted all access to, and analysis of, the data in question while it thoroughly reviews the court decision.

Goodale said he became aware of the ``full scope of the issue'' when the court judgment was made available to him in preliminary form a couple of weeks ago.

He said he took the immediate step of informing the Security Intelligence Review Committee, the watchdog over CSIS, and asked the review committee to supervise management of the data and ensure full compliance with the judgment.

Coulombe ``understands my expectations here,'' Goodale added.

``A serious error has been made. This situation needs to be remedied. It has to be remedied quickly.''

Privacy commissioner Daniel Therrien said the spy service had already contacted his office. ``At this point I can tell you that we welcome discussions on changes to CSIS policies required by the judgment.''

It marks the second time in recent months that CSIS's data analysis practices have been questioned.

In its latest annual report, tabled in September, the intelligence review committee said CSIS used datasets to identify previously unknown individuals of interest by linking together types of information that have indicated ``threat behaviour.''

``They can be used to conduct indices checks by taking information already connected to a potential threat _ such as an address, phone number or citizen identification number _ and using it to search for 'hits' in the data,'' the review committee report said.

CSIS argued that openly sourced and publicly available datasets were akin to the phone book and therefore restrictions in the CSIS Act limiting collection to ``strictly necessary'' information did not apply.

However, the review committee looked at the full list of datasets held by CSIS and, in come cases, disagreed with the spy service's assessment that they were publicly available and therefore beyond the legal restriction.

As a result of the committee's intervention, CSIS finalized and implemented guidelines for acquiring bulk data and agreed to ensure it abides by the CSIS Act in collecting such information.

In his ruling on the illegal metadata analysis, Noel suggested it was time to review the 32-year-old CSIS Act to answer the needs of the present and perhaps ``unforeseen times ahead with an adaptation to new technologies at play.''

The NDP said Friday the latest revelations underscore the need for stronger parliamentary oversight.

The New Democrats are pushing for changes to a bill that would create a committee of parliamentarians to keep an eye on CSIS and other spy services. NDP MP Murray Rankin said the proposed model would allow the government to arbitrarily deny crucial information to the committee.

Goodale flatly rejected the criticism, saying the committee would have extraordinary authority to look at classified information.

China Post
The Spy Alliance Is Watching You (Canada)
Sunday, 06 November 2016
Byline: Harun Yahya

Analysis: "Five Eyes" is the name of the joint intelligence network of five countries, which are the UK, the U.S., Canada, Australia and New Zealand. The beginning of the network dates to the UKUSA, an agreement to share intelligence signed between the UK and the U.S. in March 1946. Founded by the U.S. and the UK, UKUSA was transformed into the "Five Eyes" alliance by including the British Commonwealth members Canada, Australia and New Zealand over the following years. Thus, the foundation for a giant intelligence network which monitors the communication traffic in all continents from five different points and shares this information with the allied countries was laid.
This alliance between five Anglosphere countries is based upon the principles of sharing every kind of intelligence (primarily the signals information called SIGNIT) between each other and a vow to never spy on member countries. This 70-year-old alliance monitors, analyzes and stores the world's communications today with its built-in global monitoring substructure.

The primary intelligence services of these five countries constitute the essential parts of this monitoring system: the U.S.'s "NSA," the UK's "GCHQ," Canada's "CSEC," Australia's "ASD" and New Zealand's "GCSB" being the major ones. In addition to this, other numerous subsidiary intelligence services are the most important sources of the "Five Eyes" network.

Among these, for example, there is the RAF (Royal Air Force) of the UK, which is known as the biggest electronic monitoring center in the world.

Here, intelligence is gathered for U.S. and the UK by monitoring the communication networks of the whole world. Even if we consider that only the NSA and the RAF are a part of this system, the strength and the extent of the capacity of "Five Eyes" to gather intelligence can be better understood.

As it is known, the documents revealing the secret relationships between the Five Eyes countries and the global intelligence operations they carried out were exposed by the former CIA and NSA employee Edward Snowden in 2013. These documents, which were featured in The Guardian, The Washington Post, Der Spiegel and The New York Times, brought the details of the illegal monitoring and intelligence gathering operations of Five Eyes into the light.

Far-reaching Tentacles

According to the documents, among the bodies English intelligence service listened and monitored in liaison with the NSA were diplomats from the G-20 summit, the presidents of countries including Germany, Brazil and Mexico, politicians, U.N. offices, various embassies and media outlets. The bugging and the eavesdropping of Kofi Annan's office during the early stages of the Iraq War can be considered as one of the many activities of English secret service.

There are satellite dishes, listening and monitoring stations belonging to the NSA and English GCHQ in embassies, military bases and agencies all over the world.

These have immediate access to the security cameras of almost all countries. English and American ships along the Chinese coastline are listening to the radio communications in the region.

The satellite dishes stationed in Fort Meade, Maryland, are monitoring banking transactions all over the world.

According to the news reported by The Guardian, in order to gather global communication information, the UK acquired all kinds of personal private information by secretly gaining access to the intercontinental fiber-optic cables that carry the phone communications, messages and Internet traffic. British intelligence agency GCHQ can gather information from 46 of them simultaneously.

This secret program, code named "Tempora,"had been in operation for 18 months when the news surfaced, and the amount of data (phone records, SMS messages, emails, internet usage, website login information, social media information from websites such as Facebook etc.) gathered only within that time period was of staggering proportions.

For example, approximately 600 million phone conversations were recorded only in one day. The amount of information gathered daily is equivalent to the capacity of information existent in 192 English National Libraries.

'Worse than the US'

Snowden states that this spy network is not the sole work of the U.S., but in fact the main player is the UK, and in order to emphasize the fact that English intelligence service has no limits, he says "THEY (THE UK) ARE WORSE THAN THE USA."

Prism and XKeyscore, which surfaced like Tempora, are also among the high-tech intelligence gathering, analysis and filtering programs that Five Eyes uses. These can connect to computer servers and satellites at the military and diplomatic facilities of many foreign countries. Another Five Eyes product, ECHELON, which is frequently mentioned in espionage techno-thrillers, is the oldest and most basic version of these programs.

We should also state that New Zealand's electronic monitoring agency, GCSB, is also hard at work. It gathers the communication information circulating in the Asia-Pacific region via the NSA's controversial XKeyscore program and delivers it to its bosses in the UK and U.S. in the form of metadata packages. According to the Snowden documents, the information gathered by GCSB has no relation to security threats. On the contrary, GCSB directed its spying activities to a wide range of countries comprised of New Zealand's friends, trading partners and closest Pacific neighbors.

Even if we only consider the information provided in this article, it is obvious that, contrary to popular fallacy, the U.S. is only one of the Five Eyes, while the brain governing all these "eyes" resides in Great Britain, as it has been for centuries. Based on the environment, conditions and the plans, sometimes this brain comes to the forefront, and sometimes it hides in the background.

It's for Your Own Good

The activities of Five Eyes continue on unrestrained, disregarding laws, personal lives and privacy. This dark organization carries out its illegal and illicit operations by hiding behind cliched excuses such as "terror threat" and "security issue," just like it does with its every kind of imperialistic activity.

It is obvious that the real purpose of this organization, as it has always been, is to gain the most powerful political, military and economic dominance over the world and create the most advanced manner of exploitation based on self interests.

These kinds of sinister organizations draw their strength from their secrecy.

For this reason, the best way to fight against organizations like Five Eyes is to expose them and bring them out from the darkness they hide in into the light, to make them transparent. In order to win this fight, the good must be allied together and support each other.

The name Five Eyes, which is used to describe an organization comprised of five countries, requires a brain that rules over these five eyes, evaluates the received information and makes it "seen" and the place to look for this brain is the island of Britain.

The Guardian (London)

New generation of ethical hackers aims to impress recruiters

Saturday, 05 November 2016

Byline: Rob Davies

London - As the UK's National Cyber Security Centre starts work, recruiters are busy identifying raw talent to counter future hazards

With the launch of the National Cyber Security Centre, backed by £1.9bn of funding to battle online crime, the government has made a statement.

Defence experts have long warned of the growing menace of cybercrime and now they have good reason to believe the threat is being given priority treatment.

Recognising the danger is one thing though, dealing with it another. The world - and by extension the UK - is facing a shortage of people with the skills needed to mount an effective defence.

The global cyberdefence industry is going to need another 1.5 million staff by 2020, according to non-profit security organisation (ISC) 2.

At the Cyber Security Challenge in London - a three-day competition designed to identify raw cybersecurity talents - recruiters are doing their best to address the shortage.

Stephanie Daman, the chief executive of Cyber Security Challenge UK, believes that the UK is slowly recognising the value of ethical hackers, also known as "white hats", the cybertroops required to protect our increasingly connected world.

"We're beginning to build a pipeline of people. But that, by its nature, is going to take a little while to come to fruition," says Daman, who spent 17 years working for the government on security matters.

In the meantime, events such as the Cyber Security Challenge are trying to address the skills gap.

The event is sponsored by corporations such as PricewaterhouseCoopers (PwC), BT and BAE Systems, while camera-shy staff from GCHQ and the National Crime Agency look on, hoping to unearth a new generation of cyberspooks.

Around half of the contestants in the challenge typically get a job out of it, while all are likely to be interviewed.

Recruiters like the event because it allows people who may not shine academically to show that they can still thrive in a high-pressure, realistic scenario.

Last year's Cyber Security Challenge was fairly fanciful. It involved a bio-hazard attack and a threat against a minor royal. This year, the challenge is more grounded in reality. The contestants are asked to fight an assault on a fictional energy company, Bolt Power.

They are tasked with assessing and battling an attack from "hacktivist" cybercriminals, repairing a data breach and investigating the theft of £125m.

There are good reasons to be concerned about cyber-attacks on infrastructure within energy, but also in areas such as transport and telecommunications, or even hospitals.

Earlier this year, Theresa May delayed a final decision on the Hinkley Point C nuclear power plant

, and anxiety about the involvement of state-backed China General Nuclear was thought to be among the reasons for the delay.

These concerns have been heightened by hacks perpetrated against, among others, semiconductor firms in the US, and suggestions that designs for narrow-body aircraft have also been targeted.

Understandably, few people at the Cyber Security Challenge are willing to talk about Hinkley or point the finger at Beijing. But they are clear about the nature of the threat from state-backed groups.

Kris McConkey is on the frontline of the war against cybercrime. His job is to make life intolerably difficult for hackers. When the chancellor, Philip Hammond, said the UK must "strike back" against cyber-attacks, it was people like Kris he surely had in mind as his infantry.

"A lot of cases we get called in to are where organisations find it difficult to deal with [it] themselves," says McConkey. "A high proportion of those are attributed to state-sponsored groups."

There may still be a threat, he says, even where the state in question is only involved financially in a sensitive infrastructure project.

Companies may try to set up a firewall between sensitive systems and foreign powers, but it does not always work.

"A lot of organisations have tried to do it and a lot of organisations have had their fingers burned. It's a very difficult line to walk."

"For the most part these things end up in some joint endeavour. There's almost always a people aspect and that's often where you get an insider placed there to gain information."

He cites a recent example where a cyber-espionage group had hidden inside a company's network for two years, helped by a contractor the unnamed firm had hired.

So how to stop this? Businesses can pass information to the security services, but they are not legally allowed to "hack back" by launching cyber-attacks themselves.

But they can at least lay booby-traps to confuse and deter - a concept known as "active defence".

"One way is to go and hack the bad guys, yes. The other way is to make your network a hostile place for an attacker to break into," says McConkey.

"If you've got a burglar coming through your door, you want them to be standing in a house of mirrors, you want them to think there are many more systems than there are."

That may be easier said than done, but the Cyber Security Challenge is about finding out who has the requisite technical ability, as well as the decision-making and interpersonal skills needed to liaise with businesses facing a threat.

Contestants are encouraged to think on their feet and a team of mischievous PwC staff sits on the sidelines, occasionally throwing cyber-attacks at the contestants themselves in a bid to trip them up.

The atmosphere is tense and the contestants, many barely out of school, are feeling the heat.

But despite the technical expertise on show, there is something that does not add up.

Of the seven competing teams - all named after famous cryptographers - four honour brilliant women, while 24-year-old Holly Rostill oversees the day's events in the role of game master.

Lisa, 21, is a fourth-year computer science student and one of only two women competing out of 42 contestants. "This challenge is hard and it's gradually getting harder. Some of it is more like a whodunnit. You approach it with a technical mindset, but the challenge isn't necessarily technical."

"It's a real-world simulation. If something breaks then the cybercriminals don't stop. They take advantage, they get you when you're weak."

The stark gender imbalance is all the more concerning when the talent pool needs to be as deep as possible.

"There's a horrible dearth of women in this space," admits Daman. "Because we haven't engaged girls and women at school and kept them engaged when they make subject choices, we've lost a generation of women."

Lisa, who asked for her surname to be omitted, adds: "It's well known that the tech industry is short on women, but there's a lot of work being done to engage women into Stem subjects [science, technology, engineering and maths].

"Maybe it's a lack of awareness, but it is improving. Girls can do it too, we're just as good."

Daily Mirror
Chaos after cyber attack on hospitals
Saturday, 05 November 2016

London - Specialist police teams are probing the suspected cyber attack by Russia that forced three hospitals to cancel their operations.
Appointments were axed and 3,000 patients were affected after the virus hit Northern Lincolnshire and Goole NHS Trust on Sunday.

Normal service in Grimsby, Scunthorpe and Goole resumed on Thursday.

The Yorkshire & Humber Regional Cyber Crime Unit is probing the strike.

Last night, a senior NHS official downplayed reports of Russian involvement but added: "This is a very real and very serious threat."

The Guardian (London)
Call for Prevent-style strategy to stop children engaging in cybercrime
Monday, 07 November 2016
Byline: Vikram Dodd

London - Britain's cybercrime tsar will formally ask the government to set up a programme based on the controversial Prevent strategy to stop children as young as 12 becoming involved in sophisticated computer offences, the Guardian has learned.
Dr Jamie Saunders said training was needed to help spot teenagers at risk as many young internet users experiment with hacking or other cyber offences without realising that what they are doing is a crime.

Saunders, the director of the national cyber crime unit at the National Crime Agency (NCA), said he was proposing the scheme, known internally as Cyber Prevent, to ministers. It is modelled in part on Prevent, the official counter-radicalisation programme that has been dogged by controversy.

But instead of trying to divert aspirant jihadis away from terrorism, Cyber Prevent would aim to deter computer-literate youngsters from carrying out distributed denial of service attacks (DDoS) and other cybercrimes, such as hacking private details.

Saunders said the programme could also be used to recruit tech-savvy young adults. "We need education for schools on the [1990] Computer Misuse Act, on what it is and isn't [a cybercrime]. A lot of kids don't realise they are committing a crime," he said.

"We don't want them to go to prison, we want them to come and work for us."

Demand for computer skills is forecast to grow in coming years. One core message at the heart of Cyber Prevent is that young adults with computer skills can earn good amounts of money legitimately, as opposed to perpetrating cybercrimes and being pursued by law enforcement.

"A lot of kids are stumbling into this crime. This activity has consequences for them and others. There are legitimate opportunities for their skills," Saunders said.

The target group would be those aged 12 to 25. One major cyber- attack, which is currently subject to legal restrictions, was carried out by a teenager.

Analysis of investigations undertaken by the national cyber crime unit in 2015 found the average age of suspects was 17. The previous year, the average was 24.

Saunders said some cyber-attacks had been carried out by children who did not realise the harm they could do. "We are not dealing with serious criminals. Some are sucked in and damage their careers and do a lot of harm," he said.

Research shows that some who end up committing cybercrime start by learning how to outwit games programmers. "One of the entry points is cheating on online gaming - you have to be quite clever to do that," Saunders said.

Cyber Prevent would be relatively low cost, especially compared with the harm it aims to thwart, Saunders said. The scheme would hire a network of regional specialists and companies could contribute to the cost.

The programme would also target parents so they had a better chance of knowing what their children might be up to.

The sheer volume of online offending means only a fraction of offenders are likely to be caught.

Compared with other major types of crime, intelligence about cybercrime offenders is at a relatively early stage. "We keep finding clean skins, people we did not know about," Saunders said.

The NCA said malicious software called remote access trojans (RATs) is popular among teenage computer users. It allows users to remotely take full control of another computer. An NCA-led operation

targeting users of the Blackshades RAT found that the average age of the 22 people arrested was 18, with the youngest 12 years old.

Saunders became director of the national cyber crime unit in 2014, joining from the Foreign Office, where he was director of international cyber policy. Before that, he worked at GCHQ.

Washington Post
The coming clash with China
Monday, 07 November 2016
Byline: Josh Rogin

Column from Beijing - If Hillary Clinton is elected, her national security team plans to urgently address the growing North Korean nuclear and missile threat. That would surely raise tensions on the Korean peninsula - and it could also lead to an early and acrimonious confrontation between a Clinton administration and the Chinese government of Xi Jinping.
Xi is staunchly opposed to Clinton's plan to drastically increase sanctions on the regime of Kim Jong Un. At the Munich Security Conference Core Group meeting here last week, Chinese officials and experts delivered a clear and unequivocal message to the visiting Westerners: China will not take any steps against Pyongyang that might increase the chance of a confrontation with the North Korean regime or encourage regime change on China's border.

Chinese Vice Foreign Minister Zhang Yesui said that although China might endorse a limited U.N. Security Council resolution in response to North Korea's recent provocations, there's no Chinese appetite for further pressure. The Chinese rationale is simple: Beijing values stability on the Korean peninsula more than it fears the growing prospect that North Korea will succeed in its goal of becoming a full-fledged nuclear power capable of striking the West.

"China will never allow war or chaos on the peninsula, and if that occurs that will help no one," Zhang said. "We need to bring the issue back to the track of dialogue and consultation."

In Washington, there's bipartisan consensus that returning to the negotiating table without significantly more leverage against the Kim regime would be a futile and perhaps even dangerous misstep. At best, it would only repeat a failed pattern of bribing the North Korean government into a short-term pause in its mischief.

Top Clinton foreign policy advisers have been open about their intention to apply to North Korea a version of the playbook the Obama administration used with Iran. They are promising to drastically increase sanctions on Pyongyang before sitting down at the table. They are also considering secondary sanctions on foreign firms that enable North Korea's illicit industries, which means punishing Chinese companies keeping Kim's nuclear and missile industries afloat.

For the Chinese government, both of those ideas are seen as direct assaults on China's primacy over an issue it considers a core interest. Rather than respond to the threat of sanctions by leaning on its client state, Beijing is more likely to buck Washington and fight back against the new policy.

"If the assumption of any new American administration is that China is the one to blame and we need to put pressure on or even punish China, that would be a big mistake," said Dong Wang, professor at the School of International Studies at Peking University. China may retaliate with punitive measures against the United States in other areas of the bilateral relationship, he said.

Chinese officials at the conference warned that the proposed Clinton policy carries a risk of sparking a war on the Korean peninsula, and they expressed the suspicion that the unstated U.S. motivation was to spur regime change in Pyongyang.

The Clinton team has a plan to allay Chinese fears about regime change. Her advisers intend to push for a new dialogue with Beijing to discuss what would happen if the sanctions inadvertently cause the regime to collapse or if the regime implodes on its own due to mounting internal tensions.

"We are not talking about creating a regime change, but should something happen, China needs to know its interests are going to be protected," Wendy Sherman, a former undersecretary of state for political affairs and a top Clinton campaign foreign policy adviser, said last month at the Meridian Global Leadership Summit. "The South Koreans believe in tightening the noose around North Korea. ... We believe in that as well."

But the Chinese government has no intention of entering a dialogue with the United States about planning for the day after the Kim regime falls. For Beijing, preventing the fall of the regime is a must, and therefore coordinating plans for its collapse is off-limits.

David Shambaugh, director of the China Policy Program at George Washington University, said that addressing the North Korean nuclear threat will be the first serious test of the strategic relationship between the United States and China in the next administration, regardless of who wins.

"China is really crucial to this and we'd like to get a paradigm shift in the thinking of the Chinese leadership," he said. "But if they continue to refuse to move into these discussions, the temptation for the American side is just to move unilaterally."

Clinton's advisers are threatening to do just that, but they should have no expectation that China is going to comply. In fact, the North Korea issue could mean that the first foreign crisis of a potential Clinton presidency will come not in the Middle East or with Russia, but in northeast Asia.

New York Times
F.B.I. Says Review Clears Clinton in Email Inquiry

Monday, 07 November 2016
Byline: Multiple reporters

Washington - The F.B.I. director, James B. Comey, told Congress on Sunday that he had seen no evidence in a recently discovered trove of emails to change his conclusion that Hillary Clinton should face no charges over her handling of classified information.
Mr. Comey's announcement, just two days before the election, was an effort to clear the cloud of suspicion he had publicly placed over her presidential campaign late last month when he alerted Congress that the F.B.I. would examine the emails.

"Based on our review, we have not changed our conclusions that we expressed in July with respect to Secretary Clinton," Mr. Comey wrote in a letter to the leaders of several congressional committees. He said agents had reviewed all communications to and from Mrs. Clinton in the new trove from when she was secretary of state.

The letter was a dramatic final twist in a tumultuous nine days for both Mrs. Clinton and Mr. Comey, who drew widespread criticism for announcing that the F.B.I. had discovered new emails that might be relevant to its investigation of Mrs. Clinton, which ended in July with no charges. That criticism of Mr. Comey from both parties is likely to persist after the election.

While the new letter was clear as it related to Mrs. Clinton, Mr. Comey's message was otherwise vague. He did not say that agents had completed their review of the emails, or that they were abandoning the matter in regard to her aides. But federal law enforcement officials said that they considered the review of emails related to Mrs. Clinton's server complete, and that Mr. Comey's letter was intended to convey that.

One senior law enforcement official said that as recently as Friday, it was not clear whether the review would be completed by Election Day. But after days of working in shifts around the clock, teams of counterintelligence agents and technology specialists at the bureau's headquarters in Washington finished their examination of the thousands of emails. Officials had decided to make their decision public as soon as they had reached it, to avoid any suggestion that they were suppressing information.

According to the law enforcement official, many of the emails were personal messages or duplicates of ones that the bureau had previously examined during the original inquiry.

Brian Fallon, a spokesman for Mrs. Clinton, said in a post on Twitter that the campaign had always believed she would be cleared of any wrongdoing.

"We were always confident nothing would cause the July decision to be revisited," Mr. Fallon said. "Now Director Comey has confirmed it."

Kellyanne Conway, Donald J. Trump's campaign manager, lamented the fact that Mr. Comey had again inserted himself into the election, but she predicted that his conclusion would have no effect on the outcome.

"The investigation has been mishandled from the beginning," Ms. Conway said on MSNBC, arguing that Mrs. Clinton had wasted taxpayer money and federal resources because of her email practices. "She was reckless, she was careless, she was selfish."

The new review began after agents discovered a cache of emails in early October in an unrelated investigation into the disgraced former congressman Anthony D. Weiner, the estranged husband of one of Mrs. Clinton's closest aides. When searching Mr. Weiner's laptop for evidence of whether he had exchanged illicit messages with a teenage girl, they discovered emails belonging to the aide, Huma Abedin.

That announcement renewed talk of an investigation that had shadowed Mrs. Clinton for much of the Democratic primary campaign. She and her aides had been under investigation for improperly storing classified information on Mrs. Clinton's private email server. The discovery of new emails raised the prospect that the laptop might have new information that would renew the F.B.I. inquiry.

Federal law enforcement officials had said for the past week that only something astounding would change their conclusion that nobody should be charged. But the mere potential for legal trouble was enough to make Republicans gleeful, and Mr. Trump highlighted the F.B.I.'s actions in campaign ads.

At the end of a rocky week for Mrs. Clinton that included wild, false speculation about looming indictments and shocking discoveries in the emails, Mr. Comey's letter swept away her largest and most immediate problem.

Republicans immediately accused Mr. Comey of making his announcement prematurely. "Comey must be under enormous political pressure to cave like this and announce something he can't possibly know," Newt Gingrich, a Trump adviser, wrote on Twitter.

Mr. Comey's move is also sure to prompt questions from Democrats. Most important among them: Why did Mr. Comey raise the specter of wrongdoing before agents had even read the emails, especially since it took only days to determine that they were not significant?

Just hours before Mr. Comey sent the letter to Capitol Hill, Senate Democrats said hearings should be held to examine how Mr. Comey had handled the matter. After the letter's release, Senator Dianne Feinstein, Democrat of California, said the Justice Department "needs to take a look at its procedures to prevent similar actions that could influence future elections."

"There's no doubt that it created a false impression about the nature of the agency's inquiry," she added.

The F.B.I. director's vague, brief announcement on Oct. 28 left Mrs. Clinton with few details to rebut and little time to do it. Many current and former F.B.I. agents and Justice Department officials said Mr. Comey had needlessly plunged the F.B.I. into the politics of a presidential election, with no clear way out.

A long list of former Justice Department officials, including Attorney General Eric H. Holder Jr., chided Mr. Comey. Despite the fact that the bureau did not find anything that changed its original conclusion about Mrs. Clinton, Mr. Comey has insisted that he had no choice but to inform Congress about the new emails because the investigation had been completed and he had pledged transparency, according to senior F.B.I. officials.

Because of Mr. Comey's Oct. 28 letter, Attorney General Loretta Lynch made completing a review of the emails a top priority. Late last month, Mr. Comey ordered agents to work around the clock to sift through the messages. That process, senior F.B.I. officials said, was painstaking, because each message that had been sent to Mrs. Clinton had to be reviewed to determine whether it had sensitive national security materials.

In Mr. Comey's short letter to Congress on Sunday, he said he was "very grateful to the professionals at the F.B.I. for doing an extraordinary amount of high-quality work in a short period of time."

Wall Street Journal
Beijing Tightens Its Control Over Internet With New Law
Monday, 07 November 2016
Byline: Josh Chin, Eva Dou

Beijing - China's government approved a broad new cybersecurity law aimed at further tightening and centralizing state control over the internet, including the role foreign companies play in Chinese cyberspace.
The law, passed by the standing committee of China's legislature and issued publicly on Monday, tasks agencies and enterprises with improving their ability to defend against network intrusions while demanding security reviews for equipment and data in strategic sectors.

The law includes provisions such as a requirement that internet operators provide unspecified "technical assistance" to authorities in cases involving national security.

It also requires security checks for equipment used for critical infrastructure, which is defined as including information services, energy, transportation, finance and other important sectors.

During the drafting, the law was criticized by some foreign business groups and technology experts as a blueprint for further walling off China's already isolated internet.

China's lawmakers described the law as necessary to bolster its online security at a time of multiplying threats.

China, which is often accused of supporting cyberattacks on other countries but which says it is a frequent victim of hacking, has moved aggressively to bolster cybersecurity since President Xi Jinping took office four years ago.

Reuters
China adopts cyber security law in face of overseas opposition
Monday, 07 November 2016
Byline: Sue-Lin Wong and Michael Martina

Beijing - China adopted a controversial cyber security law on Monday to counter what Beijing says are growing threats such as hacking and terrorism, but the law triggered concerns among foreign business and rights groups.
The legislation, passed by China's largely rubber-stamp parliament and set to take effect in June 2017, is an "objective need" of China as a major internet power, a parliament official said.

Overseas critics of the law say it threatens to shut foreign technology companies out of various sectors deemed "critical", and includes contentious requirements for security reviews and for data to be stored on servers in China.

Rights advocates also say the law will enhance restrictions on China's Internet, already subject to the world's most sophisticated online censorship mechanism, known outside China as the Great Firewall.

Yang Heqing, an official on the National People's Congress standing committee, said the Internet was already deeply linked to China's national security and development.

"China is an internet power, and as one of the countries that faces the greatest internet security risks, urgently needs to establish and perfect network security legal systems," he told reporters at the close of a bimonthly legislative meeting.

More than 40 global business groups petitioned Chinese Premier Li Keqiang in August, urging Beijing to amend what they said were controversial sections of the law. Chinese officials have said it would not interfere with foreign business interests.

Contentious provisions remained in the final draft issued by the parliament, including requirements for "critical information infrastructure operators" to store personal information and important business data in China, provide unspecified "technical support" to security agencies, and pass national security reviews.

Those demands have raised concerns within companies that fear they would have to hand over intellectual property or open back doors within products in order to operate in China's market.

"VAGUE, AMBIGUOUS"

James Zimmerman, chairman of the American Chamber of Commerce in China, called the provisions "vague, ambiguous, and subject to broad interpretation by regulatory authorities."

Human Rights Watch said elements of the law, such as criminalising the use of the Internet to "damage national unity", would further restrict online freedom.

"Despite widespread international concern from corporations and rights advocates for more than a year, Chinese authorities pressed ahead with this restrictive law without making meaningful changes," Sophie Richardson, China Director at Human Rights Watch, said in an emailed statement.

Zhao Zeliang, director of the Cyberspace Administration of China's cyber security coordination bureau, told reporters that every article in the law accorded with rules of international trade, and China would not close the door on foreign companies.

"They believe that [phrases such as] secure and independent control, secure and reliable, that these are signs of trade protectionism. That they are synonymous. This is a kind of misunderstanding, a kind of prejudice," Zhao said.

China's foreign ministry spokesman Lu Kang told a regular press briefing that the law was similar to other countries' rules and did not distinguish between foreign and Chinese companies.

Many of the provisions had been previously applied in practice, but their formal codification coincides with China's adoption of a series of other regulations on national security and foreign civil society groups.

The law's adoption comes amid a broad crackdown by President Xi Jinping on civil society, including rights lawyers and the media, which critics say is meant to quash dissent.

Last year, Beijing adopted a sweeping national security law that aimed to make all key network infrastructure and information systems "secure and controllable".

"China's government has come to recognise that cyberspace immediately and profoundly impacts on many if not all aspects of national security," said Rogier Creemers, a researcher in the law and governance of China at Leiden University in the Netherlands.

"It is a national space, it is a space for military action, for important economic action, for criminal action and for espionage," he said.

Xinhua News Agency
China adopts law on cybersecurity
Monday, 07 November 2016
Byline: Staff reporter

Beijing - China's top legislature on Monday adopted a Cybersecurity Law to safeguard sovereignty on cyber space, national security and the rights of citizens.
The government will take measures to "monitor, defend and handle cybersecurity risks and threats originating from within the country or overseas sources, protecting key information infrastructure from attack,intrusion, disturbance and damage," the law reads.

Efforts will also be made to punish criminal activities online and safeguard the order and security of cyberspace.

Individual users and organizations are not allowed to jeopardize security on the Internet or use it to "damage national security, honor and interests," according to the provisions.

Online activities that are attempts to overthrow the socialist system, split the nation, undermine national unity, advocate terrorism and extremism are all prohibited, according to the provisions, which also forbade activities including inciting ethnic hatred, discrimination and spreading violence and obscene information online.

The law was passed at the bimonthly session of the National People's Congress (NPC) Standing Committee, which concluded Monday, after a third reading.

Canberra Times
Spy fear over China link to NBN Component builder linked to Party
Sunday, 06 November 2016
Byline: Richard Baker and Nick McKenzie

Canberra - More than 1 million Australian homes and businesses have been connected to the National Broadband Network by components made in a Shanghai factory controlled by China's Communist Party. The revelation comes at a time when China is suspected of mounting massive cyber-espionage attacks on Australia and after successive Labor and Coalition governments banned Chinese company Huawei from NBN involvement on security grounds. Fairfax Media has confirmed that NBN contractor, France's Alcatel- Lucent, used its Shanghai-based subsidiary to make fibre optical and copper components used to link homes and businesses to the network. Archived webpages of Alcatel-

Lucent Shanghai Bell show the Chinese subsidiary to be part- owned by the Chinese government and clearly under the control of the country's Communist Party, despite the French holding a majority stake by one share. To celebrate November 2012's 18th Chinese Communist Party National Congress, Alcatel-Lucent's Shanghai arm boasted it would "carry out the Party's mass line educational practice" and "ensure oversight party and state policies in the enterprise implementation execution". "Shanghai Bell will ... create a new situation in the socialist cause," the website declared. "The company will follow the higher deployment, under the leadership of party committees at all levels of the party syndicalist organisation." Alcatel-Lucent won the $1.5 billion NBN supply contract in 2010. But the origin of its components has never been disclosed, with NBN Co stating only that "the active equipment is manufactured in large-scale electronics facilities offshore". China has been accused as the culprit in recent major cyber- attacks on Australian agencies, including the Bureau of Meteorology. In response, the Turnbull government announced in April a $230 million national cyber security strategy. The government declined to answer specific questions about the extent of the Chinese-made components in the NBN or whether Australia had security-tested products

sourced from the Shanghai factory. A spokeswoman for Communications Minister Mitch Fifield said the government was "confident that NBN Co has robust measures in place to identify and mitigate security threats, including potential supply chain risks". The importance of security testing telecommunications components was highlighted in a recent private address by one of America's top cyber security officials, National Security Agency deputy national manager Curtis Dukes. Fairfax Media has obtained a transcript of Mr Dukes' remarks to the American Enterprise Institute last month in which he said all "foreign-developed kit" should be tested for spying implants.

Mr Dukes also said he did not support the ban on Huawei so long as it agreed for its products to be tested. However, Fairfax Media has confirmed that the federal government has no intention of reviewing its ban on Huawei. The full story behind Australia's decision to block Huawei is not known. However, US embassy cables leaked by WikiLeaks show that as far back as 2008 Australian intelligence agencies were worried about Huawei and its links to China's military. Huawei, which has tried to alter this perception by appointing former senior Australian politicians such as Alexander Downer and John Brumby to its local boards, was founded by former People's Liberation Army engineer Ren Zhengfei. Appointment of figures such as Mr Downer and Mr Brumby aimed to bolster the company's credentials.

Motherjones
The Democratic National Committee Has Told the FBI It Found Evidence Its HQ Was Bugged
Saturday, 05 November 2016
Byline: David Corn

Washington - In an episode reminiscent of Watergate, the Democratic Party recently informed the FBI that it had collected evidence suggesting its Washington headquarters had been bugged, according to two Democratic National Committee officials who asked not to be named.

In September, according to these sources, the DNC hired a firm to conduct an electronic sweep of its offices. After Russian hackers had penetrated its email system and those of other Democratic targets, DNC officials believed it was prudent to scrutinize their offices. This examination found nothing unusual.

In late October, after conservative activist James O'Keefe released a new set of hidden-camera videos targeting Democrats, interim party chairwoman Donna Brazile ordered up another sweep. There was a concern that Republican foes might have infiltrated the DNC offices, where volunteers were reporting to work on phone banks and other election activities. (For some of their actions, O'Keefe and his crew have used people posing as volunteers to gain access to Democratic outfits.)

The second sweep, according to the Democratic officials, found a radio signal near the chairman's office that indicated there might be a listening device outside the office. "We were told that this was something that could pick up calls from cellphones," a DNC official says. "The guys who did the sweep said it was a strong indication." No device was recovered. No possible culprits were identified.

The DNC sent a report with the technical details to the FBI, according to the DNC officials. "We believe it's been given by the bureau to another agency with three letters to examine," the DNC official says. "We're not supposed to talk about it."

A Democratic consultant who has done work for the DNC, who asked not to be identified, says he was recently informed about the suspected bugging.

The DNC officials will not say what countermeasures were subsequently taken. "As a general policy, we don't talk about such efforts," the other DNC official says. But this official adds, "You have to take all of this incredibly seriously." The first DNC official notes, "We are the oldest political party in this country, and we are under constant attack from Russia and/or maybe others."

Adam Hodge, a spokesman for the DNC, says, "The DNC is not going to comment on stories about its security. In all security matters, we cooperate fully with the appropriate law enforcement agencies and take all necessary steps to protect the committee and the safety and security of our staff."

The FBI did not respond to a request for comment.

CBC.CA
Why hackers might be drawn to your smart light bulbs
Saturday, 05 November 2016
Byline: Natalie Dobbin

Halifax - The technology that can turn on the lights in your home with a simple swipe on your smartphone may seem really cool. Thing is, hackers could have their eye on the same thing.

New research by Dalhousie University PhD student Colin O'Flynn and colleagues in Israel has found smart bulbs could be susceptible to infiltration -- so much so that lights in a household, or even an apartment building outfitted with the technology, could be taken over by hackers.

The researchers have released a draft paper, which hasn't yet been published in a journal or peer-reviewed, that details a study of Philips Hue lamps, which use LED light bulbs operated through apps.

O'Flynn, who studies in the department of electrical and computer engineering at Dalhousie, said the study looked at two things: "Can you reprogram it? Can you make it do bad things?"

The answers were yes and yes, according to the research.

Lights out

The researchers drove around their campus, the Weizmann Institute of Science in Israel, and controlled lights along the route, making them blink SOS in Morse code. They also flew a drone, with an attached device, over office buildings.

O'Flynn and his colleagues were able to make the bulbs talk to each other, which means it was possible to create a widespread viral infection.

Someone could program their light bulb to turn off their neighbour's, for instance. The range of a virus could be from 30 to about 400 metres, O'Flynn said.

"What happens if it's a big city and these are really popular?" O'Flynn said on CBC's Information Morning. "Maybe somewhere like San Francisco that might have a whole apartment building where a lot of people have these bulbs. Could you turn off a whole building? Could you do other stuff with them?"

No virus, company says

In a statement, Philips said its bulbs have not been infected by any virus and that it moved to patch a potential vulnerability when notified of it by the researchers last summer.

"The academics with whom we co-operated via our responsible disclosure process merely demonstrated the possibility of an attack," the statement said.

"They did not create a virus nor disclose information necessary for someone else to do so. Their research findings helped us to develop and roll out the software update."

The company recommends customers install the update using the Philips Hue app.

The internet of things

There are many devices, from thermostats to security cameras, that are now part of "the internet of things," which means they connect to the web and can be accessed through a smartphone.

One little device can be used to get into another, O'Flynn said.

Recently, hackers crippled Dyn Inc., a major U.S. internet firm, which disrupted the availability of popular websites including Twitter, Netflix and PayPal.

A group claiming to be responsible for the attack said it organized networks of connected devices to create a massive botnet that threw 1.2 trillion bits of data every second at Dyn's servers, overwhelming the targeted machines.

Internet of things industry puts all at risk, experts say

Consumer pressure

Items like smartphones or even a fridge have the potential to be affected, O'Flynn said.

"Maybe from this smart bulb you could get into a wireless thermostat. From that you can get onto some other network," O'Flynn said.

He said there are solutions, but they cost companies money and time.

"It's really up to consumers to push the manufacturers," O'Flynn said. "The only reason they won't put good money into security is people don't ask for it."

With files from CBC's Information Morning, Associated Press

Politico.com
The FBI looks like Trump's America
Saturday, 05 November 2016
Byline: Josh Zeithz

Washington - The typical Federal Bureau of Investigation special agent is white, male, and middle-aged, often with a military background -- in short, drawn from the segment of the U.S. population most likely to support GOP nominee Donald Trump.
That demographic reality explains much of the heat FBI Director James Comey is taking from his own work force at the moment for his handling of the Hillary Clinton email investigation and inquiries into the Clinton Foundation.

Days before the presidential election, FBI finds itself at the center of a political maelstrom, with Comey being sharply criticized by Democratic presidential nominee Hillary Clinton and even President Barack Obama, who've faulted the FBI director for going public with word of new evidence in the Clinton email probe.

That furor has exposed dissension in the FBI's ranks, prompting a flurry of leaks about alleged efforts to impede the Clinton-related inquiries and exposing lingering anger among agents about Comey's July decision not to recommend any charges in the email probe.

Incendiary, politically charged remarks from former FBI officials -- with one prominent ex-FBI leader publicly calling the Clintons a "crime family" -- are also endangering the law enforcement agency's reputation for sober, nonpartisan investigation.

Largely overlooked in the imbroglio is how the fact that the FBI doesn't look much like America is complicating Comey's effort to extricate himself and his agency from the political firestorm.

According to numbers from August, 67 percent of FBI agents are white men. Fewer than 20 percent are women. The number of African-American agents hovers around 4.5 percent, with Asian-Americans about the same and Latinos at about 6.5 percent.

If Trump were running for president with an electorate that looked like that, he'd win in a landslide.

"The bureau does tend to be more conservative than people you see in the general populace. It's a natural outgrowth of the demographics. ... That's just math, " said retired agent Emmanuel Johnson, one of several African-American agents who sued the FBI for racial discrimination in the 1990s. "What's troubling is you look at the same population groups they were having trouble [recruiting] 20, 30, 40 years ago and they're having the same trouble today."

Comey has publicly insisted that his agents are apolitical. Asked last year whether politics might color the FBI's handling of the Clinton email investigation, the FBI chief was indignant.

"If you know my folks, you know they don't give a rip about politics," Comey told reporters.

But with numerous leaks from inside the bureau in the final weeks of the presidential race and some prominent former officials denouncing Hillary Clinton and former President Bill Clinton in scathing terms, the FBI chief's assurances that the bureau is completely untainted by politics are in doubt.

"The Clintons: That's a crime family, basically. It's like organized crime," former FBI Assistant Director James Kallstrom said on New York radio station WNYM-AM on Sunday. "I mean the Clinton Foundation is a cesspool. We don't have enough time to talk about the things they've done, screwing people and the public in general. It's just outrageous how Hillary Clinton sold her office for money. And she's a pathological liar and she's always been a liar."

"The agents are furious with what's going on. I know that for a fact," Kallstrom added.

Other ex-FBI officials confirm an uproar in the ranks.

"The stuff about a rebellion going on inside the bureau is absolutely true, but that's not going to influence his decision," one former top bureau official said of Comey, while expressing doubt such concerns played a role in his decisions on the Clinton email case or about informing Congress of new developments, as he did last Friday.

"He loves his troops, but it's not a fair judgment that that's why he did it," said the ex-official, who asked not to be named.

Current FBI officials also insist that Comey's decisions on the Clinton email probe, recommending its closure without charges in July and telling Congress about new evidence last week, were made without any eye to politics.

However, it's clear that the FBI director has felt an unusual need to explain those moves to his own work force, perhaps detecting deep skepticism. The director has sent two agencywide memos defending his handling of the email mess.

"The case itself was not a cliff-hanger; despite all the chest-beating by people no longer in government, there really wasn't a prosecutable case," Comey wrote in a two-page memo to FBI personnel in September explaining the agency's conclusions in the case. He seemed to acknowledge that he was getting grief about the decision from former FBI agents he had met around the country.

When Comey decided last Friday to notify Congress about new evidence in the Clinton email probe, he also fired off a two-paragraph letter to all hands, acknowledging that the move was sure to stir controversy.

"We don't ordinarily tell Congress about ongoing investigations, but here I feel an obligation to do so given that I testified repeatedly in recent months that our investigation was completed," the director wrote. "In trying to strike that balance, in a brief letter and in the middle of an election season, there is significant risk of being misunderstood, but I wanted you to hear directly from me about it."

Some former FBI officials saw the messages as an acknowledgement that the FBI's rank-and-file were suspicious of the decisions being made at the top.

"I think Comey saw he was losing the agents," former FBI agent Ivian Smith said.

Another sign of such trouble: a steady stream of leaks out of the bureau, many of them apparently coming from New York-based agents unhappy with decisions to keep an investigation into the Clinton Foundation in low gear.

"The insurrections usually come out of the New York office," Smith observed.

Another former official said the trouble for Comey began with his early July press statement, in which he was sharply critical of Clinton, then said there were would be no charges. That confused many inside the bureau.

"I think they looked at it and said what he laid out in his July 5 press conference was ample information that they had specific violations of federal law," said former FBI assistant director Tom Fuentes. "When I talked to other people watching that, I thought, he's actually going to recommend the charge. When he didn't ... there were some in the ranks who were concerned about why."

Fuentes blames part of Comey's predicament on the unusual partial recusal Attorney General Loretta Lynch made after holding a meeting with President Bill Clinton on an airplane tarmac in Phoenix in June. She later said she'd defer to career prosecutors and the FBI on the case. That put an unusual degree of weight on the FBI chief in a highly politically-charged case, the former official said.

Fuentes also said he's worried that the current flurry of charges and countercharges could damage the FBI's credibility not just domestically, but around the world, where the agency is seen as the gold standard for detached, professional law enforcement.

"I think it's a possibility people are going to think the FBI is totally politicized," Fuentes said. "When you have people saying the FBI has either been corrupted or is incompetent or both, that is serious stuff."

An FBI spokesperson declined to comment for this story.

However, one FBI official noted that Comey sends agencywide messages on a variety of topics and added that the Clinton probe-related messages only seemed unusual in large part because Comey's decision to make a public statement about a case where no charges were filed was an unusual one.

The typical Federal Bureau of Investigation special agent is white, male, and middle-aged, often with a military background -- in short, drawn from the segment of the U.S. population most likely to support GOP nominee Donald Trump.

That demographic reality explains much of the heat FBI Director James Comey is taking from his own work force at the moment for his handling of the Hillary Clinton email investigation and inquiries into the Clinton Foundation.

Days before the presidential election, FBI finds itself at the center of a political maelstrom, with Comey being sharply criticized by Democratic presidential nominee Hillary Clinton and even President Barack Obama, who've faulted the FBI director for going public with word of new evidence in the Clinton email probe.

That furor has exposed dissension in the FBI's ranks, prompting a flurry of leaks about alleged efforts to impede the Clinton- related inquiries and exposing lingering anger among agents about Comey's July decision not to recommend any charges in the email probe.

Incendiary, politically charged remarks from former FBI officials -- with one prominent ex-FBI leader publicly calling the Clintons a "crime family" -- are also endangering the law enforcement agency's reputation for sober, nonpartisan investigation.

Largely overlooked in the imbroglio is how the fact that the FBI doesn't look much like America is complicating Comey's effort to extricate himself and his agency from the political firestorm.

According to numbers from August, 67 percent of FBI agents are white men. Fewer than 20 percent are women. The number of African-American agents hovers around 4.5 percent, with Asian-Americans about the same and Latinos at about 6.5 percent.

If Trump were running for president with an electorate that looked like that, he'd win in a landslide.

"The bureau does tend to be more conservative than people you see in the general populace. It's a natural outgrowth of the demographics. ... That's just math, " said retired agent Emmanuel Johnson, one of several African-American agents who sued the FBI for racial discrimination in the 1990s. "What's troubling is you look at the same population groups they were having trouble [recruiting] 20, 30, 40 years ago and they're having the same trouble today."

Comey has publicly insisted that his agents are apolitical. Asked last year whether politics might color the FBI's handling of the Clinton email investigation, the FBI chief was indignant.

"If you know my folks, you know they don't give a rip about politics," Comey told reporters.

But with numerous leaks from inside the bureau in the final weeks of the presidential race and some prominent former officials denouncing Hillary Clinton and former President Bill Clinton in scathing terms, the FBI chief's assurances that the bureau is completely untainted by politics are in doubt.

"The Clintons: That's a crime family, basically. It's like organized crime," former FBI Assistant Director James Kallstrom said on New York radio station WNYM-AM on Sunday. "I mean the Clinton Foundation is a cesspool. We don't have enough time to talk about the things they've done, screwing people and the public in general. It's just outrageous how Hillary Clinton sold her office for money. And she's a pathological liar and she's always been a liar."

"The stuff about a rebellion going on inside the bureau is absolutely true, but that's not going to influence his decision," one former top bureau official said of Comey, while expressing doubt such concerns played a role in his decisions on the Clinton email case or about informing Congress of new developments, as he did last Friday.

"He loves his troops, but it's not a fair judgment that that's why he did it," said the ex-official, who asked not to be named.

Current FBI officials also insist that Comey's decisions on the Clinton email probe, recommending its closure without charges in July and telling Congress about new evidence last week, were made without any eye to politics.

However, it's clear that the FBI director has felt an unusual need to explain those moves to his own work force, perhaps detecting deep skepticism. The director has sent two agencywide memos defending his handling of the email mess.

"The case itself was not a cliff-hanger; despite all the chest-beating by people no longer in government, there really wasn't a prosecutable case," Comey wrote in a two-page memo to FBI personnel in September explaining the agency's conclusions in the case. He seemed to acknowledge that he was getting grief about the decision from former FBI agents he had met around the country.

When Comey decided last Friday to notify Congress about new evidence in the Clinton email probe, he also fired off a two-paragraph letter to all hands, acknowledging that the move was sure to stir controversy.

"We don't ordinarily tell Congress about ongoing investigations, but here I feel an obligation to do so given that I testified repeatedly in recent months that our investigation was completed," the director wrote. "In trying to strike that balance, in a brief letter and in the middle of an election season, there is significant risk of being misunderstood, but I wanted you to hear directly from me about it."

Some former FBI officials saw the messages as an acknowledgement that the FBI's rank-and-file were suspicious of the decisions being made at the top.

Another sign of such trouble: a steady stream of leaks out of the bureau, many of them apparently coming from New York-based agents unhappy with decisions to keep an investigation into the Clinton Foundation in low gear.

"The insurrections usually come out of the New York office," Smith observed.

Another former official said the trouble for Comey began with his early July press statement, in which he was sharply critical of Clinton, then said there were would be no charges. That confused many inside the bureau.

"I think they looked at it and said what he laid out in his July 5 press conference was ample information that they had specific violations of federal law," said former FBI assistant director Tom Fuentes. "When I talked to other people watching that, I thought, he's actually going to recommend the charge. When he didn't ... there were some in the ranks who were concerned about why."

Fuentes blames part of Comey's predicament on the unusual partial recusal Attorney General Loretta Lynch made after holding a meeting with President Bill Clinton on an airplane tarmac in Phoenix in June. She later said she'd defer to career prosecutors and the FBI on the case. That put an unusual degree of weight on the FBI chief in a highly politically-charged case, the former official said.

Fuentes also said he's worried that the current flurry of charges and countercharges could damage the FBI's credibility not just domestically, but around the world, where the agency is seen as the gold standard for detached, professional law enforcement.

"I think it's a possibility people are going to think the FBI is totally politicized," Fuentes said. "When you have people saying the FBI has either been corrupted or is incompetent or both, that is serious stuff."

An FBI spokesperson declined to comment for this story.

However, one FBI official noted that Comey sends agencywide messages on a variety of topics and added that the Clinton probe-related messages only seemed unusual in large part because Comey's decision to make a public statement about a case where no charges were filed was an unusual one.

At a House Judiciary Committee hearing in September, Comey insisted he was unaware that the decision to conclude the Clinton email probe without recommending charges had caused any backlash within the bureau. He also seemed personally pained by the suggestion.

"This has provoked some controversy within the ranks of current and former agents?" Rep. Ron DeSantis (R-Fla.) asked.

"Not within the FBI. Again, who knows what people don't tell the director," Comey replied. "If there are agents in the FBI who are concerned or confused about this, please contact me. We will get you the transparency you need to see that your brothers and sisters did this the way you would want them to."

Told that some agents believed a decision was made not to prosecute Clinton even before her July 2 interview at FBI headquarters, Comey seemed troubled.

"If colleagues of ours believe I am lying about when I made this decision, please urge them to contact me privately, so we can have a conversation about this."

Now, there's little doubt that Comey finds himself caught in the middle, under fire from the left and the right, as well as some in his own organization.

While the FBI director has been mounting an aggressive drive to focus on the FBI's shortcomings in diversity, it's less clear if he anticipated how the make-up of his own work force would complicate the handling politically polarizing investigations.

However, he has described the demographic challenges in stark, urgent terms.

"We have a crisis in the FBI and it is this: slowly but steadily over the last decade or more, the percentage of special agents in the FBI who are white has been growing, ... We are now 83 percent white in our special agent cadre," the FBI director said in a July speech at historically black Bethune-Cookman University in Daytona Beach. "I've got nothing against white people -- especially tall, awkward, male white people -- but that is a crisis for reasons that you get and that I've worked very hard to make sure the entire FBI understands. That is a path to fall down a flight of stairs."

For the embattled FBI chief and former prosecutor, there is some good news. There are early signs that his focus on diversity -- which includes displaying a rainbow flag on the FBI's recruiting website -- may be paying off.

The number of African-American agents climbed to 603 in August, up from 581 in March. However, both numbers are lower than the 652 the bureau had four years ago.

The number of Latinos also ticked up slightly, to 888 from 882 in March, but still well below the 983 the FBI had in 2012.

Comey has said he doesn't want to "jinx" himself, but believes the decline in minority agents is being reversed.

"I will have failed if I don't change this. And I have a good feeling it's already changing," he said in July. "I don't want to jinx it ... but we're making progress. People are understanding: It's not just 'the man.'"

Straits Times
S'pore can be model for cyber security
Saturday, 05 November 2016
Byline: Lim Yan Liang

Singapore has a chance to lead by example in its push to get cyber security right, said a visiting former cyber security official from the United States.
As a country aspiring to be a smart nation, Singapore can demonstrate how to build a resilient national critical information infrastructure needed to leverage technology and data, said Mr Sean Kanuck, formerly the most senior cyber security official at the US Office of the Director of National Intelligence.

"Countries around the world, and especially in your neighbourhood, will be looking at the Singapore model, and, hopefully when it's successful, copying parts of it," said Mr Kanuck, who is now a lawyer.

He noted that a comprehensive national cyber security strategy launched last month by Singapore outlines its long-term approach to securing its cyberspace and critical infrastructure against attacks.

At the same time, the strategy also looks into nurturing a home- grown infocomm technology (ICT) sector capable of generating its own valuable intellectual property.

Mr Kanuck said Singapore needs to be more engaged in international discussions on cyber issues if it aims to shape such norms.

He called Singapore's Cyber Security Agency a "great step forward" as it focuses government expertise in thinking about long-term cyber- related issues.

But even as the agency gets to work translating the national strategy into actionable goals - such as boosting talent to fill an estimated 30,000 new ICT jobs that will be created here by 2020 - it needs to stay alert.

"It has to be dynamic and adaptive because the threats it is dealing with are also very dynamic and adaptive," he said.

To stay abreast of innovation in the technology sector, the government has to keep up an active discussion with private sector technology companies, he said.

With eye on China, Japan ramps up presence in Asean

Wall Street Journal Online
Electoral chaos in West being sowed to safeguard Putin's hold on power, Kremlin watchers say
Sunday, 06 November 2016
Byline: Alan Cullison

Washington - A Russian-backed hacking effort that has rocked the presidential campaign may peak on Election Day, but is likely to continue next year and into 2018 as Moscow seeks to influence U.S. politics and key elections in Europe, Obama administration officials warn.

Russian meddling, in fact, may become more potent in Europe than in the U.S., White House officials and other experts say, because Moscow has long courted political figures there, and has forged ties with euroskeptic political parties strengthened by the recent influx of migrants and refugees.

Upcoming contests in Europe include Dutch elections in March, French presidential elections in April and May, and German elections in the fall. Moscow is hoping that gains by

Kremlin-friendly parties like France's National Front could help Russia break free of some of the diplomatic isolation and sanctions imposed on Moscow after its seizure of the Ukrainian peninsula of Crimea in 2014, Kremlin watchers say.

"The German elections, the French elections and other elections in the coming year all have big geopolitical implications for Russia," said Pasi Eronen, Russia project researcher at the Foundation for Defense of Democracies, a Washington-based think tank.

Although large-scale interference from the Kremlin is relatively new to the U.S., Mr. Eronen said Russia has been active in Europe for the past two years with hacking and disinformation campaigns designed to weaken those the Kremlin considers to be political rivals.

Officials say that even if Russia fails to elect its own allies in European elections next year, the sustained meddling in the U.S. and Europe will serve a long-term Kremlin goal--namely, to put Russian President Vladimir Putin's perceived foes in the West in disarray, making it easier for him to safely reseat himself as Russian president when his country holds elections in 2018.

U.S. and European observers have criticized previous elections under Mr. Putin as rigged and marred by obvious fraud--criticism that Mr. Putin has described as a veiled attempt to overthrow him.

Mr. Putin hopes to inoculate himself against such criticism by sowing so much chaos in U.S. and European elections before then that Western leaders will be too preoccupied with domestic problems to spend much effort criticizing the Russian poll, one senior White House official said.

By hacking and dumping emails, Russia is trying "to denigrate the American electoral system, to make it look chaotic, make it look manipulable, make it look subject to intrusion, cheating and vulnerable so you can't trust it...to make us look no better than the Russian electoral system," the official said.

If the West criticizes Putin's re-election in 2018, Russia's response will be, "'Yeah, you're not so good either,'" the White House official said, calling the Russian strategy "a long-term challenge that the United States is going to have to deal with and probably other countries, including those in Europe, [will have] to take seriously."

Russia has dismissed allegations that it has tried to influence elections outside its borders or that it has anything to do with the hacking of Democratic Party emails this year. But senior U.S. intelligence officials

have said repeatedly they are convinced the Russian government stole and then leaked emails in an effort to interfere with the U.S. elections.

They say that conclusion is based on digital evidence left behind in the hacks and the way the information was leaked, which closely mirrors how Russia has tried to interfere in previous elections in Europe. Although the hacks into Democratic Party computer systems were performed months ago, the data was parceled out in the past few weeks on the eve of voting, apparently when it would have maximum impact.

Because Moscow is more likely trying to disrupt U.S. politics than to elect any specific candidate, more emails may be dumped after the elections, said Tom Graham, managing director of Kissinger Associates in New York and former White House adviser on Russia to President George W. Bush.

"The national nightmare might only be beginning," he said.

If Hillary Clinton prevails in the vote, the Russians may choose to dump more information about her afterward to raise a clamor for impeachment proceedings, Mr. Graham said. Or the Kremlin may hang on to some particularly damaging information and privately show it to the White House in a blackmail attempt, he said.

Cyberexperts say attempts to hack into the computer systems of several German political parties this summer were likely a harbinger for similar problems for Europe. German counterespionage officials informed two political parties and the lower house of parliament in September that some of their email inboxes had been targeted by hackers with apparent ties to a foreign intelligence agency.

The group German officials identified as responsible for the attack, APT28, was also tied by investigators to the U.S. hacks as well as cyberattacks last year on a French-language TV broadcaster and the German lower house of parliament, which forced the legislature to shut down its computer system for several days.

Germany's domestic intelligence agency said the hacking group appeared to be "steered by the Russian state."

Sunday Telegraph (UK)
GCHQ wants internet providers to rewrite systems to block hackers
Sunday, 06 November 2016
Byline: Cara McGoogan

London - GCHQ is urging internet providers to change long-standing protocols to help prevent computers being used to set off large-scale cyber attacks.

The Government's cyber-defence arm said it plans to work with networks such as BT and Virgin Media to rewrite internet standards to restrict "spoofing" - a technique that allows hackers to impersonate other computers and manipulate them to carry out anonymous attacks.

"Distributed denial of service" (DDoS) attacks, which employ this method, have been used in numerous high-profile incidents in the past fortnight, including an unprecedented hack that brought down Netflix, eBay and hundreds more popular websites.

"We think we can get to a point where we can say a UK machine can't participate in a DDoS attack," Ian Levy, GCHQ's National Cyber Security Centre, told The Sunday Telegraph.

"We think that we can fix the underpinning infrastructure of the internet through implementation changes with ISPs and CSPs [communications service providers]."

The plan would involve changes to the Border Gateway Protocol (BGP) and Signalling System 7 (SS7) standards that are widely used for routing traffic. GCHQ wants providers to stop the trivial rerouting of UK traffic and to help prevent text message scams.

The Internet Service Providers Association (ISPA) expressed scepticism, saying GCHQ was applying a "we can fix it - it's easy" approach to a complex, historic system.

James Blessing, of ISPA, said internet providers are working on their own fixes for such insecurities. But he said the complex nature of the technology makes it a time-consuming process.

The Telegraph (UK)
US braces for Russian cyber attacks
Sunday, 06 November 2016

Washington - Sixteen years after technical incompetence was blamed for the first inconclusive presidential election in US history, the very opposite of it, namely, technical competence, is shaping up to be the key to next Tuesday's contest between Democrat Hillary Clinton and Republican Donald Trump for the White House.
American intelligence officials are bracing for cyber disruption of the presidential poll by Russia and deploying all the technological resources at their command to prevent such a catastrophe.

While these officials do not expect Russian state-sponsored hackers to throw the entire poll process out of gear on or before Tuesday, cyber experts at the US National Intelligence Agency anticipate that Moscow will meddle with voting systems in states which do not have state-of-the art technology deployed in polling booths.

The Russian objective, they believe, is to create enough doubts among the American public about a rigged election that will persuade Trump supporters to cry foul and question the legitimacy of the outcome if Clinton is declared the winner on the basis of returns notwithstanding allegations of foul play.

That Trump has constantly alleged rigging by the establishment - both in his own party and by Washington vested interests as well as Democrats - to prevent him going to the White House will be interpreted as sanction to Republican supporters to protest or take to the streets on election night to challenge the result.

James Clapper, the director of National Intelligence and Jeh Johnson, director of the department of homeland security, have issued statements that they are convinced the recent election-related hackings of the American cyber systems have been authorised by "Russia's senior most officials". That is a euphemism for Russian President Vladimir Putin.

That the two officials issued a formal statement alleging Russian state meddling in the American poll process was in itself unusual. The move is also being seen here as "anticipatory bail" by the two vulnerable officials if there are allegations on election night or afterwards that the US intelligence apparatus was caught napping.

If Russia's state-sponsored hackers succeed in calling into question voting in battleground states on Tuesday sowing doubts among Americans about the poll process, it would be payback time for Putin.

Successive American Presidents have used a variety of means to undermine Russia's own nascent democracy and repeatedly cast doubts worldwide about Putin's victories - both his own and elections to Russia's legislature, the Duma.

The Americans tried and failed in the past to trigger a "colour revolution" in Moscow's Red Square aimed at unseating Putin. Similarly, US dirty tricks were behind colour revolutions in both Ukraine and Georgia as well as some former Soviet Central Asian republics to weaken Moscow's hold on these countries or disrupt Russian strategic interests there.

Naturally, Putin feels justified in disrupting American elections and casting doubts about the legitimacy of polls in what Americans never tire of trumpeting as the world's oldest democracy.

Putin is unlikely to get another chance at doing this. Not with such ease, at any rate because Trump's personality and political strategy offer fertile ground to put the Russian plans - if US and European allegations are true - into practice.

Trump has been given intelligence briefings with details of what American agencies have gathered about Russian hacking of US election-related websites. But he has chosen not to believe these briefings and has publicly exonerated Putin of any association with the alleged Russian efforts.

Presidential candidates in the US receive top secret intelligence briefings once the major parties formally nominate them as candidates at their national conventions.

Hillary Clinton has also received the same briefings which have been given to Trump, but she has subsequently accused Russia of complicity in the hacking. If Clinton and Trump had stood together and thrown their weight jointly against alleged Russian meddling in US elections, the ground would have been less fertile for the Russians. The hacking has so far resulted in considerable political casualties this election season.

The damage has almost entirely been to Democrats. The party lost its head of the National Committee, Congresswoman Debbie Wasserman Schultz: her equivalent in the BJP would be Amit Shah, the party president.

It has exposed serious failings by Clinton's campaign manager, John Podesta, and sowed mistrust all round within the Democratic party, especially between Clinton and her main rival in the primaries, Senator Bernie Sanders, after the two patched up and agreed to work together. American intelligence is said to have favoured surgical strikes against Russian websites in retaliation, but sources here said President Barack Obama vetoed those plans.

Obama feared that a cyber war against Russia at this stage would only embolden Moscow to do in the open what its cyber warriors are said to have been doing in private so far. Obama's priority is to see through the elections peacefully in the knowledge that the Russians have the capacity to disrupt them if they chose to.

New York Times
A Muted Alarm Bell Over Russian Election Hacking
Sunday, 06 November 2016
Byline: Liz Spayd

Comment: Last winter, as primary voters in Iowa and New Hampshire headed to the polls, a covert and cunning Russian plot was underway to disrupt the American political process. With aliases like Guccifer 2.0 and Fancy Bear, Russian hackers were targeting critical computer systems.
In June, they struck, hitting the Democratic Party, and by July its chairman was ousted in the fallout. Soon embarrassing emails were spilling from the computers of Hillary Clinton and her staff. Republican officials were hit, too. So was the National Security Agency. Now, hackers are meddling with the voting systems in several states, leaving local officials on high alert. Come Election Day, they'll find out what, if anything, the cyberspies have in store.

This is an act of foreign interference in an American election on a scale we've never seen, yet on most days it has been the also-ran of media coverage, including at The New York Times.

The emails themselves -- exposing the underside of the Democratic political machinery, and the conflicts, misjudgments and embarrassing communications of its top ranks -- have received bountiful attention. What rarely makes the main narrative is the spy-versus-spy cyberwarfare: the tactics, the players and the government efforts to tame it. In a calamitous campaign unlike any in memory, it's not surprising that other story lines get squeezed out. But one of the most chilling chapters of this election is the role of Russian intelligence and the growing threat of digital espionage. With days to go, readers have been shortchanged on this part of history.

The email dumps and the hacking have posed challenges for the press, requiring tough calls on news judgment and ethical standards. Some of the emails were personal communications between family and friends, and some contained gossipy exchanges. How does The Times balance the right to privacy against the public interest?

And then there is the unease that comes with feeling used by a foreign superpower. How does the paper avoid becoming an amplifier for a plot that needs the media to work? How does it verify the accuracy of several thousand illegally obtained emails? And most critically, what has it done to try to establish whether Donald Trump was colluding with Russian intelligence, as Clinton suggests?

Considering the journalistic swamp, The Times acquitted itself well on some of these questions. Editors restrained themselves from publishing every email, avoiding the reckless decisions of that some news outlets made. And The Times made reasonable attempts to determine the accuracy of the emails -- though when solid verification couldn't be had, it went with its gut.

Carolyn Ryan, the political editor, acknowledges the challenges when the provenance of information is so suspect. "We do not want anyone, including hackers, to dictate the news cycle in this campaign, or determine what we cover," she said. "We have been restrained."

History will judge The Times's institutional commitment to reporting on the actual foreign intervention less favorably, I suspect. The team in Washington produced commendable, competitive work on an exceptionally difficult reporting target. Led by David Sanger, The Times was first to link the Russians to the hacks, to examine the baffling role of Julian Assange and WikiLeaks and to smartly explore the options that the Obama administration could use to retaliate. I have no substantive complaints about the stories The Times has done.

What was missing is a sense that this coverage is actually important. After The Washington Post broke the story that the Democratic National Committee had been hacked, The Times came back with its own solid piece, but it didn't crack the front page and it earned only a modest mention on the home page. A piece laying out evidence that the Russians may be trying to falsify voting results in state databases ran on A15 and got minimal play digitally. Another on Vice President Joseph R. Biden Jr. signaling that the White House was prepared to order a rare covert cyberattack against Russian found a home on page A19.

What's more, while several reporters have periodically contributed to the coverage, no one was dedicated to it full time. That's too bad. In my view, The Times should have assembled a strike force and given it a mandate to make this story its top priority. You can tell from the outside when the newsroom is turbocharged by a story. The latest coverage of the F.B.I. director, James Comey, is one example. Industrial-scale cybercrime, it appears, is not.

Turbocharged coverage might have led readers inside the cloak-and-dagger underworld of the hackers and the hacked. It might have more fully explored the government lapses in protecting information systems. And it could have told readers more about the effort to uncoil Trump's involvement, if any, in the hacking. When you think about it, there are few more crucial assertions than whether a possible occupant of the White House participated in an act of espionage against his country.

Many readers have raised concerns. Jack Archer, a resident of Oakland, Calif., asks: "If reports of ties between Trump and the Russians are accurate, and several of them are, as we now know, why is The Times ignoring what is potentially the most important story about presidential politics in how long? In your and my lifetime, at least."

The Times finally weighed in on this question last week, concluding that there is no compelling evidence linking Trump to the hackers. The piece, which ran on A21 and down page on the website, appeared to have been in the works for some time. Yet it was published just seven days before the election, and was unsatisfying in exploring the back story that led to its conclusions.

I asked Sanger, a highly knowledgeable and seasoned hand on matters of cyberwarfare, about the challenges in covering information hacks. "American drone strikes and Russians bombing a hospital in Syria are immediate, gripping, tragic human stories," he said. "A cyberstrike, by nature, is subtle, its effects often hidden for months, its importance usually a mystery. The bigger story here is that a foreign power has inserted itself in the fundamental underpinnings of American democracy using cybertechniques. We've never seen that before."

That sounds like a pretty powerful argument for all-hands-on-deck coverage. After all, Trump's treatment of women, Clinton's email servers, the foundations of each candidate -- all of it will soon fade out. The cyberwar, on the other hand, is only getting started.

The Guardian (London)
Invasion of the troll armies: from Russian Trump supporters to Turkish state stooges
Sunday, 06 November 2016
Byline: Leo Benedictus

Analysis: Governments all over the world are manipulating social media for their own ends. That's where the digital footsoldiers come in - smearing opponents, spreading disinformation and posting fake texts for 'pocket money'

We don't know who they are, or what their mission is. We only know that there are thousands of them out there, pretending to be us. They may be at home, or in special offices, or sitting beside you on the train. They use social media, and write blogs and comments. Some of them may visit the bottom of this article.

You can hire your own troll army if you have the cash. In 2011 the PR firm Bell Pottinger told undercover journalists that they could "create and maintain third-party blogs", and spruce up Wikipedia profiles and Google search rankings. Indeed marketing has a rich history of so-called "astroturfing", which is laying down fake grassroots. Take Forest, "the voice and friend of the smoker", which at least admits in nearly invisible small print that it is paid for by the tobacco industry.

Now, however, manipulating social media has become part of the business of government. It may yet influence how governments are formed. Recent reports suggest that many of Donald Trump's most fervent online supporters are not themselves Americans, but Russians being paid by their government to help him win. One told Samantha Bee that she pretends to be a housewife from Nebraska. Why she would confess it now is unexplained, but when you look around it begins to feel like everybody does it. It's just that no two countries' methods are the same.

China The existence of the wumao dang or "50 Cent Party" is not a secret in China, but then it is hard to employ up to two million people secretly. Even the state-owned Global Times reported with approval on the practice in 2010, citing Changsha's party office as the source of the name after it paid a team of commenters 600 yuan a month in 2004, plus half a yuan - hence "50 cent" - for each glowing post they made.

Since then, paying stooges to praise your work online has become about as routine for local government in China as hiring traffic wardens. A recent study at Harvard University found that the Chinese authorities were placing 448m phony comments on the internet each year. In an analysis of 43,800 pro-regime comments, the researchers concluded that 99.3% of them were made by civil servants from a wide variety of government departments. The postings tended to come in bursts at testing times, such as during protests or party meetings.

Interestingly, few of the comments qualify as trolling, in the strict sense. Rather than attacking unbelievers, they focus on swamping the doubters with a flood of positive messages, or cleverly diverting the conversation. As with any job, some practitioners are laughably bad at it. In January 2014, quartz.com found many stooges simply cutting and pasting a suggested question into an online discussion with a party secretary in Ganzhou. "It seems like taxis are far more orderly than in past years," they all wanted to tell him.

Two years before, however, Ai Weiwei interviewed an anonymous 26-year-old with very sophisticated methods. The young man, whose own family knew nothing of his work, estimated that 10- 20% of the comments he saw were left by the 50 Cent Party. He described creating several identities in one forum, and structuring arguments between them so that the most authoritative voice could ultimately settle matters in the government's favour. Another tactic was to be deliberately provocative, and thus draw public anger on to himself and away from the authorities. "Sometimes I feel like I have a split personality," he said. "I wouldn't say I like it or hate it. It's just a bit more to do each day. A bit more pocket money each month, that's all."

Estimated troops Between 300,000 and 2m people, many part-time.

Favourite subjects Excellent local facilities, why democracy doesn't work, Taiwan.

Russia

Long before Donald Trump met Twitter, Russia was famous for its troll factories - outside Russia, anyway. Allegations of covert propagandists invading chatrooms go back as far as 2003, and in 2012 the Kremlin-backed youth movement Nashi was revealed to be paying people to comment on blogs. However most of what we know now comes from a series of leaks in 2013 and 2014, most concerning a St Petersburg company called Internet Research Agency, then just "Internet Research". It is believed to be one of several firms where trolls are trained and paid to smear Putin's opponents both at home and internationally.

Related: Salutin' Putin: inside a Russian troll house

According to internal documents released by a group of hackers in 2013, Internet Research Agency employed more than 600 people across Russia, and had an implied annual budget of $10m - half of which was paid out in cash. Employees were expected to post on news articles 50 times a day. Those who wrote blogs had to maintain six Facebook accounts and publish at least three posts daily. On Twitter, they had to have at least 10 accounts, on which they would tweet 50 times. All had targets for the number of followers and the level of engagement they had to reach.

Later, an investigator called Lyudmila Savchuk went undercover at the company and afterwards published her experiences. These included smearing the character of the opposition leader Boris Nemtsov in the days following his murder, and promoting the theory that he was killed by his own friends, rather than by friends of Putin. "I felt the bullets between my own shoulders," Savchuk said. "I was so upset that I almost gave myself away. But I was 007. I fulfilled my task." When a Finnish reporter called Jessikka Aro wrote about Internet Research in 2014, she herself became the target of a frightening campaign of threats and smears.

As you might expect, many Russian trolls lack a certain polish when posting in English. "I think the whole world is realizing what will be with Ukraine, and only US keep on fuck around because of their great

plans are doomed to failure," one Internet Research employee wrote on a forum. Indeed the Guardian's own moderators have begun to notice regular clues, especially on articles about Ukraine. "We can look at the suspicious tone of certain users, combined with the date they signed up, the time they post and the subjects they post on," says one senior moderator. "Zealous pro-separatist comments in broken English claiming to be from western counties are very common."

Estimated troops Several thousand.

Favourite subjects Putin and Trump being great, the opposition being corrupt, the Nato conspiracy against Russia, the effeminacy of Barack Obama.

Israel There's been an Israeli public relations war for about as long as there's been an Israel. In Hebrew it's called "hasbara", literally meaning "explanation", and it involves trying to improve the world's opinion of the country and its causes. Accordingly there are around 350 official Israeli online channels, covering the full range of social media. For instance, besides its well-known Twitter accounts in English, Hebrew and Arabic, the Israeli Defence Force even has its own Pinterest page, featuring photo collections with themes such as "Soldiers' Stories" and "IDF Style".

In 2013, the Israeli government revealed that it would also recruit "covert units" however. These would be staffed by a mixture of international supporters and domestic students, whose high intelligence, low income and familiarity with social media make them generally well suited to professional trolling. "We need a unified effort to explain why we have a legal right to be here in Israel," the Knesset member Dov Lipman told the Jerusalem Post. "That is key to defeat the movements pushing to boycott, divest and sanction Israel." Those who signed up would get quick access to government information, and leaders of student groups would also be awarded scholarships.

Sure enough, during the war in Gaza the following summer, a student group called Israel Under Fire emerged as one of many voices promoting the Israeli side of the story. "We counter Palestinian propaganda and explain the Israeli perspective," the group's leader, Yarden Ben-Yosef, said. "Social media is another place where the war goes on. This is another way to tell our story." We do not know whether Israel Under Fire was itself one of these covert units, or whether Ben-Yosef got a scholarship. The group's Facebook Page is still active today.

Estimated troops Low thousands.

Favourite subjects Palestinian brainwashing, friendliness of Israeli troops, justifiedness of Israeli force.

Ukraine If Russia has a troll army, why shouldn't Ukraine? With this logic, last February, the country's new Information Policy Ministry announced the launch of its own i- army, based at i-army.org, with plans to challenge the enemy version of events on social media. "I already said more than once that we should effectively combat Russian bots and fake information," Ukraine's information policy minister

Yuriy Stets said. "I think this project will give us many volunteers who are ready to disseminate truthful information and expose fake reports from Russia."

It is not clear how many Ukrainians or Ukraine supporters have yet taken up the cause. The i-army.org site itself, where volunteers can join, is certainly not very appealing to outsiders. It is a crazed and relentless jumble of unflattering stories about Russia - from details about the MH17 air crash, to doping by its athletes, to unsubstantiated allegations from the western media that Putin is a paedophile. "Do not let yourself be deceived - spread the truth!" the site says, rousingly.

More obvious signs of life can be found on the i-army's Twitter page. This is very active, with 12,800 followers, which isn't bad, and retweets regularly runs into dozens or hundreds. Clearly some of its followers have been arguing Ukraine's case online, but the tweets themselves are not very persuasive, offering photographs of captured Russian military hardware, dry political statements and sudden comic memes about Russia's federal reserves, for example.

The account's wallpaper perhaps tells you everything you need to know about the Information Policy Ministry - or the "Ministry of Truth", as some Ukrainian wags prefer. It depicts a group of noble white knights carrying the ministry's logo into battle against, literally, an army of fantastical trolls (who rather incongruously carry the logos of RT television and Russia 24). No matter how sympathetic one might feel towards the Ukrainian cause, it is hard not to feel that this particular region of the conflict needs a lighter touch.

Estimated troops A few hundred.

Favourite subjects Russia, Russia, Russia, Russia, Russia.

UK The so-called "Twitter Troops" of the 77th Brigade were somewhat misunderstood by the media when the new army unit was created last year. In fact social media was just one example of many non-military skills that the specialist soldiers were intended to bring to the army. And in any case, the MoD informs me, it would not be a soldier's job to launch a disinformation campaign on the battlefield, even if they had the time.

You don't hear much about JTRIG in Britain, however, and they do just this kind of thing. Indeed the very existence of the Joint Threat Research Intelligence Group was a national secret until documents from Edward Snowden were published by Glenn Greenwald and Andrew Fishman in 2014. And they reveal a very busy group of people, whose work within GCHQ was intended to help everyone from the police and MI5 to the Department for Children, Schools and Families and the Bank of England.

Some of JTRIG's tactics, such as hacking into websites and setting up sexual "honeypot" stings, sound more or less like conventional spying. Others were carefully designed to manipulate and deceive. In the words of the leaked document, these included "Uploading YouTube videos containing persuasive messages; establishing online aliases with Facebook and Twitter accounts, blogs and forum

memberships ... sending spoof emails and text messages as well as providing spoof online resources; and setting up spoof trade sites."

Some of this sounds reasonable, and frankly welcome, such as disrupting the online activities of terrorists or child abusers. Indeed, if it still exists, JTRIG seems to target specific groups or individuals, rather than trying to influence public opinion. Which groups, however, and who chooses them, might be a legitimate concern. The document mentions the English Defence League, for example, whose members were no doubt not happy to be included. For its part, GCHQ will only say that all its work is legal.

Estimated troops A few dozen.

Favourite subjects Sex, drugs, not travelling to Syria please.

North Korea, South Korea Most North Koreans' experience of social media is none at all, unless they have been given an illicit glimpse by a foreigner or a government official. Facebook, Twitter and YouTube are all officially blocked, just in case. Domestically, there is thus no online opinion for the regime to bother about controlling. (Unless they launch their own version of Facebook, as some believe they plan to.) Across the border, however, just about all South Koreans have smartphones, KakaoTalk and the fastest internet in the world. They also have about 200 North Korean trolls to contend with, according to a report published by a South Korean think-tank, the Police Policy Institute, in 2013. In total the report estimated that North Korean agents had posted 41,373 pieces of propaganda in 2012. (That's about one every two days per agent, which is hardly Stakhanovite.)

Given the extreme strangeness of the regime in Pyongyang, it is easy to presume that they would not know how to talk to a sophisticated southern audience. In fact their approach, as revealed in the report, is rather clever. Instead of hammering people with outlandish and unconvincing Juche propaganda in the usual North Korean way, Pyongyang's trolls focus on areas that are still debated in the south - such as whether to give southerners access to sites (currently blocked) that praise the northern regime. Aware that recently started accounts with little background often arouse suspicion, northern agents also tend to work behind identities stolen from real southern users.

Clearly the problem has been serious enough for South Korea to react, and indeed to overreact. For years the country's National Intelligence Service has been routinely posting messages of its own to attack those coming from the north, and at times these have allegedly strayed into attacks on South Korea's own opposition parties. Last year the country's former intelligence chief Won Sei-hoon was convicted of trying to influence the outcome of the 2012 presidential election in favour of the incumbent Park Geun-hye. A retrial has since been ordered, but in the original Won was alleged to be running a team of nine agents who used at least 658 Twitter identities to post many thousands of messages to discredit the north - and also, in the case of 274,800 messages, to smear President Park's opponents, who were described as, among other things, "leftist followers of North Korea".

Estimated troops 200 (north) 9 (south).

Favourite subject Whether North Korea is a) paradise b) paranoid.

Turkey President Erdogan was taught a lesson by the Gezi Park protests of 2013. Not, unfortunately, that Turks should be allowed to live more freely, but that he should take control of social media, with which they had organised themselves against him. By the end of the summer, the ruling Justice and Development Party (AKP) had begun recruiting a team of 6,000 social media operatives. "We aim at developing a positive political language which we are teaching to our volunteers," a party official told the Wall Street Journal at the time. "And when the opposing camp spreads disinformation about the party, we correct them with valid information, always using positive language." But not always being open about it. When asked to name some of the people who would be correcting this misinformation, the official declined.

Sadly for Erdogan and the AKP, their new army of volunteers proved overenthusiastic and, let's say, under-subtle. In the months that followed it became common for those who even mildly criticised the government to be showered with far from positive remarks. Often the abuse arrived in bursts, from people with not very convincing profiles, making accusations that were not only bizarre but bizarrely similar. For instance when the journalist Emre Kizilkaya criticised the government's handling of a hostage negotiation in October, he found himself repeatedly accused of "Zionism".

At times the "AK Trolls", as they became known, spread false stories. In July 2014, it was reported that they started a fake Twitter account supposedly from the musician Erkan Ogur, used it to tweet controversial comments about the state intelligence services, then complained about "his" tweets to the AKP authorities in Sakarya, who promptly cancelled Ogur's forthcoming concert there. Later, Erdogan's own daughter Sumeyye was apparently recorded asking one of his advisers for help from "our trolls". When recordings allegedly showing Erdogan's own corruption began to spread on Twitter in the spring of 2014, he simply (but not very effectively) shut Twitter down.

Perhaps aware that this Putinesque farce wasn't making the AKP more popular, the party changed tack just before the general elections last spring, launching the New Turkey Digital Office, which would henceforth dish out more conventional online propaganda. "All of our accounts will be officially announced," spokesman Besir Atalay told the Turkish media. "Our messages will be determined at the party headquarters. None of the other accounts would be related to us, including those ones [the trolls]." Nevertheless the AKP lost its majority in the elections. Then regained it in new elections later in the year.

Estimated troops Formerly 6,000, probably still 6,000.

Favourite subjects Standing up to the Kurds, standing up to Russia, standing up to Arabs, standing up to Israel ...

BBC News
Hack attacks cut internet access in Liberia
Saturday, 05 November 2016

Tripoli - Net access in Liberia comes via a single cable that is shared with 20 other nations
Liberia has been repeatedly cut off from the internet by hackers targeting its only link to the global network.

Recurrent attacks up to 3 November flooded the cable link with data, making net access intermittent.

Researchers said the attacks showed hackers trying different ways to use massive networks of hijacked machines to overwhelm high-value targets.

Experts said Liberia was attacked by the same group that caused web-wide disruption on 21 October.

Those attacks were among the biggest ever seen and made it hard to reach big web firms such as Twitter, Spotify and Reddit.

Short bursts

The attacks were the first to send overwhelming amounts of data from weakly protected devices, such as webcams and digital video recorders, that had been enrolled into what is known as a botnet.

A botnet variant called Mirai was identified by security firms as being the tool used to find and compromise the insecure devices.

The source code for Mirai has been widely shared and many malicious hacker groups have used it to seek out vulnerable devices they can take over and use to mount what are known as Distributed Denial of Service (DDoS) attacks.

"There're multiple different botnets, each with a different owner," security researcher Kevin Beaumont told the BBC. "Many are very low- skilled. Some are much better."

'This feels serious' - BBC Africa's Jonathan Paye-Layleh in Liberia

For more than two weeks, my internet has not been working properly. At first I thought it was a problem with my internet provider, which often suffers from slow speeds. But this feels more serious.

Even when you do get online, the connection repeatedly cuts out. I've spent the past week trying to upload some photos and audio to send to London, without success.

A woman who runs a computer club for young people in the capital, Monrovia, tells me that they have been having trouble getting on to Facebook and that their connection has slowed in recent weeks.

The hotel I am staying at in the north-eastern town of Ganta is right next to the network tower of a company that provides my internet service, but the connection is still coming in and out.

The hackers behind the "huge" network that attacked Liberia, dubbed botnet#14, were "much more skilled", Mr Beaumont said.

"The attacks are extremely worrying because they suggest a Mirai operator who has enough capacity to seriously impact systems in a nation state," he wrote in a blogpost.

Media captionEXPLAINED: What is a DDoS attack?

Network firm Level 3 confirmed to tech news site ZDNet that it had seen attacks on telecoms firms in Liberia making access to the web spotty. Other reports suggested mobile net access was affected too.

The attacks varied in length with some lasting only 30 seconds and the longest being sustained for a few minutes. At times the amount of data being funnelled towards Liberia exceeded 600 gigabits per second.

Net access in Liberia comes via an undersea cable whose capacity is shared with many other nations in West Africa.

"They're trying a number of different techniques for short bursts, against the companies who own the submarine cable to Liberia," said Mr Beaumont, adding that commands to botnet#14 seemed to originate in the Ukraine.

Mr Beaumont said the controllers of botnet#14 were refining their control of the attack system but it was not yet clear who it would be turned against next.

A Twitter account, called #Miraiattacks has been set up by a security company to monitor the many different attack targets hit by Mirai botnets. Earlier targets included computer security firms, schools, food-ordering services and gaming sites.

Daily Star London
Anonymous 'hacks Met Police in Million Mask March arrest revenge'
Sunday, 06 November 2016

London - Central London was brought to a standstill as the demonstrators - wearing their trademark Guy Fawkes masks to hide their faces - chanted anti-Government slogans.
But after cops arrested more than 47 rowdy protesters hackers allegedly had their revenge.

The protest was inspired by the work of anonymous - a network of hacktivist groups who have previously attacked the the US government, ISIS and the KKK.

Now The Met's news site - where they earlier reported the number of people arrested in the protest - has been taken down in an apparent attack claimed by hacker 'Crash OverRide'.

Taking credit for the website's domain being taken away the alleged hacker tweeted: "Arrests = Downtime b****".

But even though it happened in the middle of the Million Mask March, The Met police haven't confirmed if the site was hacked.

Speaking to Dailystar.co.uk a spokesman for the Metropolitan Police said: "We'll be speaking to our web supplier about it but it's too early to precisely say what the cause it at this time.

It comes after protesters wreaked mayhem in central London for this year's Million Mask March as police crackdown on violence.

Mayhem erupted in the capital with many protesters dressed in Guy Fawkes masks.

The mob started by gathering at Trafalgar Square and by 9pm cops had made at least 47 arrests for a variety of offences.

Two protesters were detained after refusing to remove their masks, while others were arrested for drugs possession, carrying a weapon and criminal damage.

One clip shared on social media showed the moment officers wrestle a protester to the ground.

Anarchists launched fireworks at Buckingham Palace as the mob made their way through central London.

New York Times
What We're Missing While We Obsess Over John Podesta's Email
Saturday, 05 November 2016
Byline: Zeyned Tupekci

OpEd: I once asked Daniel Ellsberg -- who in 1971 leaked the secret history of the Vietnam War known as the Pentagon Papers -- if he had any regrets. He told me, as he told many others, that he regretted only that he had not leaked them earlier, when they might have had more impact and perhaps shortened the war.

Whistle-blowing, as Mr. Ellsberg did, is a time- honored means for exposing the secret machinations of the powerful. But uncensored release of huge amounts of hacked data does the opposite. Such leaks threaten our ability to dissent by destroying privacy and unleashing a glut of questionable information that functions, somewhat unexpectedly, as its own form of censorship, rather than as a way to illuminate the maneuverings of the powerful.

The latest example of these data dumps comes from WikiLeaks, which is releasing the emails of Hillary Clinton's campaign chairman, John Podesta, in dribs and drabs going back to 2008, when Mr. Podesta was the co-chairman of Barack Obama's transition team.

"Wait," you might think. John Podesta is about as far from dissident politics as you can get. These leaks have produced genuine news. We finally got to see the text of Mrs. Clinton's paid speeches to Goldman Sachs, for example. What's wrong with that? Doesn't that serve the public interest?

The hacked emails did provide the public with some notable information. But any benefit of such mass data releases does not undo their harm. And that harm goes well beyond the possibility that the data was stolen by a foreign government seeking to influence this election.

The victims here are not just Mr. Podesta and the people in his contacts list who are embarrassed or compromised. The victim of leaks of private communication is the ability of dissidents to function in a democracy.

Demanding transparency from the powerful is not a right to see every single private email anyone in a position of power ever sent or received. WikiLeaks, for example, gleefully tweeted to its millions of followers that a Clinton Foundation employee had attempted suicide; news outlets repeated the report.

Wanton destruction of the personal privacy of any person who has ever come near a political organization is a vicious but effective means to smother dissent. This method is so common in Russia and the former Soviet states that it has a name: "kompromat," releasing compromising material against political opponents. Emails of dissidents are hacked, their houses bugged, the activities in their bedrooms videotaped, and the material made public to embarrass and intimidate people whose politics displeases the powerful. Kompromat does not have to go after every single dissident to work: If you know that getting near politics means that your personal privacy may be destroyed, you will understandably stay away.

Data dumps by WikiLeaks have outed rape victims and gay people in Saudi Arabia, private citizens' emails and personal information in Turkey, and the voice mail messages of Democratic National Committee staff members. Dissent requires the right to privacy: to be let alone in our vulnerabilities and the ability to form our thoughts and share them when we choose. These hacks undermine that crucial right.

Mass data releases, like the Podesta emails, conflate things that the public has a right to know with things we have no business knowing, with a lot of material in the middle about things we may be curious about and may be of some historical interest, but should not be released in this manner.

All campaigns need to have internal discussions. Taking one campaign manager's email account and releasing it with zero curation in the last month of an election needs to be treated as what it is: political sabotage, not whistle-blowing.

These hacks also function as a form of censorship. Once, censorship worked by blocking crucial pieces of information. In this era of information overload, censorship works by drowning us in too much undifferentiated information, crippling our ability to focus. These dumps, combined with the news media's obsession with campaign trivia and gossip, have resulted in whistle- drowning, rather than whistle-blowing: In a sea of so many whistles blowing so loud, we cannot hear a single one.

What is the right response, then, to living in a world where we will see more mass hacks of information, and more titillating and occasionally newsworthy private communication made public?

The answer is not simply to tell people to stop writing things down. "Don't discuss things over email if you don't want to see them on CNN" is the new "don't wear a miniskirt if you don't want to get assaulted." That would take us back to the pre-internet world where only the powerful could communicate with ease. People with resources will create their own online gated communities -- buying more expensive, secure devices, hiring specialists and flying around more to meet in person -- while dissident groups with fewer resources will be left behind.

Since these hackers won't stop, we need to build resilience by emphasizing curation, context and ethics, and by no longer acting as if something that has been hacked and dumped is all up for grabs.

Journalism ethics have to transition from the time of information scarcity to the current realities of information glut and privacy invasion. For example, obsessively reporting on internal campaign discussions about strategy from the (long ago) primary, in the last month of a general election against a different opponent, is not responsible journalism. Out-of-context emails from WikiLeaks have fueled viral misinformation on social media. Journalists should focus on the few important revelations, but also help debunk false misinformation that is proliferating on social media.

Those of us who aren't reporters need better ways to respond, too. These hacks are done to steal our attention and to confuse us; the only effective response is to refuse to play this game on the hackers' terms.

In old-school access journalism, journalists trade access for docile coverage, and we are often served gossip or trivia: the kind the powerful would like us to know. In this form of hacked emails, we still get gossip and trivia. But we get the kind the hackers want us to focus on, while distracting us from the real issues.

We can't shrug off these dangers just because these hackers have, so far, largely made relatively powerful people and groups their targets. Their true target is the health of our democracy.

Follow The New York Times Opinion section on Facebook and Twitter (@NYTOpinion) , and sign up for the Opinion Today newsletter .

Zeynep Tufekci is an associate professor at the University of North Carolina School of Information and Library Science and a contributing opinion writer.

Times of India
Soon, separate cyber cell to keep tab on miscreants
Monday, 07 November 2016
Byline: Staff Report

Jaipur - The state police are setting up a separate cyber cell to keep an eye on miscreants responsible for fanning communal passions on social media platforms like Facebook and Twitter.
According to UR Sahoo, ADG, intelligence, special training will be given to cops on social media platform. "The decision was taken to ensure that nobody exploits the reach and penetration of social media to flare up communal passions. It will also deter miscreants from posting venomous texts that is likely to trigger tension," he added.

Sahoo added that the state government had earlier given its nod to setting up of such a unit. The specially trained cops would scan through the social media platforms round-the-clock. The unit would operate from a control room and would be connected to all the police stations across the state.

This unit will work in three different shifts, and any suspicious post will be reported to the police station area or the district SP.

"The social media in itself is such a vast sphere that it would not be an easy task for us to scan every page or post. But having a dedicated unit may minimize these crimes to some degree in the state," an intelligence official said.

Sources said that other state police in Maharashtra and New Delhi have already set up thier cyber cell. "The police in communally sensitive areas had been facing difficult times due to posts on social media. There have been incidents where dubious videos were released and shared on mobile phones. Cops were often caught unaware when such posts and videos were posted," the official said.

The cyber cell has been specifically asked to monitor Facebook pages and posts where people are being asked to gather in large numbers at a particular place. The cyber cell would alert the local station house officer about such post and share real time information.

"The misuse of social media was left unattended by the cops for a very long time, allowing miscreants to use it for provocation and stoking communal fire," Sahoo said.

Bangkok Post
Cyber centres fighting on all fronts
Monday, 07 November 2016
Byline: Wassana Nanuam

Bangkok - Having been set up for two years under the Defence Ministry's policy, the so-called cyber war centres of the Royal Thai Armed Forces are fully capable of countering cyber threats from within and outside of the country, sources say.
The Royal Thai Armed Forces Headquarters (RTAFH) and the three armed forces run their own "cyber centres", with the Army's cyber division serving as the lead centre.

Located in the basement of the RTAFH on Chaeng Watthana Road, the army's cyber division is equipped with military experts in cyberspace who have undergone training in Thailand and overseas and the latest technology.

The army last week changed the name of its technology and communications centre to the cyber centre. The name change followed a major upgrade at the facility of both equipment and personnel.

Although not intended to handle political conflicts in cyberspace, the centre has aided state efforts to tackle issues online such as lese majeste comments. That's why the centre has been perceived as taking aim at political issues, according to experts.

Army commander Chalermchai Sitthisart insisted the cyber centre was established to cope with escalating cyber threats that pertain to the hacking and spreading of misleading rumours online, and national security.

"Also, websites offending the royal institution, and online acts in violation of Section 112 of the Criminal Code [for lese majeste] need to be checked," said Gen Chalermchai.

Ritthi Intharawut, director of the army's cyber centre, said the main duty of the centre is to create a system to prevent hacking into the army's websites and information databases, fight against other threats and develop the army's computer and internet system. The centre has also been training soldiers on cyber security, he said.

Information Operation is another area the centre has been overseeing, with the aim of improving public understanding via the dissemination of news and information, he said.

Fending off cyber attacks and cyber terrorism from outside of the country is also a priority, he said, adding that the ideals and propaganda of terrorists are easily disseminated over the internet.

Maj Gen Ritthi said the centre constantly monitors websites which are sources of distorted information and doctored images undermining internal security and the monarchy. When those threats are detected, the RTAF alerts the Ministry of Digital Economy and Society and the Royal Thai Police, he said.

Due to a large number of websites and Facebook pages containing security threats and lese majeste violations, the armed forces' cyber centres have been divided up to monitor them separately, said an army source.

The Signal Department is involved in similar work, employing many capable programmers, dubbed "cyber warriors", said the source. In addition, the Internal Security Operations Command's coordination and operation Centre No.1 is involved in the military's cyber work.

Wisanu Traiphum, the Centre No.1 director, said his centre is linked to the armed forces' cyber centres, although it has limited resources. Its main charge is to keep a look out for websites insulting the monarchy.

Despite being able to deal with cyber threats on a large scale, the armed forces' cyber centres typically deal with issues on the domestic front, said a source at the RTAFH.

And now the operators of Line and Facebook have agreed to cooperate with the government in fighting the spread of improper and offending messages. The armed forces' cyber centres are facing an even bigger workload, said the source. "We don't spy on people's Line conversations. We only check cases for false rumours," Gen Chalermchai.

Jerusalem Post
ISIS cyber recruiting, financing hits new levels
Monday, 07 November 2016
Byline: Yonah Jeremy Bob

Jerusalem - The Islamic State is considered a pioneer among terrorist organizations regarding innovation in the cyber world, including making leaps forward in sophisticated recruiting and fundraising schemes, according to an advance copy of IDC's International Institute for Counter- Terrorism 2016 cyber trends report obtained exclusively by The Jerusalem Post.
"Unlike in the past when the processes of mobilization, manpower recruitment and training mainly took place in the physical realm, today the Internet has become a central and anonymous arena in which these activities take place," the report says, adding that a deeper "technological focus" gave ISIS and others "a free hand to recruit using an anonymous connection between the recruit and the terrorist organization through the Internet, irrespective of their physical location or standing."

Internet-based manpower recruitment was crucial in light of the need to import foreign fighters to Syria, Iraq and other countries, says the report, and that ISIS disseminated messages on a range of Internet platforms both directly and via secondary agents to maximize its recruitment potential.

Most impressively, "terrorist organizations have recently been investing efforts in adjusting the recruitment content for a specific target audience (narrow casting), such as speakers of various languages or certain professionals. For example, a campaign for the recruitment of children that includes computer games and comics, [and] campaigns for the recruitment of hackers, Web designers and developers for this specific population."

But ISIS has gone even further in this kind of tailored campaigning, reminiscent of the current US election campaign in which both parties tailor their pitches to local state specific issues, using recognizable local terminology.

The IDC report says Isis has "leveraged existing technological platforms more than any other terrorist organization, with one of its prominent 'flagships' reflected in a venture named 'Nasher' (publisher), which is responsible for translating the organization's official materials into various languages and distributing them on Telegram channels."

Further, adapting the message to a specific "target audience is not only part of recruitment, but is also part of the format in creating specialized target audiences for lone wolves on social networks, such as Facebook and Telegram."

The report explains that this technological development increased the "use of advanced communications applications (mostly encrypted) by jihadist organizations in the advanced stages of the recruitment process, such as Telegram, Skype, WhatsApp and Kik."

As with many other areas, ISIS has outplayed al-Qaida in this arena. Al-Qaida continues to operate on a much more limited and less dynamic basis in Web forums and Internet sites, though it is not completely absent from social networks, says the report.

Whereas al-Qaida's size and breath is limited by its emphasis on maintaining a connection between various arenas of jihad and "Al-Qaida Central," ISIS has altered its recruiting and propaganda strategy when necessary, notes the report, recently moving from seeking volunteers in Syria and Iraq to focusing on "the 'far enemy' and on encouragement for 'lone wolf' attacks and cyber attacks against the West" with no strings attached to its central hub.

Moreover, the report indicates that "the competition between the Islamic State and al-Qaida is... manifested in a propaganda battle that includes...'hashtag wars' and publications on ideological matters.

Al- Qaida supporters accuse ISIS of "establishing an Islamic Caliphate in sin, killing innocent Muslims, conduct contrary to sharia, and deviation from the principles of Islam."

ISIS supporters accuse al-Qaida of "deviating from the path of Osama bin Laden, and describe it as an organization that has run its course and is occupied with survival and the narrow interests of its leaders," according to the report.

Recruiting is not the only place that ISIS and other terror groups have revolutionized in a short time.

ICT's report describes the field of terrorism financing as significantly changing in parallel with technological development, both in terms of fundraising and the transfer of funds.

"The Internet has enabled the practice of fundraising and the transfer of funds from any location to any location in the world," the report says.

"It has expanded the circle of fund-raisers and the ability to raise capital through them and directly from the potential target."

Furthermore, "the network organizational structure has also enabled the independent mobilization of funds by terror cells and foreign fighters on their way to battle arenas, eliminating the need to find ways to transfer money from country to country."

Put differently, just as US election campaigns have shifted from a sole focus on fundraising from big-money bundlers to a large volume of small online contributors, ISIS and others have done the same with their fundraising.

This empowers smaller cells to even do their own fundraising without having connections to high- net-worth individuals or senior terrorist operatives.

In addition, "The Internet also serves as a preferred arena for fundraising due to the sense of security that it gives the donor who tends to believe that his identity remains anonymous, even if this is not always the reality," says the report.

Press TV
Cyber strike empowered Iran: Nuclear chief
Monday, 07 November 2016

Tehran - Iran's top nuclear official says the 2011 cyber attack by the US and Israel against the Iranian nuclear energy program worked against their intended objectives and helped improve the Islamic Republic's readiness against such acts of sabotage.

The head of the Atomic Energy Organization of Iran (AEOI), Ali Akbar Salehi, said the deployment that year of a malware dubbed Stuxnet against Iran's nuclear facilities made the country realize how it should prepare against such attempts, Tasnim news agency reported on Saturday.

He said Iran can fill "an entire exhibition room with the West's acts of industrial sabotage against Iran, things like this very Stuxnet virus."

"They give us equipment in which they have planted explosives so that it would blow up sometime later, or they interfere with the equipment so that... it later damages the whole system."

He explained that as an act of precaution, Iran has been checking the pieces of equipment it buys for any potential interference.

"We don't immediately put to use whatever equipment that we buy; rather, we do all kinds of tests on it, and we don't use it before there is complete assurance" that it is safe, Salehi said.

"In fact, before the Stuxnet, we were not this careful, and the attack opened up a new science to us. Just by testing different equipment for [potential] industrial sabotage, we learn a lot," he said. "We owe them a thank you, of course," he said jokingly, referring to the US and Israel.

The Washington Post reported in June 2012 that the US National Security Agency (NSA), its spy service CIA, and Israel's military had worked together to launch Stuxnet against Iran's nuclear facilities.

Salehi also said Iranian officials are taking the necessary measures to pursue litigation against the perpetrators of the cyber attacks against Iran.

Meanwhile, Swiss prosecutors have said that they had found malware on a number of computers at a hotel in Geneva that hosted talks between Iran and six other countries on the Islamic Republic's nuclear program last year.

The hotel, believed to be Hotel Président Wilson, was raided on May 12, 2015 after the state prosecutor's office, the OAD, launched an investigation over suspicions that illegal intelligence services were operating in Switzerland.

The OAD has, however, had to close the case after failing to establish who was behind the cyber attack that implanted the malware on the computers.

The talks at the Swiss hotel and elsewhere led to the conclusion in Vienna on July 14, 2015 of a nuclear agreement between Iran and the five permanent members of the United Nations Security Council -- the United States, Britain, France, China and Russia -- plus Germany.

Also on Saturday, Salehi announced the inking of the first document of cooperation between Iran and the International Thermonuclear Experimental Reactor (ITER) project, an international nuclear fusion research and engineering megaproject.

ITER will be the world's largest magnetic confinement plasma physics experiment, established in southern France. Salehi said he hoped that Iran would have joined the ITER project by the end of 2016.

He said Iran and the ITER Organization have committed under the document signed on Saturday to keep information exchanged between them confidential.

The document was signed by Salehi and Bernard Bigot, who is the director general of the ITER Organization, in Tehran.

Vice Canada

Overnight Security Guards Keep Finding Classified or 'Protected' Documents Around Parliament

Wednesday, 09 November 2016

Byline: Rachel Brown

A number of federal departments, including Canada's spy agency, have been careless with classified or secure government documents.

Since the Liberals took office last November, there's been more than 10,000 incidents in which such documents were mishandled or improperly stored, according to a 93-page report tabled last week in the House of Commons in response to a question from Conservative MP Gord Brown. The Conservatives have been quick to condemn the government, but it's not clear how many similar incidents occurred when they were in power.

The report, first cited by the CBC, provides few details about what the documents are or how exactly were mishandled. It's not clear whether any of the incidents compromised security or privacy.

Public Services and Procurement Canada and Global Affairs are the worst offenders, reporting a combined 5,624 instances where employees didn't abide by the security protocols for the documents.

The Canadian Security Intelligence Service (CSIS) reported 659 such instances, 12 of which "required further investigation." And the Communications Security Establishment, Canada's foreign intelligence agency, reported 491 incidents, although the agency notes that none of the documents ever left Parliament.

Officials at the Canada Border Services Agency reported 77 incidents where protected documents were mishandled.

A number of cabinet ministries also confessed to mishandling documents, including 11 such incidents reported by the office of Democratic Reform Minister Maryam Monsef.

Public Safety Minister Ralph Goodale's office--which is responsible for national security--reported six instances of document carelessness. The department overall reported more than 270 incidents, many of which seem to have been discovered during the night shift by parliamentary security officials, including "where cabinets were found unlocked by security during evening patrols."

"For all instances where a cabinet was left unlocked, it is impossible to confirm if the cabinet contained any Protected or Classified documents," the department states in the report.

Dozens of other departments, including the Transportation Safety Board and the Public Prosecution Service, reported zero instances where secure or protected documents were mishandled. According to the report, no employee was stripped of their security clearance as a result of any of the incidents.

Opposing MPs have expressed alarm over the reported incidents.

"We're a G7 country, and when we do not handle these kinds of documents with the appropriate way it's amateur hour," Conservative public safety critic Tony Clement told the CBC. "It might be a signal to our allies and our partners that we cannot be trusted."

Under the Conservative government in 2008, the foreign affairs minister at the time, Maxime Bernier, came under fire for leaving classified government documents at the Montreal home of his girlfriend, who reportedly had ties to a criminal biker gang. Bernier eventually resigned over the matter.

At the time, MP Ralph Goodale, who now serves as the public safety minister, said former prime minister Stephen Harper had "a lot of explaining to do."

Early in 2015, in response to the Bernier incident, the Conservatives imposed a revamped policy on secret federal cabinet documents to prevent leaks. It required all potential breaches, no matter how small, to be reported to the Prime Minister's Office or the Privy Council Office right away.

Montreal Gazette
Coderre cancels inquiry into police surveillance
Wednesday, 09 November 2016
Byline: René Bruemmer

Montreal - Two days after he announced Montreal inspector general Denis Gallant would hold an ad hoc "administrative review" into the police surveillance scandal enveloping the police force and city hall, Mayor Denis Coderre said Tuesday Gallant's investigation is no longer necessary and has been cancelled. Given that a provincial inquiry called by Premier Philippe Couillard last week is already looking into the Montreal police force's surveillance of La Presse journalists, including one who had been investigating a $444 ticket issued to Coderre, as well as the Sûreté du Québec's monitoring of reporters in a separate case, Gallant's inquiry is no longer necessary, the mayor said in a statement.

Coderre said he obtained the assurance Tuesday morning of Quebec Public Security Minister Martin Coiteux that the provincial inquiry will investigate the Montreal police's surveillance techniques. Having another inquiry, Coderre said, risks becoming "counter-productive." Montreal city council's public security commission is also investigating the matter.

Coderre had announced Gallant would organize the inquiry outside of his duties as inspector general, in which his department is charged with investigating municipal contracts and reports to city council. Gallant said he accepted to do the job pro bono, and said it would not affect his independence. But opposition party members said using Gallant for such a highly politicized inquiry in which the mayor is implicated threatened to undermine Gallant's credibility as inspector general.

Tuesday's reversal shows Coderre is mismanaging the surveillance file, said Alex Norris, the Projet Montréal councillor who sits on the city's security commission.

"This is yet another example of improvisation on the part of Mr. Coderre and further evidence he has fully lost control of the dossier on espionage of journalists by the Montreal police force," said Norris, adding that the Quebec government made it clear last week their inquiry included investigating the Montreal police force. As well, Norris said, the law makes it clear that Gallant's mandate as inspector general is a full-time position and he is not allowed to take on other duties.

In Quebec City, Couillard stressed the need for distance between elected officials and the police.

"We should be all extremely careful ... of any significant contacts between elected officials and the police force, at any level," Couillard said. "This is why we must take a step back now, because I see that tempers are flaring up a little bit in recent days ... and have a real independent commission looking into this, presided by a judge."

Toronto Star
Ottawa should protect press
Wednesday, 09 November 2016
Section: editorial

When it was revealed last week that Montreal police had been spying on Patrick Lagacé, a columnist for La Presse newspaper, in an effort to uncover his sources, we decried the practice as a "troubling threat to freedom of the press" that was "unprecedented in Canadian history." It turns out we were only half right: it was indeed troubling, but hardly unprecedented.
In the week since, it has come to light that, in fact, at least 10 other reporters in Quebec have had their cellphones surveilled by local or provincial police since 2008, some for more than five years. In the wake of these alarming disclosures, the province has announced that it will launch a public inquiry into press freedom and police surveillance of journalists.

That's a welcome development, especially as crucial questions remain about the possible complicity of some politicians and senior police officials in the spying. But the problem is not limited to Quebec. The revelations have also exposed a gap in the federal law that protects journalists and their sources - one that Ottawa should move quickly to bridge.

It should not surprise us that police were tempted to spy on journalists to expedite their investigations. What's more concerning is that several justices issued warrants that, based on what we know, seem to be inconsistent with the spirit of the Supreme Court's rulings on the protection of journalistic sources.

In each case, the journalist being monitored was suspected of nothing untoward. He or she was privy to no imminent threats to public safety. Rather, the journalists in question were simply doing their job:

telling stories that happened to be embarrassing to the police or to government. The warrants appear to have been sought to identify existing whistleblowers and intimidate prospective ones. Given the chilling effect such surveillance is likely to have on the media, it's hard to conclude that, on balance, democracy was well served by the decisions.

Moreover, the Supreme Court has said journalists should be able to protect their sources if they can show doing so is in the public interest. No such opportunity was provided to them. It seems that neither legislation nor jurisprudence provides sufficient protection for the journalist-source relationship that the top court has said serves a "vital role" in democracy.

No one would speak to a reporter if they believed he or she was unable to protect a source or, worse, was collecting information on behalf of police. Journalists must be free to seek the truth from all manner of sources - whistleblowers and criminals included - to keep the public informed on the issues that matter.

That's why Ottawa should take seriously the suggestion of Sen. André Pratte, a former editorial page editor at La Presse, who is calling on the government to convene a Senate-Commons committee to study the current safeguards for journalists and their sources and quickly suggest improvements. The existing legislation was written before technology vastly expanded both the set of journalistic tools and the state's ability to spy on them. It should be updated for the digital world.

The recent stories out of Quebec raise important questions about troubling police practices in that province and to what extent politicians were involved. A public inquiry is the right response. But the protection in law of freedom of the press is a matter of national importance. Ottawa should do its part.

Journal de Montréal
Mieux protéger les journalistes que les citoyens?
Tuesday, 08 November 2016
Byline: Pierrot Péladeau

Blogue - Le film 'La vie des autres' se déroule en Allemagne de l'Est à l'époque où, volontairement ou sous la contrainte, un citoyen sur sept espionnait ses voisins pour la Stasi (Ministère de la Sécurité d'État)
Est-ce souhaitable à l'égard de la surveillance policière des communications ? Ou même possible ? Coup d'oeil sur la réalité matérielle des choses.

Évidemment, nous ne pouvons que nous inquiéter des révélations sur le fait que la police a surveillé les communications d'autant de journalistes dont aucun n'était pourtant soupçonné de quelque crime que ce soit.

Premièrement, à cause des rôles clés que le journalisme a joués dans l'émergence, puis pour la vitalité des démocraties modernes.

Deuxièmement, du fait les journalistes s'avèrent être le proverbial canari dans la mine. Lorsque la démocratie est attaquée, les journalistes se retrouvent souvent en première ligne de ceusses qui subissent la répression sous diverses formes. Et sinon en première ligne, le groupe sur lequel les attaques sont les plus voyantes, les plus difficiles à dissimuler.

Troisièmement, les journalistes et les médias d'information se situent à des noeuds de communications sociales. Attaquer ces noeuds provoque donc des répercussions sur l'ensemble de la société.

C'est sur ces noeuds de communications que je m'attarderai surtout dans ce texte et d'autres qui suivront. Voilà une perspective sous laquelle l'empressement dont a fait montre la classe politique québécoise à mieux protéger les journalistes de la surveillance policière ne me rassure pas du tout.

Révéler qu'on a surveillé pendant cinq ans les télécommunications de Denis Lessard revient à déclarer qu'on a surveillé les actions de toute la classe politique québécoise

La réalité à laquelle nous sommes confrontés m'apparait d'ailleurs beaucoup mieux représentée par les hésitations manifestes des gouvernement Trudeau, Gendarmerie royale (GRC) et Service canadien du renseignement de sécurité (SCRS) à nous offrir quelque garantie concrète sur ce même sujet.

Communication 101

Rappelons une évidence. Dans son expression la plus simpliste, une communication est une mise en relation entre deux personnes au minimum. Conventionnellement, on nomme ces deux personnes, Alice et Bob.

Bien sûr, une communication électronique implique bien d'autres acteurs de soutien: les fournisseurs de télécommunications, d'appareils et d'applications, notamment. J'en traiterai dans le prochain texte. Pour l'instant, concentrons-nous uniquement sur les acteurs principaux.

Si la policière Ève (autre nom conventionnel) espionne les communications d'Alice, alors elle espionne aussi Bob. En fait, Ève espionne aussi toutes les Carole, David, François, Grace et autres personnes avec qui Alice se retrouve en communication durant la période de surveillance.

Le cas Denis Lessard

Appliquons ce constat simple au journaliste Denis Lessard. On comprend alors immédiatement pourquoi Philippe Couillard a été si prompt à réagir, puis à promettre la mise en place d'une commission d'enquête publique.

Denis Lessard est journaliste et commentateur couvrant l'actualité parlementaire et politique québécoise. Son travail le met donc quotidiennement en communication avec des députés, des attachés et assistants politiques, des militants.

Or, ces communications de Denis Lessard ne se limitent surtout pas aux déclarations officielles. Loin de là ! Une très large part comporte, sous le couvert de l'anonymat, des déclarations officieuses, confidences, ballons d'essai, pistes à explorer, fuites et autres échanges concernant tout autant le propre camp de l'interlocuteur qu'un camp adverse. Ces communications sont le théâtre d'innombrables jeux discrets indispensables, non seulement au travail du journaliste, mais à l'action politique elle-même.

L'affirmation d'une immunité personnalisée n'est-elle pas un terrible leurre lorsqu'il s'agit de télécommunications ?

Révéler qu'on a surveillé pendant cinq ans les télécommunications de Denis Lessard revient donc à déclarer qu'on a surveillé les actions de toute la classe politique québécoise.

Ainsi, derrière les bannières de la liberté de presse et de la démocratie dans lesquelles se sont immédiatement drapés les membres de l'Assemblée nationale, il y a un puissant réflexe d'autodéfense des députés. D'où dès le jour des révélations, la proclamation immédiate qu'il faut que les journalistes profitent d'une relative immunité contre la surveillance policière qui soit équivalente à celle des députés.

Mais l'affirmation d'une telle immunité personnalisée n'est-elle pas un terrible leurre lorsqu'il s'agit de télécommunications ?

Qui sont les députés ?

Il est aisé d'identifier qui sont les députés, donc qui pourraient bénéficier d'une immunité relative. Les députés sont officiellement désignés par le Directeur général des élections au terme de la compilation des votes.

Les députés doivent pouvoir échapper à la surveillance arbitraire de leurs communications. Et pas seulement pour préserver le libre jeu politique nécessaire à la vie démocratique. Ils doivent également pouvoir y échapper à cause de leur rôle de médiation entre les citoyens et l'appareil d'État. Interrogez n'importe quel député. Vous apprendrez que dans leur comté ils doivent recevoir mille confidences souvent intimes sur les situations financières, sociales, médicales et souvent même psychologiques de leurs commettants.

Or, si les députés doivent jouir d'une immunité, leurs personnels politiques oeuvrant tout autant sinon plus dans le jeu politique et de la médiation citoyens-État ne le devraient-ils pas aussi ?

Et si les personnels politiques des députés, pourquoi pas les personnels des partis ?

Et si les personnels des partis, pourquoi pas les militants politiques de ces mêmes partis ?

Et si les militants des partis, pourquoi pas les personnes qui, à un moment ou un autre, font aussi de l'action politique à travers d'innombrables regroupements ou organisations parsemant la société civile ?

Toutes ces personnes exercent leur liberté d'association, d'opinion et d'action politique qui, lorsque licite, doit aussi échapper à la surveillance policière de leurs télécommunications. Et toutes peuvent aussi devenir des Bob, Carole, David, François ou Grace appelées à communiquer avec une Alice, journaliste.

Qui sont les journalistes ?

Or s'il faut garantir une relative immunité aux journalistes, qui est journaliste ? C'est une question à laquelle on se bute depuis longtemps.

Cela peut sembler évident dans le cas d'un Denis Lessard ou autre personne qui fait profession de journaliste pour un grand média comme La Presse, Radio-Canada ou Le Journal.

S'il faut garantir une relative immunité aux journalistes, qui est journaliste ?

Mais si un Patrick Lagacé qui fait professionnellement du commentaire pour un grand quotidien est considéré comme un journaliste, pourquoi pas moi qui - comme de nombreux autres - fait aussi du commentaire pour un grand quotidien même si ce n'est pas à temps plein ?

Et si moi et de nombreux autres journalistes à temps partiel, pourquoi pas les bénévoles qui publient le journal communautaire mensuel de ma municipalité de banlieue ?

Et si ces journalistes bénévoles, pourquoi pas ceusses qui tiennent blogues sur l'actualité de leur municipalité, comté ou domaine d'activité sociale ?

Toutes exercent leur liberté d'expression et d'opinion journalistique. Toutes sont autant d'Alice, journaliste, qui doivent échanger aussi avec autant de Bob, Carole, David, François ou Grace oeuvrant plus ou moins sur quelque terrain politique.

Isolation est incompatible avec communication

C'est ici que les proclamations de nos députés québécois apparaissent surréalistes en contraste avec les louvoiements des représentants du gouvernement fédéral, de la GRC et du SCRS.

Un, comment peut-on protéger la démocratie en immunisant de la surveillance policière que quelques-uns parmi tous les citoyens ?

Deux, comment même garantir une immunité relative à quelque Alice, journaliste, quand quelque Bob faisant l'objet d'une surveillance policière licite peut à tout moment établir une communication avec elle ? Ou avec quelque député ?

Trois, comment d'autant plus alors que notre propre Centre de la sécurité des télécommunications canadien (CST) participe à des opérations de surveillance de masse de la NSA ? Ou que nous savons que nos corps de police peuvent demander de surveiller les plusieurs milliers d'abonnés dont les communications sont relayées par une tour d'antenne cellulaire ?

Qu'est-ce que ces attaques sur des journalistes révèlent sur la surveillance de communications de toute personne sur laquelle ne repose aucun soupçon ?

On ne peut insoler les communications de quelques personnes en particulier. Encore moins lorsque ces personnes, journalistes ou députés, constituent des noeuds de communications intenses.

Autant dans le cas de la Russie présentement, on imagine aisément comment la démocratie est sapée par la surveillance policière généralisée des journalistes, des députés ainsi que des militants politiques ; autant il faut concevoir comment la démocratie serait tout aussi efficacement sapée si seuls les journalistes et les députés bénéficiaient d'une immunité alors que le reste de la population pourrait faire l'objet de surveillance policière de leurs communications en absence de tout soupçon d'activité criminelle.

Réalisme

Les journalistes doivent donc canaliser leur juste indignation à enquêter non seulement sur les attaques à la protection de leurs sources, mais sur comment ces attaques révèlent toute forme de surveillance de communications de toute personne sur laquelle ne repose aucun soupçon.

Quant aux députés de l'Assemblée nationale, ils ne doivent accepter qu'une commission d'enquête publique dont le mandat explorerait et résoudrait, par-delà la protection des journalistes et députés, ce contexte qui permet en pratique la surveillance des télécommunications de tous les citoyens sur lesquels ne repose pourtant aucun soupçon.

Je vous reviens sous peu sur d'autres dimensions de la même question.

Global Times
US perverse in opposing China's cyber law
Wednesday, 09 November 2016

Byline: Staff reporter

Beijing - China's top legislature on Monday passed a cybersecurity law, which drew criticism and doubts from mainstream Western media. James Zimmerman, chairman of the American Chamber of Commerce in China, accused the law of creating obstacles to foreign businesses in China and called the provisions "vague, ambiguous, and subject to broad interpretation by regulatory authorities." Some said the law is a setback to the freedom of expression as a closed-door approach. The Chinese public is tired of those hackneyed accusations.
Cybersecurity is a top priority nowadays. A country as big as China must have a cybersecurity law and clear cyber development strategies. It is understandable that big Western companies in China do not want any regulations. But it is unrealistic - how can they urge China to strengthen law enforcement on the one hand and reject the governance of authorities for their own interests on the other?

All the big powers are cautious about whether national security will be subject to cyber technologies. The US has been one of the most aggressive. It claims it is a target of the most cyber attacks from overseas and has kept the highest alert on foreign IT products. Yet the PRISM scandal reveals that the US is the very country that has no sense of rules in the cyber world. Its wiretap and cybersecurity sabotage in other countries have gone beyond international law and morality.

Whenever China passes a law, some Westerners will voice their objections. It is a twisted mentality. US companies in China and officials in Washington clearly understand the necessity of legislation in China and that the companies are subject to Chinese laws. But they seem uncomfortable when it comes to practice.

The new law requires firms to store their data in China and submit them for security reviews to move the data overseas. If such supervision has to be given up, it means China will be laid bare. Will the US allow Chinese enterprises to buy a US high-tech company, transmit all data concerning the US to China and submit them to China's security authorities?

US flagship Internet enterprises have expanded across the globe like an invincible armada, but suffered a setback in China. They attributed their failure to "unfair treatment." But China's rules are for all enterprises. If "unfair treatment" does exist, it's the opposite. Foreign Internet companies operating in China can always publish some information that is forbidden on Chinese websites.

China won't abandon the policy of opening-up. Enhancing exchanges with the outside world is one of the lifelines of China's development and progress. But foreign institutions should respect Chinese laws, and foreign governments and media should encourage such respect.

Exchanges between China and foreign countries will be a mutually beneficial and win-win process. Without a sound legal system in China, the continuous increase of communication cannot be sustained. China must take legislation into its own hands. The American habit of criticizing China's legislation under an imperialistic mind should have been changed long ago.

New York Times
Julian Assange Releases More Emails and Defends WikiLeaks' Mission
Wednesday, 09 November 2016
Byline: Steve Eder

New York - Julian Assange operates from the Ecuadorean Embassy in London, where his internet connection was recently cut off. But that has not stopped him from being one of the most significant and unusual players in the 2016 election campaign in the United States.
His WikiLeaks platform has released tens of thousands of hacked emails from inside Hillary Clinton's campaign and the Democratic National Committee, making Mr. Assange a reviled figure among supporters of the Democratic nominee and a hero to backers of Donald J. Trump.

On Tuesday morning, Mr. Assange weighed in one last time as Americans headed to the polls, releasing a statement that offered an explanation for making the leaks public, an assertion of impartiality and a defense of the WikiLeaks mission.

"The real victor is the U.S. public, which is better informed as a result of our work," Mr. Assange wrote, adding that his organization publishes information as quickly as possible and "as fast as the public can absorb it."

"This is not due to a personal desire to influence the outcome of the election," he said.

Four years ago, Mr. Assange sought and was granted asylum in the Ecuadorean Embassy in London while he was being pursued in a Swedish rape investigation, which he said was a cover for a United States effort to extradite him for publishing a trove of National Security Agency documents.

Ecuadorean officials have not sought to evict him, but last month said that his internet access was disabled out of fear that the country was being drawn into Mr. Assange's efforts to interfere with "electoral processes."

Mr. Assange's operation did not fold, but continued to publish daily releases of emails stolen from the accounts of John D. Podesta, the chairman of Mrs. Clinton's campaign. WikiLeaks published another installment on Tuesday, bringing the total number of messages made public to more than 58,000.

The Clinton campaign has declined to authenticate or comment on the emails, saying that the hack, which American intelligence officials believe originated in Russia, was part of the Russian government's efforts to meddle in the election to benefit Mr. Trump.

The emails, at times, have been embarrassing to the Clintons and their closest aides, revealing confidential and candid details about the inner workings of the campaign and the Clinton Foundation. It

has also shined a light on the Clintons' private work, including lucrative speeches for banks like Goldman Sachs.

While Mr. Assange has made no secret of his dislike for Mrs. Clinton, he said in his Tuesday statement that WikiLeaks published the emails because it had the material and, "It would be unconscionable for WikiLeaks to withhold such an archive from the public during an election."

The lack of leaks pertaining to Mr. Trump, Mr. Assange said, resulted from the fact that his organization was not in possession of Mr. Trump's information. "We cannot publish what we do not have," he wrote.

He went on to criticize The New York Times for withholding "evidence of illegal mass surveillance of the U.S. population for a year until after the 2004 election," which he said denied vital information to voters about George W. Bush.

Mr. Assange, though, has faced similar criticism, with the suggestion that the leaks of emails from the Clinton campaign and the Democratic National Committee were timed to inflict maximum damage or blunt negative stories about Mr. Trump.

A first batch of Democratic National Committee emails -- which led to renewed anger about the party's treatment of Bernie Sanders's campaign -- were released on the eve of the party's summer convention.

In the final month of the campaign, WikiLeaks unloaded the emails of Mr. Podesta, which cover a period of several years ending in the spring of 2016. The first portion of those emails were published the same day that a recording surfaced where Mr. Trump was caught on a hot microphone making lewd statements.

London Times
Brazilians suspected as GCHQ investigates Tesco cyberattack
Wednesday, 09 November 2016
Byline: Multiple reporters

London - The cyberattack on 40,000 Tesco Bank accounts "looks unprecedented", the chief City watchdog said yesterday, as it emerged that GCHQ is helping to investigate the crime.
Reports from victims pointed to Brazil as the origin of the biggest hack to strike a British bank, but the country's authorities have not yet been contacted by their British counterparts.

Tesco said that it had been hit by "a systematic, sophisticated attack" with 20,000 customers having an estimated £17 million drained from their accounts. The bank has frozen all online transactions and many customers have had their debit cards blocked.

Andrew Bailey, chief executive of the Financial Conduct Authority, told MPs that he was worried about weaknesses in banks' IT systems. He said: "The heart of the concern is what is the root cause of this and what does it tell us about broader threats."

The National Cyber Security Centre, a new part of GCHQ that tackles online crime, confirmed that it was providing "on-site assistance" to Tesco. It is working alongside the National Crime Agency to investigate.

Several customers said that fraudulent transactions were made in Rio de Janeiro. Adam Hawkins had £279 stolen in a contactless payment to a company called Parada Do Lanche. Another customer noticed four attempted transactions, two of which were successful, made minutes apart in Rio de Janeiro.

Police in Brazil said that they had not received any complaints from banks or individuals about the cyberattack, and were unaware of any action being taken to investigate. Few in Brazil will be surprised that the country is suspected of being the source of the attack because it is ranked second -- after Russia -- for the number of cyberattacks carried out from its soil.

The problem has become so chronic that many foreign tourists have trouble withdrawing money from cash machines because British banks often register such transactions as automatically suspect. Many others have their credit cards cloned and money siphoned from their accounts.

Brazilian legislators have been slow to respond to the threat, and lenient penalties for hacking do little to deter cybercrime. Hackers can expect prison sentences of less than a year if caught, compared with sentences of up to ten years and hefty fines in America.

Having originally bought hacking software from eastern Europe, Brazilians have developed their own tools to clone credit cards, break into online banks and carry out phishing attacks. In 2015 Brazilian banks lost more than £440 million to online fraud, though many companies are reluctant to report figures for fear of losing consumer confidence, experts say.

Tesco Bank declined to provide more details of the attack and did not respond to requests to comment on whether all customers had been refunded.

Behind the story

Brazil is surfing the global cybercrime wave, with weak legislation and enforcement creating a hacker's paradise where online pirates siphon billions from the world economy (James Hider writes).

The Igarape Institute, which studies crime in Latin America, said last year that cybercrime rose by 197 per cent in 2014, while data theft accounted for up to $4.7 billion in 2013.

Online security experts have identified some hackers posting videos of themselves on YouTube rapping about their crimes with lyrics such as: "We steal from the rich, like Robin Hood."

Poor security has been compounded by the fact that Brazilians are among the most dedicated web users in the world. Almost half of the country's banking transactions are online. Suspicious sites grew by 83 per cent before the Olympic Games.

Associated Press
US official: Security controls 'working' despite NSA theft
Wednesday, 09 November 2016
Byline: Staff report

Washington - The top U.S. counterintelligence official announced that secret government data is vulnerable to thieves, such as the National Security Agency insider accused of working undetected for more than 20 years to steal a large trove of classified material, even as he defended the security controls put in place after the Edward Snowden theft.
"I believe the reforms are working very well. I think we've done an amazing job in the intelligence community and across the government in executing our reforms," said Bill Evanina, the chief counterintelligence and security adviser to the national intelligence director. "However, I will say that if someone wakes up tomorrow and they make a decision that they're going to steal data from the government, they will be successful at it."

Evanina told The Associated Press in a recent interview that no matter how good security controls are, they will never catch every insider or hacker -- and they must be continually improved because of technological advances. His extensive comments followed the August arrest of former NSA contractor Harold Thomas Martin III, 51, of Glen Burnie, Maryland. Martin remains in custody after a judge deemed him to be a flight risk.

Federal prosecutors said Martin illegally removed highly classified information, storing it in an unlocked shed, hi car and his home. Court documents say investigators seized, conservatively, 50 terabytes of information, or enough to fill roughly 200 laptop computers.

Evanina said that since the Snowden breach in 2013, enhanced efforts to counter insider threats in the nation's spy shops have not only uncovered improper activity and situations ripe for possible breaches but have identified employees who might need help. He would not detail the activity uncovered.

Yet there are indications the government might have missed red flags in Martin's personal life. Prosecutors have alleged that he had a binge-drinking habit -- Maryland court records show a 2006 drunken driving charge involving someone of the same name -- and kept firearms concealed from his wife. Defense lawyers said Martin, who like Snowden had worked as a Booz Allen Hamilton contractor, had mental health issues that contributed to him being a "compulsive hoarder" over the course of two decades.

National security breaches have evolved in recent years from unearthing moles working for foreign governments to stopping intelligence workers before they leak or share documents with journalists, Evanina said.

Things changed with Chelsea Manning, a former intelligence analyst in Iraq, who was sentenced to 35 years at the military prison in Leavenworth, Kansas, for leaking more than 700,000 secret military and State Department documents to Wikileaks.

"It was a leak," he said. "It was a big sea change for us."

After Manning, President Barack Obama issued an executive order setting up a National Insider Threat Task Force and requiring federal agencies that handle classified material to seek out possible double agents or prospective leakers.

Then came Snowden, a man Evanina likens to a "shop vac."

"Snowden raised the bar and provided a new level of vulnerability of big IT systems," Evanina said. "Again, it was leaking."

Most of the technological reforms came after Snowden, but others have been in place for several years.

Evanina said agencies are continuously monitoring key indicators like a slowed career, divorce or bankruptcy that could signal a stressed or disgruntled employee on the brink of installing malware, sneaking out with classified material or showing up at work with a weapon.

He shuns requiring body or package searches that would damage trust built with some 4 million Americans who hold security clearances, including 1.3 million vetted to handle top-secret materials.

"We have to weigh: 'How do we garner trust without being "A Clockwork Orange" or "Big Brother"?' " Evanina said, referring to a futuristic movie about behavioral modification and George Orwell's novel "1984" where every citizen is under surveillance.

V. Miller Newton, chief executive officer of PKWARE, cited a Government Accountability Office report that said the number of security incidents at federal agencies rose from 5,503 to 77,183 between fiscal 2006 and fiscal 2015. That's a 1,303 percent increase.

"The fact that this is not the centerpiece of these [presidential debates] is really disturbing to me," he said.

James Lewis, an internationally recognized expert on cybersecurity, said Martin should not have been able to get the material out of the building where he worked.

"Part of what the expanded monitoring would have done is notified NSA that someone was downloading material," he said. "It might have worked. Maybe it notified them. We don't know. I kind of doubt it, but that would be the happy-face story."

Tribune de Genève
« Nous détectons plusieurs cyberattaques par mois »
Wednesday, 09 November 2016
Byline: Journaliste maison

Berne, Suisse - Le chef de la division informatique du Service de renseignement de la Confédération (SRC)dévoile les coulisses de la traque aux pirates informatiques
C'est lui qui repousse les cyberattaques pour le Service de renseignement de la Confédération (SRC). Et qui, depuis que la Suisse a voté oui à la nouvelle Loi sur le renseignement, peut aussi contre- attaquer. Nous rencontrons le chef de la division informatique du SRC au siège du Service de renseignement, dans la banlieue de Berne. C'est la première fois qu'il accorde une interview - sous couvert d'anonymat. Après avoir déposé carte d'identité et téléphone portable à l'entrée, nous pouvons commencer l'interview. Notre interlocuteur est un homme avenant d'à peine plus de 40 ans, qui ne correspond ni au cliché de l'agent ni à celui du génie de l'informatique. Auparavant dans le secteur privé, l'homme travaille « depuis longtemps » pour le SRC. Sous l'oeil vigilant de la responsable de la communication, le chef de la division informatique répond sans ambages - mais s'arrête immédiatement lorsqu'il est question de détails opérationnels.

La nouvelle Loi sur le renseignement a été clairement acceptée. Qu'est-ce que cela signifie pour votre division?

Jusqu'à présent, nous nous heurtions à des limites lorsque nous avions affaire à une cyberattaque. Prenez l'incident survenu au cours des pourparlers sur le programme nucléaire iranien en 2015 à Genève. Nous avons enregistré une attaque menée avec un virus informatique contre des systèmes informatiques d'hôtels de luxe. Ainsi, il est, par exemple, possible d'écouter des appels téléphoniques. Nous avons pu détecter l'attaque et identifier le logiciel malveillant. Mais, à l'époque, il nous manquait la base légale pour obtenir davantage d'informations sur les auteurs de l'attaque. Nous n'avions pas l'autorisation de pénétrer dans le réseau informatique ennemi pour y recueillir des informations et, si nécessaire, prendre des contre- mesures.

Allez-vous désormais rattraper cela?

La nouvelle loi n'entrera en vigueur que le 1er septembre 2017. Quant aux questions opérationnelles, nous ne donnons aucune information. Lorsqu'un Etat étranger se cache derrière une cyberattaque, une contre-attaque de notre division peut rapidement dégénérer. C'est pourquoi ces opérations sont strictement réglementées. De toute façon, il faudrait d'abord examiner toutes les solutions possibles avant de demander la permission d'entrer dans un système ou un réseau informatique à l'étranger afin

d'y perturber, prévenir ou ralentir l'accès à des informations, comme le prévoit la loi. L'approbation du Conseil fédéral serait nécessaire. Le ministre des Affaires étrangères, qui est responsable des bonnes relations avec l'étranger, devrait également donner son consentement avant que nous puissions commencer.

Avez-vous le droit d'engager des contre-attaques contre des ordinateurs situés en Suisse?

Non. En Suisse, nous pouvons uniquement pénétrer dans des ordinateurs lorsqu'une menace grave et concrète existe et lorsque les investigations des services de renseignement ont jusque-là été infructueuses. Et il nous faut également l'approbation du Tribunal administratif fédéral et du ministre de la Défense. Les contre-mesures ne sont toutefois pas autorisées quand il s'agit de collecter des informations.

L'existence d'attaques ou de menaces est- elle impérative? Ou pouvez-vous pénétrer de votre propre initiative dans des ordinateurs?

Comme je l'ai indiqué, cela est autorisé à l'intérieur du pays uniquement en cas de grave menace. A l'étranger, cette exigence n'est pas obligatoire. Cependant, nous collectons uniquement des informations dans les domaines de l'espionnage, de la prolifération et du terrorisme. Les obstacles sont majeurs: pour une telle opération à l'étranger, la Cour administrative fédérale, les ministres de la Défense et des Affaires étrangères ainsi que la ministre de la Justice doivent donner leur consentement.

Combien d'opérations par an - que ce soit de collectes d'informations ou de contre-attaques - menez-vous environ?

Ces opérations sont rares. Au SRC, nous prévoyons un total de dix à douze cas par an où des mesures de collecte spéciales sont employées. Dans le même temps, nous détectons tous les mois plusieurs cas de cyberattaques informatiques dans les domaines de l'espionnage, de la prolifération et du terrorisme.

Qui est la cible de ces attaques?

On a appris l'attaque contre la société d'armement RUAG, que nous avons découverte en janvier. Mais la Genève internationale, la place bancaire ou encore de plus petites entreprises qui offrent des technologies intéressantes constituent également des cibles.

Aidez-vous des particuliers à se défendre contre une cyberattaque?

Dans le cadre d'un programme de prévention, le SRC est en contact avec diverses entreprises. Il s'agit également de protéger ces entreprises contre les cyberattaques. Lorsque nous détectons des attaques, nous abordons les sociétés. En principe, le SRC est compétent lorsque des autorités publiques de l'étranger sont soupçonnées d'attaquer les intérêts suisses. Il peut ainsi s'agir d'attaques contre des

infrastructures essentielles, d'attaques contre des grandes banques ou des individus s'ils présentent un intérêt particulier pour un Etat étranger.

Comment procédez- vous lorsque vous apprenez une telle attaque?

En règle générale, nous obtenons une première information. Nous l'examinons et nous nous appuyons sur diverses sources. Nous essayons ensuite d'identifier les réseaux informatiques des assaillants. D'où l'attaque a-t-elle été lancée? Où se trouvent les serveurs? Comment l'attaque s'est-elle exactement déroulée? A- t-elle laissé des traces? Nous analysons l'identité de la victime - y a-t-il ici un modèle, une victimologie? Cela peut permettre de tirer des conclusions sur les motivations de l'assaillant et donc sur l'assaillant en lui-même.

Et quand vous avez identifié l'assaillant?

Si ce sont des autorités publiques, le Conseil fédéral doit décider de la façon de réagir. Le spectre s'étend de la diplomatie à la possibilité mentionnée précédemment d'une cyber-contre-attaque.

Pour vos opérations, vous avez également besoin de logiciels malveillants. Où achète-t-on ces chevaux de Troie d'Etat?

Il y a des fournisseurs sur le marché. Nous disposons en outre des ressources nécessaires pour développer nous-mêmes ces logiciels. Cela dépend de la nature de nos besoins dans un cas concret.

Les possibilités accrues offertes par la nouvelle Loi sur le renseignement impliquent aussi un plus grand besoin de personnel. Comment votre division va-t-elle se développer?

Le Conseil fédéral a spécifié dans son message relatif à la nouvelle loi que le SRC créerait au total 15,5 nouveaux emplois. Nous ne détaillons pas davantage ce chiffre dans la mesure où cela permettrait de tirer des conclusions au sujet de la taille de notre division. Je peux toutefois affirmer que, chez nous comme dans d'autres divisions du SRC, des agents de collecte d'informations et des analystes exploitent ces informations. Les analystes techniques dont nous avons besoin dans le domaine informatique, comme par exemple pour l'analyse de logiciels malveillants ennemis, constituent une des particularités de notre service.

Où trouvez-vous vos collaborateurs? Vous avez besoin de génies de l'informatique qui maîtrisent le piratage, mais qui sont aussi tenus au plus grand secret.

Nous annonçons régulièrement les postes à pourvoir. Avant que nous n'embauchions un candidat, celui-ci doit passer le test de sécurité le plus élevé qui existe pour les employés fédéraux. Ce test est effectué par la Division de la protection des informations et des objets (DPIO) du Département de la défense. La vie privée du candidat est également passée au crible, pour voir s'il est, par exemple, vulnérable au chantage. Nous sommes en mesure de choisir parmi un grand nombre de candidatures qualifiées.

Des services secrets étrangers recrutent des collaborateurs lors de championnats de hackers. Le faites-vous également?

Non, nous ne faisons pas cela. L'idée que nous sommes à la recherche du jeune génie de l'informatique au visage blafard qui passe la journée dans sa cave et pirate des ordinateurs est fausse. La cybersécurité est un domaine hautement professionnel avec des spécialistes bien formés et expérimentés. Ce sont des gens qui travaillent par exemple dans la cyberdéfense pour une institution financière ou qui effectuent des recherches dans une université.

Et ces personnes passent tout d'un coup dans le service secret?

Toute personne qui travaille chez nous contribue à la sécurité du pays et se dévoue à la défense contre des dangers réels. C'est un défi que de nombreux spécialistes aiment relever.

En 2012, un collaborateur du SRC a volé une grande quantité de données secrètes qu'il voulait vendre. Il a été démasqué par hasard. Comment éviter de tels incidents?

Nous ne donnons aucune information sur les mesures de sécurité internes - à l'exception du fait que les collaborateurs doivent passer périodiquement le contrôle de sécurité, même après une embauche. Vous pouvez cependant vous assurer que les leçons ont été tirées de cet incident.

Ne craignez-vous pas que l'un de vos collaborateurs ne devienne un jour un Edward Snowden suisse et ne dévoile les rouages internes?

J'ai entièrement confiance en mes collaborateurs.

Vos collaborateurs peuvent-ils dire à leur entourage qu'ils travaillent au Service de renseignement?

Dans le monde extérieur, ils disent généralement qu'ils sont employés par le Département de la défense, ce qui est également vrai. Nos collaborateurs doivent signer un accord stipulant qu'ils restent tenus au secret après avoir quitté le service et qu'ils n'ont pas le droit de transmettre des informations classifiées. Auquel cas ils sont passibles d'une peine. Ils peuvent en outre devenir des cibles pour les services de renseignement étrangers si le nom de l'employeur pour lequel ils ont travaillé est divulgué publiquement.

Vous menez donc la vie classique d'un agent qui ne peut dire à personne ce qu'il fait toute la journée?

Ce serait exagéré, nous ne menons pas une double vie. Ma femme sait, par exemple, où je travaille et ce que je fais. Mais, en règle générale, je discute avec elle d'autres sujets que mon travail. (Rires.)

Le Monde
Le site officiel d'information pour émigrer au Canada ne répond plus (Canada)
Wednesday, 09 November 2016
Byline: Journaliste maison

Ottawa - L'origine précise du plantage n'est pas connue mais pourrait être liée à une surcharge de connexions alors que la victoire de Donald Trump devenait de plus en plus crédible.
Alors que les premiers résultats de l'élection présidentielle américaine donnaient Donald Trump favori face à Hillary Clinton , mercredi 9 novembre, de nombreux internautes ont constaté que le site d'information officiel du gouvernement canadien pour émigrer au Canada n'était plus accessible.

L'origine précise de ce plantage n'est pas connue mais est vraisemblablement liée à une surcharge de connexions. Elle coïncide avec une légère hausse du nombre de recherches sur Google aux Etats-Unis pour l'occurrence «déménager au Canada» , remarquée sur Twitter par un chercheur du MIT, Erik Brynjolfsson.

La tendance avait déjà été constatée par Google au moment des victoires de Donald Trump lors des primaires républicaines, en mars. La blague de «déménager au Canada» en cas de victoire du candidat républicain à la Maison Blanche était ensuite devenue récurrente. Sur le Gawker, un Américain étant parti au Canada après la victoire de George W. Bush en2000 donnait même quelques conseils pour y parvenir .

Le site d'information Quartz y a répondu quelques jours avant l'élection en rappelant que le Canada dirigé par Justin Trudeau n'était pas forcément lehavre de paix idéal que les Américains pouvaient se plaire à imaginer. Le maire de Montréal a néanmoins annoncé, alors que la victoire de Donald Trump devenait de plus en plus crédible, que les bureaux d'intégration des nouveaux arrivants allaient rester exceptionnellement ouverts pour la journée:

Al Jazeera
Opinion: Under surveillance in Russia
Wednesday, 09 November 2016
Byline: Roman Dobrokhotov

Towards the end of September, I received a few emails from Google informing me that someone tried to break into my email. It was not the first time I had received messages like that, so the first thing I did was check the email address from which they were sent.
Users who are not careful might miss the fact that these email addresses only vaguely look like real ones: one email came from no-reply@accounts.google.com.mail.com, and another from: no-reply@accounts.google.com.yandex.com. The links in the emails led to phishing websites made to look like Gmail and if I had put my password there, hackers would have gained control over my email.

In late September and early October, dozens of other Russian journalists, activists and workers in NGOs such as Transparency International received similar phishing emails. This is the biggest wave of hacking attacks on dissidents in Russia so far, but by far not the first one.

I have been encountering such phishing emails since 2014 and it is not a secret who is behind them. Back then in 2014, the hacking group which was behind such attempts was known as Pawn Storm; today after the attacks on the servers of the US State Department, this group has become known as Fancy Bear.

Just in case, I sent the emails to four different organisations dealing with cyber security and they confirmed that they originated from Fancy Bear/Pawn Storm.

This is the group that regularly attacks people and institutions of interest to the Kremlin: from Russian opposition politicians and journalists, to NATO and US political organisations.

Even the support services of Gmail think that there are connections between these hackers and the government. They sent me and other journalists a warning that our emails have been targeted by "state-sponsored attackers".

They are attacking not just email accounts, but also various messengers. For example, the Telegram accounts of two Russian activists - Grigory Alburov and Oleg Kozlovski - were hacked. The perpetrators managed to break in by intercepting the SMS confirmation sent through the mobile operator.

Some internet companies have also actively been cooperating with the Federal Security Service (FSB) and the General Administration for Combating Extremism.

Those companies who do not cooperate with the FSB start facing problems. It was resistance to the FSB demanding access to the social networking site Vkontakte that resulted in its founder, the Russian businessman Pavel Durov, leaving his post as chief executive of his company and departing from Russia for good.

He lost his company, but he did gain quite a reputation. That's why many Russian and other opposition activists and journalists use his encrypted messenger, Telegram, which you can use to avoid getting hacked by choosing the double authentication setting.

We have long got used to the idea that our emails are being read, our phone conversations tapped, and our finances and travels abroad followed. That's why with every passing year, journalists, activists and NGO workers are getting more and more informed about questions of cyber security.

Instead of a regular phone, we use the app Signal; instead of regular SMS, we use Telegram; we buy plane tickets at the last minute; and we always think of which photo we should and should not post on social media.

Members of the political opposition often get stopped at the border; usually they just get interrogated, but sometimes it goes beyond that. For example, in the case of one activist who was going to a conference abroad, a page was ripped from his passport, which invalidated it and he couldn't travel.

I was on a watch list for a while. It would happen that during a regular train ride, I would be approached and taken to a local police station for a "preventative chat". It would be a completely meaningless action whose only purpose was to make me understand: "We are watching you closely."

But these days, state surveillance has been expanding beyond spying on the usual suspects. Most recently, under the guise of a sociological study, a survey was carried out in Russian universities to probe protest activity and readiness. The organiser of the survey admitted that the information on all students who showed opposition attitudes were submitted to the authorities.

The state is not even trying to hide the extensive surveillance over its citizens. State TV and websites regularly release "leaks" discrediting public figures; they are usually obtained through email hacks, phone tapping and hidden cameras, like in the case of the sex tape of the leader of PARNAS Party Mikhail Kasyanov - which was shot without his knowledge.

Sometimes these "leaks" contain genuine information, sometimes they are fabricated and sometimes both. For the first time since Putin came to power, the standard of living in Russia has started to deteriorate due to the drop in oil prices.

The latter happened with opposition leader Alexei Navalny, whose financial documents were published online by hackers. But before posting on the internet, hackers changed some of the information to make it look like he gets money from the Soros Foundation.

Sometimes the purpose of these hacking attacks is not to discredit, but to get inside information. For example, after the phishing attack in 2014, many activists from the "Solidarnost" political movement found out that their email accounts had been set up to forward their correspondence to an unknown email address.

They noticed the hack by chance and it is possible that there are some people who still do not know that their emails are being forwarded to someone else. This is a much faster way to obtain information than setting up surveillance and wire-tapping.

Naturally, the latter methods are still used. Those activists and journalists, who the Kremlin finds particularly unpleasant - like those who cooperate with exiled Russian businessman Mikhail Khodorkovsky - often notice that they are followed in the streets.

The authorities also don't necessarily hide the fact that they follow activists. Perhaps the goal is to scare just them. After all, not everyone is ready to continue work under such pressure.

Of course, the good old snitching methods are also being used, and opposition movements and parties often find informers within their ranks. Some have even found "bugs" in their offices, as was the case with the Navalny's anti-corruption fund.

This type of surveillance tells the opposition figure (or the journalist) that he is a person of interest. Everyone knows what this means. In the best case scenario, you could be thrown in jail; in the worst - you would end up like Boris Nemtsov - shot dead in the streets of Moscow.Unsurprisingly Nemtsov's phone was also tapped and tapes were published in pro-Kremlin publications before his murder.

People don't feel safe - even abroad. Recently, a number of Russian dissidents living abroad have faced the same set-up. Some individuals in their host countries complain to the local authorities about them, accusing them of paedophilia or possessing child pornography and so the local authorities start an investigation. Even if the accusation is not confirmed, the individual is discredited. This is what happened with the dissident Vladimir Bukovsky, who was supposed to give testimony in the Alexander Litvinenko murder case.

All these instruments - following, threatening and campaigns for discrediting - are typical of the Soviet times and, of course, they are well-known to Vladimir Putin as a former KGB agent.

But why is it specifically in the past few years that we see this intense activity of the secret services in controlling public sentiments?

The reasons are several and the main one is economics. For the first time since Putin came to power, the standard of living in Russia has started to deteriorate due to the drop in oil prices. Sanctions are exacerbating the situation.

According to the official statistics, the number of people living under the poverty line has increased over the past year and a half to 23 million people, while the proportion of the population which spends all of their money for food has almost doubled from 22 percent to 41 percent.

Some commentators have objected, saying that not everything is "so bad" since there are no mass protests. Regardless of that, the state over the past few years has done everything to rein in independent media and political movements. It seems all this surveillance and intimidation is working quite well.

Roman Dobrokhotov is a Moscow-based journalist and civil activist. He is the editor-in-chief of The Insider.

Press Trust of India
India trying to fix hacked websites of seven of its embassies

Wednesday, 09 November 2016

New Delhi - Indian officials were trying on Tuesday to restore the websites of seven Indian embassies in Europe and Africa that were hacked and had data dumped online.
The security of the websites of Indian embassies in Italy, Switzerland, South Africa, Libya, Malawi, Mali and Romania was breached by hackers who identified themselves to the media as Kaputsky and Kasimierz L.

"We are aware of the problem and are trying to fix it," External Affairs Ministry spokesman Vikas Swarup told reporters.

Attempts were being made to track the IP addresses of the hackers, who posted online the names, email addresses, phone numbers and passport numbers of some embassy staff members.

Several Indian websites have come under attack this year. Last month, Pakistan-based hackers targeted more than 7,000 Indian websites after India launched a series of attacks on terror camps in Pakistan. Also in October, the security of around 3.2 million debit cards in India was breached when hackers inserted malware through an ATM network.

Fars News Agency
Hackers Can Abuse LTE Protocols to Knock Phones off Networks
Wednesday, 09 November 2016

Tehran - When you travel between countries, the mobile operators that temporarily provide service to your phone need to communicate with your operator back home. This is done over a global interconnection network where most traffic still uses an ageing protocol, called SS7, that's known to be vulnerable to location tracking, eavesdropping, fraud, denial of service (DoS), SMS interception and other attacks.
With the advance of Long-Term Evolution (LTE) networks, some roaming traffic is switching to a newer protocol, called Diameter, that's more secure than SS7 in theory, but which still allows for attacks if it's not deployed with additional security mechanisms.

For example, the Internet Protocol Security (IPsec), a secure communications suite that works by authenticating and encrypting each IP (Internet Protocol) packet, has been standardized for Diameter. But while its implementation is mandatory, its use is optional.

In practice, IPsec is rarely used on the global interconnection network for various reasons and this means that many of the attacks that are possible with SS7 are also possible or have equivalents in Diameter, according to researchers from Nokia Bell Labs and Aalto University in Finland.

The researchers ran experiments on a test network set up by an unnamed global mobile operator and simulated attacks launched from Finland against UK subscribers. They found several methods of disrupting service to users, temporarily and permanently, and even a method that could affect important nodes that provide service to entire regions. The results were presented Friday at the Black Hat Europe security conference in London.

First off, attackers would need to gain access to this private interconnection network (IPX) in order to attack another operator's systems or subscribers. However, this is not hard to achieve, as multiple incidents have shown in the past, and there are different ways to do it.

Attackers could, for example, pose as a virtual network operator and get access to the roaming network through an existing operator. They could also hack into one of the nodes run by existing operators, some of which are, sadly, accessible from the internet, when they shouldn't be.

If the attacker is actually a government, it could leverage its power over local operators to gain access through them. And if that doesn't work, bribing an employee from an operator is also an option.

Finally, access could be bought from other hackers that already have it. There have been services on the "dark" market that sold access to this network and there will probably be more in the future.

An operator's LTE network is made up of cell towers; nodes called MMEs (Mobility Management Entities) that provide session management, subscriber authentication, roaming and handovers to other networks; and a home subscriber server (HSS), the crown jewel that holds the master subscriber database. At the edge it has Diameter Edge Agents (DEAs), which serve as links to the interconnection network via IPX providers.

In order to pull off any attack on telecom networks, attackers need to know the victim's international mobile subscriber identity (IMSI), a unique number that's stored in the subscriber's SIM card. The researchers showed that attackers can easily obtain this number once they're on the IPX network by masquerading as a Short Message service center (SMSC) that's trying to deliver a text message to a phone number.

The attackers only need to know the victim's phone number in international format -- this is known as the Mobile Station International Subscriber Directory Number (MSISDN) -- and the DEA of the victim's operator. They can then send a routing information request through the DEA to the operator's HSS, which will respond with the subscriber's IMSI as well as the identity of the MME the subscriber is connected to. This provides the information needed to launch future attacks.

Such an attack involves the attackers masquerading as a partner's HSS and sending a Cancel Location Request (CLR) message to the victim's MME. This will cause the MME to disconnect the subscriber.

CLR messages are used on a regular basis inside the network when subscribers switch from one MME to another because of a change in location. However, the interesting aspect of this attack, aside from forcing an MME to detach a subscriber from the network, is that when the subscriber re-attaches, their device will send 20 different messages to the MME.

This amplification effect might pose risks to the MME if, for example, attackers force the detachment of hundreds of subscribers at the same time, although the researchers didn't test how many messages it would take to overload an MME. If an MME becomes unresponsive it would be bad, because there are only a few of them in a network and they serve large areas.

A second DoS technique devised by the researchers involves impersonating an HSS and sending an Insert Subscriber Data Request (IDR) to the victim's MME with a special value that means no service. This will permanently detach the user from the network because their subscription will be changed in the MME's records. Recovering from this can take a long time because the subscriber needs to call his mobile operator and sort out the situation.

The researchers also showed two other DoS techniques involving other types of Diameter messages, but they're only temporary as the user can recover by restarting their mobile device.

People seem to think that all will be better with LTE and Diameter, but in reality it will be different, not better, if mobile operators don't take additional security measures, said Silke Holtmanns, a security specialist with Nokia Bell Labs, during her talk at Black Hat Europe.

According to her, deploying IPsec is hard because not all traffic on the IPX network uses the Internet Protocol, and maintaining the kind of large public key infrastructures required by IPsec is costly for operators in developing countries. Nodes are also difficult to upgrade, and then there's the tough question of who should be in charge of creating and hosting the root certificates required by IPsec, which is likely to cause disputes between countries, she said.

And even if IPsec somehow becomes widely used, it still doesn't protect against attacks launched with the help of hacked nodes, rented network access, bribed employees or governmental ties, because these methods abuse legitimate access to the network.

According to the researchers, the best defense is a combination of measures. Operators should monitor the traffic on their networks and the traffic of their tenants and they should filter messages at their DEAs by using signaling firewalls. They should also harden their nodes, share their security experiences with other operators and put business rules in place so they can efficiently deal with misuse.

Asharq Al-Awsat
Saudi Arabia Launches Program to Limit Internet Usage, Enhance Information Security Level
Wednesday, 09 November 2016

Byline: Fahd Baqmi

Jeddah - The Ministry of Communications and Information Technology has announced a project to limit the internet consumption in the country and to enhance the level of information security. The ministry also announced operating a new extension for internet.
Experts in the Information Technology told Asharq al-Awsat that this step aims at raising awareness towards the dangers of information security, coordinating efforts in the field of cyber security and increasing confidence in cyber dealings.

Security Advisor Professor Yusuf al-Rumaih said that this procedure is to protect the social and economic system of the country from insecure hacking especially amidst the internet criminal organizations exploitation to reach for individuals in target such as teenagers and the youths.

The number of spam messages sent daily on the social network websites is estimated as more than 100,000. They basically encourage chaos and jihad. Security Consultant and Researcher Professor Ali al-Khashaiban said that focusing on information security is one of the basic steps that protect the society from any violations on the security and mental levels.

According to official warnings, the offenses against governmental bodies and huge companies seek coding websites through spreading malice viruses--this fact pushed parties to send warning letters for devices users to avoid falling for these attempts.

The spying program includes sending messages via the social network websites--however if users examined the messages carefully then they can deleted them and avoid the damage.

London Daily Telegraph
GCHQ to investigate Tesco bank hack
Wednesday, 09 November 2016
Byline: Ben Martin

London - TESCO has enlisted the help of GCHQ, the spy agency, to assist its investigation of what is the most serious cyber attack launched against a British bank.
The supermarket chain contacted the National Cyber Security Centre (NCSC), a new part of GCHQ that tackles crime online, after it learned of the theft at the weekend at Tesco Bank, in which money was taken from about 20,000 current accounts.

The NCSC has been providing "on- site assistance" to the company. It is working alongside the National Crime Agency to investigate the attack. Tesco Bank confirmed on Monday that it had detected "online criminal activity" in 40,000 current accounts and that money was taken from half of them.

Chris Philp, an MP on the Commons Treasury select committee, has suggested the theft could have been "state- sponsored".

Andrew Bailey, the chief executive of City watchdog the Financial Conduct Authority, told the committee yesterday that the attack against the lender "looks unprecedented in the UK".

The bank said last night that normal service had resumed after the suspension of online transactions from the affected accounts and that personal data had not been compromised.

Agence France-Presse
Terrorisme: Interpol dénonce le manque de partages de données biométriques entre Etats
Wednesday, 09 November 2016
Byline: Journaliste maison

Lyon - Le secrétaire général d'Interpol Jürgen Stock a dénoncé mercredi l'insuffisant partage entre Etats de données biométriques susceptibles de permettre d'identifier plus efficacement les terroristes. L'organisation de coopération policière estime qu'"environ 15.000 combattants se trouvent dans les zones de conflit et qu'un nombre indéterminé d'entre eux pourrait rentrer dans leur pays d'origine pour (...) s'engager dans des opérations clandestines".

L'assemblée générale d'Interpol, qui était réunie à Bali (Indonésie), a souligné "l'urgence à traiter cette menace", écrit-elle dans un communiqué.

"Bien que le partage d'information via Interpol ait permis aux organisations nationales de maintien de l'ordre d'empêcher des terroristes et des candidats terroristes de voyager, le manque de données biométriques reste un maillon faible", déclare M. Stock, cité dans un communiqué de l'organisation.

"Ne pas fournir aux agents en première ligne les informations dont ils ont absolument besoin pour identifier les terroristes de retour de zones de conflit, c'est leur bander les yeux, les obliger à faire leur travail avec une main attachée derrière leur dos", estime-t-il.

Le patron d'Interpol souligne que les informations biométriques destinées à l'identification, telles que les empreintes digitales et l'ADN, sont "cruciales" dans le contexte actuel.

"Bien qu'Interpol dispose actuellement d'informations sur près de 9.000 combattants terroristes étrangers - dont certains présents dans les zones de combat - moins de dix pour cent de ces fichiers comprennent des données biométriques ou des images en haute résolution qui pourraient être utilisées pour une reconnaissance faciale", ajoute l'organisation.

Interpol cite notamment l'exemple d'une opération menée par une de ses structures dédiées dans une prison malienne, qui a permis d'identifier un prisonnier sous un faux nom alors qu'il était recherché par

l'Algérie pour une attaque terroriste. Les empreintes digitales d'un second prisonnier ont également permis d'identifier celui-ci comme étant l'un des auteurs de l'attaque de Grand-Bassam en Côte-d'Ivoire en mars 2016.

Jakarta Post
Second day of Interpol conference addresses war against terrorism, cyber crime
Wednesday, 09 November 2016
Byline: News Desk

Jakarta - Country delegations and experts have highlighted the importance of a stronger international partnership to combat terrorism and cyber crime on the second day of the 85th Interpol General Assembly in Nusa Dua, Bali.
National Police spokesperson Sr. Comr. Martinus Sitompul said that in Tuesday's sessions, the delegations discussed efforts to fight against terrorism and cyber crime.

"We discussed Interpol strategies to combat terrorists and cyber crime perpetrators," he said as quoted by kompas.com at the Bali Nusa Dua Convention Center.

Martinus said several other topics related to global threats were also discussed, including organized crime, such as drug smuggling and money laundering, and other transnational problems. The 2016-2020 Interpol presidential election plan was also discussed in the meeting.

As reported earlier, Interpol president Mireille Ballestrazzi will end her term of office this year. The election of the new Interpol president is scheduled on the last day of the conference on Thursday.

Martinus further said that on Tuesday, all delegations had begun to compile a road map toward 2020. "Interpol will also compile a 2017-2020 action plan for the new leadership," he said.

On the first day of the conference, the delegations discussed basic principles of an Interpol partnership. They agreed that there was a need in each country to gather information.

"So there has been an awareness to share information. Geometric data becomes a guideline in identifying potential threats," said Martinus.

More than 1,300 participants from 162 countries are attending the four-day conference on terrorism and transnational crime, which will end on Thursday.

Newsweek
What a Trump Presidency Means for Cybersecurity, Net Neutrality and Internet Freedom
Thursday, 10 November 2016
Byline: Anthony Cuthbertson

New York - When billionaire entrepreneur Peter Thiel bucked the trend of Silicon Valley by throwing his cash and support behind Donald Trump, Mark Zuckerberg had some explaining to do.
As one of Facebook's board members, Thiel's move sparked criticism among the ultra liberal tech community of California. "There are many reasons a person might support Trump that do not involve racism, sexism, xenophobia or accepting sexual assault," Zuckerberg, who launched Facebook in 2004, wrote in an internal company memo.

While Trump's views on building walls and lack of belief in climate change are well documented, the president elect's stance on the issues that will directly affect technology firms, and by extension, much of the world are less obvious.

Trump has promised to immediately make cybersecurity a top priority, citing concerns about cyberattacks from the likes of China and North Korea. His written policies on cybersecurity are summed up in four bullet points that lack any concrete detail, but include the promise to develop cyber weapons.

It states: "Develop the offensive cyber capabilities we need to deter attacks by both state and non-state actors and, if necessary, to respond appropriately."

According to Uri Rivner, head of cyber strategy at biometrics firm BioCatch, Trump will take such threats seriously and combating them will be high on the future administration's agenda.

"Cyber threats to both critical infrastructure and financial systems are just the sort of clear and present danger that requires decisive action--the likes of which the president elect has been advocating," Rivner tells Newsweek . "This in turn may lead to more aggressive cyber security policies, faster response to cyber attack campaigns, and greater investment in cyber security defenses."

It remains unclear how clued up Trump is on the actual issues and specific threats facing his administration. On the occasion that he has vocalized his thoughts on cybersecurity, there is little to suggest a clear or informed perspective.

This is what Trump had to say at the first debate with Democratic nominee Hillary Clinton: "I have a son. He's 10 years old. He has computers, it's unbelievable. The security aspect of cyber is very, very tough. And maybe it's hardly doable."Barron Trump to head his father's administration on cybersecurity, anyone?

Net Neutrality and Internet Freedom

Trump's anti-regulation stance may well have an effect on internet service providers and the Federal Communications Commission's rules on net neutrality--the principle that Internet Service Providers should treat all internet traffic equally..

In 2014, Trump described the rules as an "attack on the internet" by President Obama, suggesting he may roll back the rules once in office.

Trump has also said that in the event of a cyber war, he would close parts of the internet. "When you look at what ISIS is doing with the internet, they're beating us at our own game," Trump said during the first debate."I would certainly be open to closing areas where we are at war with somebody. I sure as hell don't want to let people who want to kill us and kill our nation use our internet."

Australian Associated Press
Govt appoints new cyber affairs ambassador
Thursday, 10 November 2016
Byline: Staff reporter

Canberra - Australia has appointed its first-ever ambassador for cyber affairs.
Dr Tobias Feakin will fill the inaugural position from January as part of the federal government's $230 million cyber security strategy.

The academic, who has been the director of national security programs at the Australian Strategic Policy Institute since 2012, will work with other countries to strengthen the region's response to cybercrime and advocate against state censorship of the internet.

Scoop.co.nz
New Zealand needs a cultural shift to keep data safe
Thursday, 10 November 2016
Byline: Staff reporter

Wellington - New Zealanders need to better understand the risks of prioritising user features over security when it comes to the many internet- connected devices we use, says a Massey University cybersecurity expert.
Dr Andrew Colarik, a senior lecturer with the Centre for Defence and Security Studies, discussed the many ways in which our personal, company and national security information can be extracted and used against us at the Massey University Future NZ Forum on Cyberscurity, held this morning.

Dr Colarik warned that New Zealand hasn't invested heavily enough in infrastructure to make the country resilient against denial-of-service attacks, or to keep data safe. The problem, he says, is the

infrastructure we have built is scaled for New Zealand's population, but that same infrastructure connects us to the rest of the world.

"Everything we do in this country is now so dependent on the free flow of information and the connections that we maintain. Any disruption to that will have huge, cascading effects," he says.

"A large denial-of-service attack could shut down communications to the whole country quite easily. If targeted for competitive or political reasons, there are very few organisations that would be resilient to that sort of attack."

He says both individuals and organisations need to understand that communications infrastucture, by its nature, is not secure.

"There are only measures of security," he says. "The notion that the internet is secure is just salesmanship."

He asked how many of us really think about the access we give to our information when we download an app or a game like Pokemon Go!

"Pokemon Go! has the right to take all your pictures, all your contacts, basically everything on your phone and send it to the mother company. The company that owns it, their net worth increased by billions - how is that possible if the data isn't worth something?"

In this digital landscape, New Zealand's economic livelihood faces real threats, Dr Colarik says. New competitors are emerging all the time - and some will have the know-how and motivation to extract information for competitive advantage.

"What happens when an organisation's own information is used against it? Customer details, costing and pricing structures, and other intellectual properties are all there for the taking if not properly protected."

But he says this is not just a national security problem for the government to deal with.

"Sure, more investment in infrastructure is helpful, but what we really need is a cultural shift to strike the right balance between user features and security, and data useage and privacy. You can't have your cake and eat it too.

"This needs to be done at a whole-of- society level. We all need to take responsibility for the level to which we share our personal data, and we need more education and greater discussion about who owns and controls our information. A genuine public/private partnership is essential for ensuring everyone's prosperity in our digital future."

After his speech Dr Colarik was joined by a panel of industry experts to discuss the strategic cybersecurity issues facing New Zealand.

Panelists Ken Wallace, practice leader, technology risk and assurance at Ernst & Young; Kendra Ross, director and co-founder of Duo; and Steve Walsham, executive broker at Crombie Lockwood shared insights on how to make organisations more resilient to cyber attacks and how to get senior management buy-in for security expenditure.

They also acknowledged there was a lack of capability in New Zealand for dealing with cybersecurity issues, but identified it as an opportunity for the future.

"There is a global skills shortage - 1.5 million cybersecurity roles currently unfilled globally," Ms Ross said. "We have an ability here to actually build a workforce that we could be exporting in terms of skills and resource capability."

The Register (UK)
Trump's torture support could mean the end of GCHQ-NSA relationship
Wednesday, 09 November 2016
Byline: Alexander J. Martin

Column - If comments made on the campaign trail by Donald Trump were sincere, then today's British government will need to do some serious soul- searching very soon.
Trump, who was today announced as the president-elect of the United States of America, has been controversially outspoken while seeking to be nominated as the Republican Party's presidential candidate, and while campaigning to be elected as President.

Many of his outbursts had been criticized for their deemed sincerity - and vulgarity - but it is particularly his defense of torture (despite his nation's ratification of the United Nations Convention Against Torture, and the constitutional prohibition against cruel and unusual punishment) that could provoke problems between the UK and US.

The constitution may ostensibly be amended, and a UN convention might be derogated from, but a US decision to legalize torture would very probably prohibit the greater part of the intelligence- sharing aspects of the UK and US's special relationship - a relationship that already is substantively about the collaboration between GCHQ and the NSA (US National Security Agency).

The future of the "special relationship" is very much dependent on how Trump will exercise the US intelligence apparatus, and if he seeks to assert the position he had previously issued on torture he is very likely to receive push-back from the UK due to the nation's legal obligations, which are much more unlikely to be derogated from.

Back in February, Trump told a rally audience that "torture works." He said:

OK, folks? You know, I have these guys -- 'Torture doesn't work!' -- believe me, it works. And waterboarding is your minor form. Some people say it's not actually torture. Let's assume it is. But they asked me the question: What do you think of waterboarding? Absolutely fine. But we should go much stronger than waterboarding. That's the way I feel. They're chopping off heads. Believe me, we should go much stronger, because our country's in trouble. We're in danger. We have people that want to do really bad things!

UK-based infosec expert and ex-GCHQ specialist Matt Tait, aka Pwn All The Things on Twitter, told El Reg:

"Trump's position on torture is a really big deal. Torture of detainees is directly and unambiguously a violation of the internationally accepted laws of armed conflict - even if used against unlawful enemy belligerents, such as terrorists rather than captured prisoners of war. Trump's comments on torture are important and a unique deviation for US policy. Previous administrations, even when they have engaged in "enhanced interrogation techniques" such as under George W Bush - and even when these EITs escalate to the point that they are widely called "torture" - the US has gone to lengths to assert that the EITs it did use didn't amount to "torture"; declassified legal memos show lawyers within the Bush administration trying to define the line where interrogation becomes torture and push EITs right up to, but not over, that line.

"Whether you think the Bush administration was successful or whether it overstepped that line, they did at least know there was a line, and tried not to overstep it. No so with Trump. Trump actively embraces the idea of torturing detainees. He not only says that torture is ok; he says it's something the US should actively engage in. And not just to get information. To "punish" them as well.

"Even laying aside the enormous domestic law and eighth amendment issues this brings up, this will make it impossible for UK intelligence cooperation with the Trump administration across a range of intelligence programs. The UK will have to restrict the uses, categories and programs of intelligence sharing with the US if there is any risk the US could use that intelligence to intentionally engage in war crimes.

"This differs to Trump's position on cybersecurity. Although his positions are less clear on this topic, it seems that his position largely boils down to a much more substantial active response to cyberattacks on the US. So long as the response isn't clearly disproportionate, or targeting civilians, this doesn't look especially challenging to international partners; it's certainly not an intentional war crime. On topics such as this, the UK may end up disagreeing with the Trump administration on policy, but ultimately the UK won't be in the same position as with torture where the UK would have to take a firm line of non-cooperation to avoid being complicit in a war crime itself."

Jim Killock, executive director of the Open Rights Group (ORG), warned The Register: "If the US openly pursues a policy of torturing those suspected of terrorism, it cannot legally be enabled by the sharing of intelligence from the UK."

"However, given the close integration of the UK and US intelligence agencies, it will be difficult to separate our data sharing and technologies," Killock continued. "This presents a huge challenge for oversight, who need to be aware of the possibility that GCHQ might be urged to help with policies that are indefensible."

ORG additionally warned that Trump will exert a great deal of control over GCHQ's operations as President, and stressed the integration between the UK and US signals intelligence organizations. Such integration was today restated by the UK's Prime Minister, Theresa May, who congratulated Trump and applauded how "Britain and the United States have an enduring and special relationship based on the values of freedom, democracy and enterprise."

"We are, and will remain, strong and close partners on trade, security and defense," stated May. "I look forward to working with President-elect Donald Trump, building on these ties to ensure the security and prosperity of our nations in the years ahead." ®

Deutsche Welle
German cabinet approves cyber security strategy
Wednesday, 09 November 2016

Berlin - The German cabinet on Wednesday adopted a new cyber security strategy to counter a rising number of threats targeting government institutions, critical infrastructure, businesses and citizens. The strategy calls for the creation of a mobile Quick Reaction Force housed within the Federal Office for Information Security (BSI), as well as similar teams within the federal police and domestic intelligence agency that are able to respond to cyber threats against government institutions and critical infrastructure.

Germany's Cyber Defense Center will fall under the authority of the Interior Ministry, which will seek to foster inter- agency coordination and cooperation.

The new strategy also calls for greater cooperation and information sharing between the public and private sectors on cyber threats, a policy that is in line with United States' cyber defense strategy. The government wants to build up awareness and support for businesses and expects them to take active measures to protect against cyber threats. Of particular focus is protecting critical infrastructure, including energy and water supplies, healthcare systems, digital routing systems and transportation.

In addition, federal administrations should maintain better IT security management systems that are up-to-date to respond to evolving cyber threats. Another part of the strategy promotes raising awareness

among the population, including advocating for the use of encryption and security labels for IT products. The plan also calls for more IT training and development in schools.

According to a BSI report released Wednesday, there are a growing number of sophisticated malware targeting IT systems in Germany for which existing anti-virus programs are inadequate. Many of the cyber attacks are so-called ransomware that block computers or steal data in order to extort ransom payments, BSI said.

Interior Minister Thomas de Maziere said that an increasing number of cyber attacks originate from outside Germany's borders, mainly directed from China and Russia. Echoing comments made by Chancellor Angela Merkel on Tuesday, he warned of possible cyber attacks and disinformation campaigns directed from Russia to influence public opinion ahead next year's national elections.

He also cautioned against the use of "bots" that manipulate social media to influence opinion. He called on all political parties to commit not to use such tactics in the upcoming election after the eurosceptic Alternative for Germany (AfD) suggested the party may use the technology.

Forbes
Scared About Trump Wielding FBI And NSA Cyber Power? You Should Be
Wednesday, 09 November 2016
Byline: Thomas Fox-Brewster

New York - Americans are understandably anxious about the idea of Donald Trump wantonly wielding "The Cyber" to quiet his enemies, following his election to president today.
But whatever the future for non-white citizens, women, the climate and the free press in Trump's America, the surveillance state of the U.S. will not immediately expand as a result of his ascent to power, at least from the perspective of the most powerful of the 17 intelligence agencies. That's according to former National Security Agency staffers, including former deputy director Chris Inglis, who told FORBES prior to the election the NSA wouldn't cave to excessive demands of any president: it's first duty, he said, was to uphold the Constitution, not obey crazy demands. "Given an unlawful order... it must say 'no.'"

Dave Aitel, a former NSA computer scientist, said it was unlikely the NSA would see any change in the near future. "There's no reason to panic yet... It's much less a concern with the NSA than the Department of Justice," he said, pointing to Trump's vocal support on the feds' attempts to force tech companies like Apple into breaking their own security measures to get data on suspects.

Indeed, Trump's relationship with the FBI will be of particular concern given James Comey's much-criticized move to re-ignite the Clinton email scandal a week before the election, subsequently dropping any threat of another investigation two days ahead of the vote. The FBI will, it seems, be happy with a

president who is so keen to shine a light on the "going dark" issue and encryption. Hillary Clinton's plan, Aitel noted, was to do nothing.

Susan Hennessey, former counsel for the NSA, told FORBES she also believed a more immediate concern was how Trump might use the DoJ. The NSA, claimed Hennessey, had more safeguards in place than the FBI when it came to spying on individuals.

"The DoJ can investigate pretty much anyone they want to," she told me, pointing to the threat of vindictive prosecutions and unjustified searches of people's property. "I think... tremendous damage could be done with the DoJ.

"There's a more immediate possibility for abuse at the DoJ and the FBI than at the NSA... We should not kid ourselves about the power and trust we vest in our president."

Fear and hope over The Cyber

But, said Aitel, some of the executive orders designed to rein in the NSA in the wake of the Edward Snowden leaks could be scrapped come January 1. That's something that has concerned Jay Healey, senior research scholar at Columbia University's School for International and Public Affairs specializing in cyber conflict. Healey said whilst there are checks and balances, in two years, it'd be easy for Trump to start changing laws to bend the NSA to his will. "With a friendly Congress, after two years, the laws could easily be changed to give much more scope," he said. Trump could, for instance, rescind some of the restrictions put on the Patriot Act or limitations on the NSA's bulk telephone surveillance.

Hennessey said that if Trump were to start rolling back Obama's changes, the easiest target would be the executive order Presidential Policy Directive 28, which sought to offer more protection for foreign citizens from the NSA's mass surveillance. "Because it is newer, it is easier to undo." The Obama regime was last month accused by the Electronic Frontier Foundation on failing to deliver on PPD-28 anyway.

Whatever is coming, the intelligence agency could well be tested by the Trump regime, she presaged. "The NSA has some tremendously strong institutional protection, more importantly it is staffed by law abiding, honourable people. Those institutions and those people may be about to be tested in ways that they have never been tested before," said Hennessey, who now works at the Brookings Institution. "While I hope and I pray they will pass that test, I don't think anybody knows what is going to happen."

Aitel had a more positive outlook than most, noting it was a good time to make decisions in cybersecurity that Obama's regime has failed to deliver. Trump could come good on his promise to invigorate the U.S. Cyber Command, better known as CyberCom, an offensive cyber department currently located within the NSA. Trump could spur on CyberCom's separation from the NSA and its march towards full capability, which has been criticized for its sluggishness, Aitel suggested.

He added: "We have an opportunity to make major steps. A lot of people are afraid of what those steps could be. Both candidates ran policy-free campaigns and it's time for governance to happen."

It will likely take a major disaster for Trump to start flexing what he calls "The Cyber," said security expert Robert Graham. "NSA will be fine -- until there's something like another 9/11. Trump's populism will then have little restraint to reshape it into a massively police state," Graham told me.

Snowden himself has chimed in with a similar argument, posting a video from the year he leaked the NSA files. In it, he warned about a "turnkey tyranny," where a new leader could "flip a switch" to allow itself huge surveillance power. The populace, he added, would be helpless to stop it.

Christian Science Monitor
What Trump's victory means for cybersecurity
Wednesday, 09 November 2016
Byline: Sara Sorcher

Column- Other than a few technological glitches, voting systems Tuesday appeared to run smoothly. Election Day concerns that malicious hackers might tamper with voting, after a presidential season marked by digital attacks, didn't materialize. But that wasn't the biggest surprise of the night. That honor went to President-elect Donald Trump, whose win stunned pollsters and pundits alike.
So, what does Mr. Trump's victory mean for cybersecurity? There are already some indications.

"To truly make America safe, we truly have to make cybersecurity a major priority," Trump told a Virginia crowd in October, adding that cyberattacks from other countries including "China, Russia, and North Korea constitute one of our most critical national security concerns."

His cybersecurity plan promises an "immediate review" of the country's "cyberdefenses and vulnerabilities" including within US critical infrastructure, which includes the energy and banking sectors. He pledged to create task forces to respond to digital threats throughout the country - and get recommendations on how to enhance the military's Cyber Command with "with a focus on both offense and defense."

Still, Trump may need to brush up cybersecurity issues when he's in office. His response to a question on cybersecurity at a September debate - in which he invoked his 10-year-old son's prowess with computers and inadvertently started an internet meme by calling digital threats "the cyber" - was widely dismissed by the tech press as " incoherent" and " utterly disconnected."

There are also important questions about how a future President Trump will engage with those on the front lines of intelligence gathering in cyberspace.

During his campaign, he refused to blame Russia for hacking US political organizations. That position contradicted US intelligence officials, prominent cybersecurity researchers who investigated the hacks, and even his own senior military adviser retired Army lieutenant general Michael Flynn, who all said there was enough evidence to blame Moscow.

Instead, Trump offered up his own idea that China or " someone sitting on their bed that weighs 400 pounds" may have been responsible.

There are also lingering questions about what Trump's election means for the US quest to forge international norms for cyberspace in the Digital Age. Trump drew outrage from critics when he went so far as to encourage Russia - if its intelligence services had indeed hacked his opponent Hillary Clinton's email server - to publish the data it might have stolen.

"Russia, if you're listening," he said, "I hope you're able to find the 30,000 emails that are missing. I think you will probably be rewarded mightily by our press." The New York Times reported at the time that this call was "essentially urging a foreign adversary to conduct cyberespionage against a former secretary of state."

Now that Trump will soon hold the Oval Office, Politico's Tim Starks noted there could be consequences for remarks made in the frenzy of a heated campaign: "Trump's election may herald an era of Russian free rein ... the prospect that Russia will face no US punishment for its behavior, something experts fear will embolden President Vladimir Putin and his regime to keep mounting cyberattacks around the globe."

Trump's election may also renew the encryption fight that went unresolved during the Obama administration. Trump went so far as to call for a boycott of Apple for its stance on encryption as it pledged to fight a court's ruling to help the FBI unlock the iPhone used by the shooter in the San Bernardino terror attack.

In the remaining months of Obama's presidency, digital rights advocacy groups are making a final play for the current commander-in-chief to rein in the government's spying powers - a rallying point since former National Security Agency contractor-turned-whistleblower Edward Snowden exposed sweeping surveillance programs in 2013.

Yet, as noted privacy advocate and author Cory Doctorow wrote Wednesday on the tech blog Boing Boing, "The seven years of GW Bush- after-9/11 gave us the foundations for a surveillance state that was one madman away from totalitarianism. Then, eight years of Obama operationalized that surveillance state, gave it the competent administrators and diverse stakeholders - local police, international partners, military-industrial contractors with fat lobbying budgets - that it needs to sustain itself indefinitely."

Now, he adds, Trump will inherit control "over a surveillance arsenal that includes the legal authority to spy on all of us, all the time ... and a hoard of deadly technological vulnerabilities in tools we all rely upon that America has weaponized to attack its enemies, even if that means leaving Americans undefended against criminals, nihilist griefers, and foreign state and industrial spies." (Mr. Doctorow views him as unfit for the responsibility.)

Business Insider (US)
People in tech are freaking out about Donald Trump being given control of the NSA
Wednesday, 09 November 2016
Byline: Sam Shead

New York - Last month, Wired published a story with the headline "Imagine if Donald Trump controlled the NSA." Now there's no need to imagine.
Trump overcame all odds on Wednesday when he became the 45th president-elect of the United States. As a result, he's about to gain control of the US intelligence agencies, including the NSA (National Security Agency).

Tech workers and security campaigners have been quick to express concerns about handing control of the NSA to Trump.

The intelligence agency serves as a US spy centre that monitors, collects, and processes information on people across the world. It has made headlines over the last few years for its secretive mass surveillance methods, which overstep the mark in the eyes of many people.

Security consultant Dan Tentler wrote on Twitter: "Trump will control the NSA. Think about that for a second. What the f*** did you people do?"

Former CIA analyst Patrick Eddington questioned what the NSA will do under Trump given that it warranted mass surveillance under former president George Bush.

Frederike Kaltheuner, who works in policy at campaign group Privacy International, wrote on Twitter: "The NSA will now be run by a Trump government. This is why we should never give a carte blanche to powerful institutions."

Chris Schofield, an academic at Royal Holloway university focusing on geopolitics, highlighted on Twitter that Trump will also have control of the CIA, FBI, aircraft carriers, Navy SEALS, nuclear weapons, US diplomats, and the Senate.

Trump has promised national-security overhauls, including a potential return to enhanced-interrogation techniques, increasing bombing of ISIS, reevaluating the US relationship with Russian President Vladimir

Putin, loosening background checks for purchasing firearms, and forcing Mexico to pay for a Southern border wall.

Motherboard (VICE)
Could President Trump Really Turn the NSA Into a Personal Spy Machine?
Wednesday, 09 November 2016
Byline: Staff report

New York - It's the nightmare scenario that many worried about: the US elects a president who uses the country's nearly omnipotent surveillance powers for his or her own gain. Edward Snowden has described the NSA's spying capabilities as the "architecture of oppression," with the fear being that it could be deployed by a malicious commander in chief.
But what could President Trump, a man who has incited hate speech against minorities and threatened to jail his political rivals, actually do with the NSA? Could he turn the NSA into his own personal spying army?

"No. By and large it's not going to happen, if for no other reason than there's too many institutional safeguards that are setup," Bradley P. Moss, a national security attorney who represents intelligence community employees, told Motherboard in a phone call. If Trump did try to use the NSA for his own personal or financial gain, there would be a mass of resignations and whistleblowers coming forward, Moss said.

Trump would not be able to authorize surveillance on, say, Hillary Clinton by himself, Moss said: at minimum, the order would have to go through a court (whether that particular court is essentially a rubber stamp is another issue, though). And on top of the legality of such an operation, there are the layers of lawyers and other institutions that handle such things.

"There's the internal bureaucracy that's designed to try to limit some of the more egregious or crazy ideas that might come from a political appointee," Moss said. "You couldn't just willy-nilly start spying on any particular American citizen you wanted," he added. Foreign targets don't have the same sort of protections, however.

So the personal army theory is arguably off the table. But of course the president still has exceptional power to shake-up the agency, put different people in charge of it, and adjust some of the legalities around its work.

"Could there be aspects to which President Trump could expand or play around in the legal grey areas, more than say President Obama had, or President Clinton would have? Sure, that's absolutely possible," Moss said.

Executive orders in particular, which do not require Congressional approval to take effect, are fair game, and have played a vital role in surveillance legislation.

"A lot of the things that impose civil liberties restraints on the NSA are presidential directives, so he could easily reside those," Dave Aitel, a former NSA security researcher and now founder of cybersecurity company Immunity, told Motherboard in a phone call.

"The entire cyber policy of the United States may change. He's been much more progressively offensive," he added.

But if Trump was to make changes, he likely wouldn't be able to without setting off alarm bells, though.

"I have no doubt he could not make the kinds of broad structural changes, for example through executive order, without Congress and the courts, as well as large segments of the executive branch being aware," Susan Hennessey, a fellow in national security at the Brookings Institution think tank and former National Security Agency attorney, told Motherboard in a phone call.

Even with those caveats, there are of course still substantial concerns with Trump's relationship with the NSA, and his position on surveillance and the intelligence community more generally.

For Moss, it's Trump's penchant for secrecy that may threaten a lot of the reforms that have been accomplished in the past decade, especially with legal whistleblowers. Although there won't necessarily won't be legislative changes, policies may be curtailed internally: If people see raising concerns has a sure-fire way to be punished, then "those people are going to back off, and are not going to risk it," Moss said.

"My specific concern is ensuring that our intelligence priorities continue to reflect the priorities of the nation, and that we continue to have vital, productive relationships with our allies," Hennessey added.

Le Monde
Autour du méga-fichier TES, une série d'inquiétudes
Thursday, 10 November 2016
Byline: Martin Untersinger

Paris - M. Cazeneuve est auditionné, mercredi, par la commission des lois sur la base de données biométriques
Le ministre de l'intérieur Bernard Cazeneuve va répondre, mercredi 9 novembre, aux questions des députés de la commission des lois à propos de la base de données des titres électroniques sécurisés (TES). Ce fichier, créé par décret le week-end de la Toussaint, va permettre d'intégrer les données des demandeurs de carte d'identité dans le fichier des passeports - qui existe déjà - et d'y stocker une

longue liste de données personnelles, dont les empreintes digitales, de tous les titulaires de ces titres d'identité. Soit, à terme, la quasi-totalité de la population française.

Plusieurs associations se sont alarmées de l'existence d'un fichier d'une taille inédite depuis la deuxième guerre mondiale, et le Conseil national du numérique a appelé lundi 7 novembre le gouvernement à le suspendre.

Piratage Une des principales inquiétudes exprimées, c'est la -vulnérabilité à un piratage d'une base de données contenant autant d'informations personnelles. " On sait de longue date en sécurité informatique que la centralisation représente une source de risque, car elle désigne à un -attaquant une cible très tentante, et toute attaque peut avoir des -impacts majeurs " , explique Claude Castelluccia, chercheur à l'In-stitut national de recherche en informatique et en automatique (Inria).

Le Conseil national du numérique s'est aussi alarmé des risques de piratage du fichier, " à un moment où les cybermenaces se font redoutables " . " En matière de sécurité informatique, aucun système n'est imprenable. Les défenses érigées comme des lignes Maginot finissent immanquablement par être brisées ", estime cet organisme d'experts dans les questions numériques.

Les précédents existent. Récemment, la base de données de l'administration américaine contenant les données personnelles, dont des empreintes digitales, de 21,5 millions de fonctionnaires a été piratée. En Israël, où un projet pilote de base de données biométriques centralisées est expérimenté depuis quelques années, les dirigeants du Mossad (service de renseignement extérieur) et du Shin Bet (service de contre-espionnage) ont interdit à leurs agents de fournir leurs empreintes digitales, craignant une fuite de données.

Les risques sont importants, car les données biométriques ne sont pas des données comme les autres, comme l'a rappelé la Commission nationale de l'informatique et des libertés (CNIL) dans son avis consultatif. D'abord, parce que, à l'inverse d'un mot de passe, les données biométriques comme les empreintes digitales ne peuvent pas être changées en cas de piratage ou d'usurpation. Ensuite, il est techniquement possible de récupérer des empreintes digitales laissées par une personne sur les objets qu'elle touche.

Dans une lettre adressée lundi au président du Conseil national du numérique, M. Cazeneuve a insisté sur les précautions (le chiffrement des données notamment) déployées pour protéger les fichiers d'éventuels piratages.

Identification Le fichier tel que prévu ne permet pas d'identifier les personnes dans la base, mais seulement de les authentifier. La distinction est fondamentale : un fichier utilisé pour authentifier un individu, en comparant ses empreintes digitales pour s'assurer qu'il s'agit des mêmes que -celles qui sont en mémoire, est moins intrusif qu'un fichier utilisé pour identifier un individu, c'est-à-dire obtenir son identité à partir, par exemple, des empreintes digitales.

Concrètement, le fichier TES va permettre de s'assurer qu'une personne demandant un document d'identité n'a pas déjà fait des demandes identiques sous un autre nom, puisqu'il sera possible de vérifier si ses empreintes ont déjà été enregistrées. Le Conseil constitutionnel avait retoqué une base de données similaire, en 2012, au motif qu'elle pouvait servir à identifier, et pas seulement authentifier, des individus.

Autre exemple d'une base de données biométriques permettant d'identifier et dont la légalité fait débat, la base Agdref2, qui contient les empreintes biométriques, des dix doigts, de 7 millions d'étrangers présents légalement et illégalement en France. Elle peut notamment être utilisée pour identifier un individu à partir de ses empreintes. La CNIL avait cité cet argument pour s'opposer, en 2011, à la création de ce fichier, estimant que " si légitimes soient-elles, les finalités invoquées ne justifient pas la conservation de données biométriques telles que les empreintes digitales (...) ", et que ce dispositif " pourrait être de nature à porter une atteinte excessive à la liberté individuelle des personnes concernées " . C'est précisément un des risques de l'établissement d'un fichier unique : qu'il puisse servir, à terme, à identifier des Français.

Finalités Si l'utilisation de ce fichier est aujourd'hui clairement délimitée, il pourra en effet voir dans un second temps ses finalités élargies. C'est l'une des craintes de ses opposants : l'exemple du fichier des empreintes génétiques, créé en 1998, dont les finalités ont été notablement élargies depuis sa création, est avancé.

" Il est évident que ce n'est pas du tout aujourd'hui dans les finalités du fichier, qui a pour vocation de lutter contre l'usurpation d'identité, - mais - cet outil de grande ampleur peut faire craindre qu'il puisse être utilisé à d'autres fins, peut-être pas aujourd'hui, mais -demain? " , a expliqué Isabelle -Falque-Pierrotin, la présidente de la CNIL, à l'AFP. Une critique partagée par le Conseil national du numérique : " Les reculs démocratiques et la montée des populismes, observés, y compris en Europe et aux Etats-Unis, rendent déraisonnables ces paris sur l'avenir. "

L'outil légal choisi par le gouvernement, un décret et non une loi, laisse en tout cas à ce dernier (ou à un prochain) une plus grande souplesse pour en aménager les modalités. " A partir du moment où la base de 60 millions de personnes est là, on peut ajouter une fonction de recherche, par exemple. C'est d'autant plus facile qu'on est sur une base réglementaire, pas besoin d'adopter une nouvelle loi " , résume Guillaume Desgens-Pasanau, maître de conférences au CNAM et magistrat.

Un aménagement du décret pour permettre l'identification se heurterait cependant aux limites posées par le Conseil constitutionnel en 2012. C'est ce qu'a rappelé le ministre de l'intérieur dans sa réponseau Conseil national du numérique. De plus, il a expliqué que le fichier était techniquement organisé de sorte qu'il soit impossible de récupérer une identité à partir d'une empreinte digitale. C'est à la CNIL qu'incombe désormais de vérifier si tel est bien le cas, dans le cadre de ses missions de contrôle du fichier.

New York Times
Yahoo Employees Knew in 2014 About State-Sponsored Hacker Attack
Thursday, 10 November 2016
Byline: Vindu Goel

San Francisco - Yahoo employees knew in 2014 that a hacker backed by a foreign government had broken into its network, the company said in a securities filing on Wednesday.
But Yahoo did not say whether the attack that year -- which led to the theft of data like names, birth dates and encrypted passwords for more than 500 million accounts -- was disclosed to senior management at the time.

The timeline of who knew what about the attack and when has become central to the company's plan to sell its internet operations to Verizon Communications for $4.8 billion.

Yahoo first publicly disclosed the security breach on Sept. 22 this year, about two months after it struck the deal with Verizon. The company said it discovered the hacking, the largest known data breach affecting a private company, while investigating a hacker's claim in July to have obtained certain Yahoo user data.

The breach was not disclosed to Verizon during negotiations, and last month Verizon executives said that it might have materially diminished the value of Yahoo -- and could cause Verizon to reopen the deal, which is expected to close early next year.

In its latest disclosure, part of a quarterly filing about its finances, Yahoo said that it had discovered back in 2014 that a "state-sponsored actor" had gained access to its network. The company did not say what action, if any, it took at the time.

Yahoo also disclosed new details about the attack. The company said its board of directors and forensic experts were investigating "certain evidence and activity that indicates an intruder, believed to be the same state-sponsored actor responsible for the security incident, created cookies that could have enabled such intruder to bypass the need for a password to access certain users' accounts or account information."

Yahoo said that law enforcement authorities began sharing data with the company on Nov. 7 that purported to be Yahoo user information obtained by a hacker.

So far, 23 lawsuits related to the breach have been filed against Yahoo in the United States and abroad. The company said it was cooperating with federal, state, local and foreign officials seeking information about the breach.

Indo-Asian News Service

Symantec unveils new endpoint protection solution
Thursday, 10 November 2016

New Delhi - Leading cyber security company Symantec Corporation on Wednesday announced "Symantec Endpoint Protection 14" -- powered by artificial intelligence (AI) on the endpoint and in the cloud for better security.
The "Endpoint Protection 14" is the industry's first solution to fuse essential endpoint technologies with advanced machine learning and memory exploit mitigation in a single agent, delivering a multi-layered solution to stop advanced threats, the company said in a statement.

The solution delivers protection in a lightweight package, building on industry- leading 99.9 percent efficacy, low false positives and a 70 per cent reduced footprint over the previous generation through new advanced cloud lookup capabilities.

"Multi-layered protection, enabled by AI, backed by the world's most powerful threat intelligence force and powered by the Cloud, this is literally the smartest choice in endpoint technologies," Tarun Kaura, Director, Solution Product Management, Asia Pacific and Japan of Symantec, said in a statement.

Nextgov.com
Will Top Cyber Talent Join the Trump Team? Jury's Out
Thursday, 10 November 2016
Byline: Jospeh Marks

Washington - Will cybersecurity experts who shunned President-elect Donald Trump's campaign sign on to secure government and private sector networks during the Trump presidency? The answer's far from clear.
Some former officials and cyber experts sounded an optimistic tone Wednesday, saying duty to country would outweigh partisan divisions or hostility to Trump's particularly divisive style in technology and national security sectors.

Others were less sanguine.

"Given the overall shortage of experts in the cybersecurity workforce and the pay available in the private sector, it is always going to be hard filling top administration jobs with qualified candidates," said Ian Wallace, co-director of the New America think tank's Cybersecurity Initiative.

"Add to that the fact that some qualified candidates may not want to serve in a Trump administration, and we can expect that it will take a while to fill some of the government's top cybersecurity jobs," Wallace added.

Trump's campaign received little support from former national security leaders and tech executives. In August, 50 former Republican national security officials signed a letter opposing the brash real estate mogul's candidacy.

Whether tech and security leaders will hold onto that opposition now that the once-longshot candidate has been elected the next president of the United States could make the difference between whether government and private sector computer networks are more secure in four years or more vulnerable.

"My sense is that, out of patriotic duty, the transition is going to be staffed up and Donald Trump will be able to pull in some very experienced people on cybersecurity," said Robert Knake, former director for cybersecurity policy at the National Security Council.

"Fewer members of the national security community and the cybersecurity community in Washington were prepared for or expecting a Trump victory or had thought long and hard about would they be able or willing to take a massive pay cut and go into government service," Knake said. "Those conversations are happening now."

Tenable Network Security Chairman and Co-Founder Ron Gula, a former National Security Agency official, sounded a similar note.

"I think if the country calls and tells you, 'we want you to come secure the country,' most people are going to say yes," he said.

Others worried, though, that Trump's controversial campaign statements, such as advocating waterboarding, could make national security officials wary of the moral hazards of joining his administration.

"Based on his campaign rhetoric, I think there will be a lot of trepidation in the national security community," said Mark Fallon, a former Homeland Security Department official and director of the consultancy ClubFed. "Those types of inflammatory comments may seem flippant to him ... but I think people might think twice about wanting to join that administration."

The difficulty of staffing the Trump administration is exacerbated in cybersecurity because the pool of experts is comparatively small and private sector jobs pay much more.

Wallace noted the Obama administration had frequent difficulty finding talent for top cyber posts, especially the role of White House cybersecurity coordinator, which took the new administration roughly a year to fill.

Trump released a cybersecurity plan in October that included a full review of U.S. cyber defenses and vulnerabilities, mandatory cybersecurity training for government employees and increased coordination

between the Justice Department and federal, state and local law enforcement. The strategy also called for increasing the capacities of U.S. Cyber Command though it included few details.

The document did not explicitly mention some of the cyber debates roiling government such as whether to split the leadership of CYBERCOM from NSA, both of which are currently led by Adm. Michael Rogers, or to increase DHS authority to protect federal networks.

"I expect President-elect Trump will be challenged to find strong IT/cyber talent given that most leaders in the field, aside from Peter Thiel, opposed his election," said Jim Miller, former deputy undersecretary of defense for policy.

"I do hope that some top cyber talent will step up as a service to the nation at a critical time," Miller continued. "There is much important work to do, and there is no time to waste."

CBC News and Toronto Star
Top secret RCMP files reveal digital roadblocks in terrorism, major crime cases
Tuesday, 15 November 2016
Byline: Staff reporters

Ottawa - Suspected child predators, drug traffickers and extremists allegedly planning attacks or to join ISIS are escaping the eyes of the law due to increasingly impenetrable encryption and other digital roadblocks, according to top secret RCMP files reviewed by a CBC News/Toronto Star investigation. The Mounties provided access to the files in a bid to demonstrate how investigations of tech-savvy suspects are increasingly "going dark" because crucial evidence is beyond their reach.

The rare look inside active investigations comes amidst a thorny debate and public consultation on Canada's Anti-Terrorism Act (C-51), which includes proposals to significantly expand police powers.

Four ideas floated in the federal government's green paper on national security would enhance investigative capabilities, including the power to compel suspects to unlock their encrypted computers and cellphones and a law to require telecommunication and internet service providers to install interception and data-retention equipment in their networks.

But privacy and civil liberties advocates are fiercely opposed to such measures and demand police provide more evidence to justify their request for new powers.

RCMP Chief Supt. Jeff Adam admits law enforcement hasn't done a great job explaining the investigative challenges of the digital world to the public.

"So far, [the debate] appears to be driven very much from one side, which is those that would like more privacy and more anonymity," he said.

"What we need is an awareness of Canadians and lawmakers that our capabilities as they existed in the past, and the expectations of our ability to deliver on those, has changed significantly where we have less capability but potentially the same expectations."

To bolster its case, the RCMP granted one CBC reporter and one Toronto Star reporter access to 10 "high priority" investigations. The two journalists underwent RCMP screening to obtain top secret security clearance. They were then provided details and summaries of the 10 cases, though police withheld names, locations and other details to protect the investigations and potential court cases.

Digital chatter unreadable

In one case, police say they obtained warrants to conduct surveillance on a group of people in Eastern Canada suspected in a terrorism conspiracy.

They discovered the main suspect's phone was connecting to multiple cellular networks, none of which was technically equipped to intercept the suspect's text messages and internet traffic.

In late 2014, the Mounties spent two months and $250,000 to engineer a custom tool to intercept the target's communications only to discover all of it was encrypted and unreadable.

The individuals remain under investigation.

Laptops, phones blocked

In another case, the RCMP, working with foreign intelligence agencies, obtained warrants to intercept home and cellular phone communications of a group of suspected "high-risk travellers" in a city in Western Canada. Police believed they were planning to join extremist groups overseas.

Investigators attempted to intercept more than 30 laptops, cellphones and computers being used by the group but could only "successfully infiltrate" two of them. While those two devices delivered a bounty of evidence -- 4.4 million pieces of data, including videos, images, webpages, text messages and emails -- some of the data was encrypted and unreadable.

It's unclear whether the suspects have left Canada, and if so, whether they present any risk if they return.

In eight of the ten cases, the key stumbling block for police was either a lack of interception capabilities at the phone and internet companies or the use of encryption.

Harold O'Connell, RCMP director general in charge of national security investigations, says this combination is proving fatal for high priority investigations.

"When we do actually get the data, and it's encrypted, then we can't see it," he said. "And when we can't see it, then we can't analyze it ... You can't put together what the planning is. You can't put together any of the organizational hierarchy as to who is directing what."

Aaron Driver's online chats

The RCMP says the fatal confrontation with Aaron Driver in Strathroy, Ont., back in August is a prime example of a case in which encryption thwarted law enforcement's understanding of a threat.

Driver, a 24-year-old ISIS supporter suspected of planning a major urban attack, died after he detonated a bomb and was shot by police outside the house where he was staying.

"Hindsight would say that he was obviously farther along in preparing," said Jeff Adam, the RCMP's director general in charge of technical investigations services.

Driver attracted police attention in late 2014 when he posted comments online supporting ISIS and publicly defended Michael Zehaf-Bibeau, the extremist who gunned down a soldier at the National War Memorial and then charged across the street into Parliament's Centre Block, where police and security officers shot and killed him.

In early 2015, the RCMP and various international intelligence agencies discovered Driver was also communicating with well-known ISIS members and suspects directly involved in attacks in Texas and Australia. But the RCMP says his communication was via private Twitter messages and online chat forums protected by encryption and therefore unreadable by police.

In June 2015, police arrested Driver because they believed he posed a threat, but without hard evidence they couldn't charge him. Driver was released on a peace bond.

A year later, on Aug. 10, the FBI alerted the RCMP of an "imminent" attack being planned in Canada after it obtained an anonymous martyrdom video.

The RCMP quickly identified Driver as the man in the video, and by the afternoon had dispatched surveillance and SWAT teams to the house in Strathroy. When they arrived, Driver was climbing into a cab bound for London, Ont. As police approached, Driver detonated a bomb in the back seat of the taxi.

The taxi driver dove out of the cab moments before the explosion and suffered minor injuries.

Adam says police had long feared Driver was capable of a terrorist attack, but had no evidence he was co-ordinating one using a homemade bomb.

"It was good police work that caught him before he could detonate it in public, if that was his intent," Adam said. "The fact that he was out and available to do that is probably because we could not break the encrypted communications."

"And that's going dark. Couldn't get the evidence to charge him."

The Mounties have since completed forensic analysis and determined not all of the bomb material Driver was carrying exploded that day.

Investigators found the detonator ignited only a small portion of the explosives, which they say could have instantly killed or severely injured anyone within 2.1 metres.

Police also say they found 139 steel ball bearings (.38 calibre), which they believe were intended as shrapnel and could have killed or badly injured many more bystanders outside the immediate blast zone.

"The analysis tells us that if it had gone off, for example, on a city bus, there would've been death and grievous injuries," Adam said.

New police powers

The federal government launched its review of Canada's Anti-Terrorism Act and issued a green paper on national security in September. It discusses four proposals to enhance police capabilities:

The RCMP and other police leaders say aside from requests for basic subscriber information, these additional powers would be used only in targeted investigations and would require a warrant from a judge.

The RCMP's Harold O'Connell says technical barriers have made it difficult for investigators to keep pace with suspects and it's time for a public debate on the issue.

"We don't make the laws," he said. "We can influence, we can tell you what we think the lay of the land is, and then you as Canadians and legislators decide where you want us to be."

'Golden age of surveillance'

But privacy and civil liberties advocates aren't convinced police investigations are actually "going dark."

Ann Cavoukian, Ontario's former privacy commissioner who now runs Ryerson University's Privacy and Big Data Institute, says the metaphor doesn't give the public a complete picture.

"Even though you may not be able to access encrypted communications -- the actual content -- you can access the metadata," Cavoukian said, referring to digital logs of the time, date and location of every web query, call, text or email a user exchanges. "There is so much available to you if you actually connect the dots -- put all the pieces together."

Micheal Vonn, policy director of the BC Civil Liberties Association, says police have failed to provide sufficient evidence that each of these new powers is necessary.

"One of the great truths of the era that we're in Post-Snowden, is that we're in a golden age of surveillance," she said.

"Police have access to more information about us than they have ever had in the history of the world."

She strongly opposes allowing police to request basic subscriber information without a warrant and says the proposal to grant police the power to demand a suspect hand over their device passwords or encryption keys is "radical" under Canadian law.

"We want the police to have appropriate powers," she said. "We want appropriate oversight and constraints on those powers so that we know that we're actually getting the balance right."

The federal government won't comment on which, if any, changes to police powers it plans to endorse. The online public consultation continues until Dec. 1.

Toronto Star and CBC News
Police, Power and Privacy
Tuesday, 15 November 2016
Byline: Staff reporters

OTTAWA -- The RCMP has provided unprecedented access to the Toronto Star and the CBC in an effort to make its case that antiquated laws and diminished police powers in the digital age are allowing suspected terrorists, drug gangs and child abusers to operate beyond the law.
Journalists from the two media outlets have reviewed the details of 10 high-priority cases after clearing RCMP security checks for access to "top- secret" information. In each case, investigators were stonewalled by legal and technical obstacles in accessing digital evidence, the Mounties say. Most of the suspects remain at large.

These cases stand at the centre of an emerging national debate.

Police argue they are on the losing side of a digital divide, while on the other side are tech-savvy criminals who are shielded by impenetrable encryption, telecommunication companies and technology manufacturers.

Privacy advocates argue that police have never before had such powers of surveillance and that they have failed to provide evidence that the public's safety is in jeopardy.

The audience is Canadians who are alarmed to learn that some criminals are increasingly beyond the reach of the law. They are equally alarmed by the recent Federal Court ruling that denounced the national spy agency, CSIS, for illegally gathering the private information of Canadians, and by news that Quebec police forces intercepted and tracked the cellphones of as many as 10 journalists to discover their sources.

"We need a public debate," said RCMP Chief Supt. Harold O'Connell, the force's director general of national security investigations. "We can influence, we can tell you what we think the lay of the land is, and then you, as Canadians and legislators, decide where you want us to be."

Among the cases reviewed by the Star and the CBC:

An investigation into a group suspected of plotting terrorist acts in Canada. After obtaining a warrant, the RCMP spent two months and $250,000 attempting to intercept electronic communications. This produced no evidence because investigators were cut short by encryption that police experts were unable to break.

"These are individuals that are ... developing plans in order to commit offences in Canada," said O'Connell. "What we wanted to do was to listen to, read, see the data that the individuals are communicating."

That never happened. The suspects remain under investigation.

The RCMP attempted to intercept and decode the communications of an alleged drug and human trafficking ring, but still don't have enough evidence to charge the group's leaders. The RCMP seized kilos of cocaine and arrested low-level members. While they successfully intercepted some communications with a warrant, they failed to decrypt the messages.

"When we can't see (data), then we can't analyze it. And if you can't analyze it, then you can't actually put together what the transactions are," said O'Connell. "You can't put together what the planning is. You can't put together any of the organizational hierarchy."

The organized crime leaders are still operating.

In a western Canadian national security case involving "high-risk travellers" who police believe were involved in "terrorist activity" abroad, investigators collected evidence from only two of more than 30 digital devices.

Those two devices provided 4.4 million "digital footprints," including websites, images, videos and electronic messages. But little hard evidence emerged. After thousands of investigative hours, costly surveillance teams and $1 million spent on failed technical solutions, the suspects remain under investigation. It is unclear whether they have left Canada or if they pose a public safety risk.

"Criminals, to some extent, are walking away from crimes in Canada," said former OPP deputy commissioner Scott Tod, now deputy chief in North Bay and co-chair of the Canadian Advanced Technology Alliance's cybercrime advisory committee.

"Encryption has really changed the game on how we are able to access information that we require for court purposes. Being unable to access information makes it extremely difficult for us to form the prospect of conviction."

Public consultations in the review of Canada's Anti-Terrorism Act - currently taking place across Canada - include proposals that, if adopted, would empower police with vastly greater digital investigative powers.

Among those proposals: legislation to compel suspects to unlock - or "decrypt" - digital devices at the request of police who have a judge's warrant; giving police access to basic digital subscriber information - such as a person's name and address - without having to obtain a warrant; and compelling telecommunications companies to retain data and help police intercept communications.

Privacy advocates call such measures an indefensible power grab that would undermine civil liberties.

"Police have access to more information about us than they have ever had in the history of the world," said former Ontario information and privacy commissioner Ann Cavoukian, now executive director of the Privacy and Big Data Institute at Ryerson University.

Even without breaking into encrypted communications, police can access volumes of metadata - high-level records that won't show the content of messages, for example, but provide such details as author, creation date and file size.

"There is so much available to you if you actually connect the dots - put all the pieces together," Cavoukian said.

Police are beneficiaries of the "golden age of surveillance," said Micheal Vonn, policy director of the B.C. Civil Liberties Association.

"It's very fair to make statements, but you have to back them up with evidence ... You can't simply make the claim and expect us to rebalance the entire configuration of how we protect our rights."

Many police officials who were interviewed acknowledge that the privacy argument has dominated the debate.

"Law enforcement has not been as open or as communicative as they should have been," said RCMP Chief Supt. Jeff Adam.

But police filing cabinets contain growing evidence that digital investigative limitations pose a risk to public safety, he said.

"I believe that the (public's) expectations and our ability to deliver on those are far apart and getting farther away every day," he said. "Canadians should ask themselves whether or not they're satisfied that we cannot get evidence ... Is that where they want the state of affairs to be, where we cannot enforce the law?"

Toronto Star
Inside RCMP's file room

Tuesday, 15 November 2016
Byline: Robert Cribb

OTTAWA -- The RCMP shared details of 10 ongoing "high-priority" investigations with the Toronto Star and CBC News to begin a public debate on expanding police capabilities while investigating crimes involving digital and online evidence.
This coincides with a federal review of Canada's Anti-Terrorism Act (Bill C-51) and a public consultation on the government's Green Paper on National Security, which includes proposals to enhance police digital capabilities.

To allow access to the investigations, the RCMP conducted security screening and granted top-secret clearances to Robert Cribb of the Toronto Star and Dave Seglins of CBC News.

The RCMP provided summaries and interviews on the cases but withheld names, locations and key details that could compromise ongoing investigations, prosecutions and secretive police techniques.

The following are case summaries prepared by the Toronto Star and CBC:

Case 1: Child abuse video on locked phone

Police have testimony from a child alleging sexual assault by their father who they say recorded the crime on his phone. The phone is locked by a pass code and investigators have not been able to access the video, which would be crucial evidence. Police have no legal authority to compel the man to unlock his phone. The case remains under investigation.

Case 2: VoIP phones encrypted

The RCMP obtained a warrant to tap the phones of an individual suspected of financial fraud in Eastern Canada, only to discover that the VoIP (voice over Internet protocol) phone network the suspect was using encrypted the calls. Police made several covert entries into the suspect's office to install devices to bug the calls. At one point, the interception method failed, and for two weeks "valuable" evidence was missed.

Case 3: 'Too much information' tests RCMP capacity

RCMP intercepted cell and residential communications of a "high-risk traveller" in Eastern Canada suspected of planning to join a terrorist group overseas. The Internet/phone provider lacked interception capabilities, so police spent considerable resources to install their own equipment, but were eventually swamped by 21 million data points (web searches, images, videos, texts). Much of the data was encrypted and unintelligible. The case remains under investigation.

Case 4: Delays seeking foreign info

RCMP waited close to four months to get "high-value" evidence in order to stop a suspected "high-risk traveller" from leaving their home in Western Canada to join extremists overseas. Police say they concluded the case but were hampered by an inability to intercept communications outside of Canada and delays in the MLAT (mutual legal assistance treaty) process. Police had to forward a Canadian judge's order through government channels, which were then delivered to a social media company outside the country. The company eventually filled the order, sending the material back to police - again through government channels - but police discovered the messages were encrypted and unreadable.

Case 5: A 10-month wait to access records

During an investigation into a group of Daesh (also known as ISIS or ISIL) supporters who police believed were "high-risk travellers" based in Eastern Canada, the RCMP spent 10 months trying to obtain social media communications outside Canada. Analysis of the data is continuing, and police have evidence that one of the suspects is abroad in a "high-risk country." The case remains under investigation.

Case 6: Terrorist group communications prove elusive

RCMP are investigating a group of individuals suspected of participating in a terrorist organization and plotting to travel overseas. Police attempted a court-ordered interception of their devices but found the communications were encrypted. As a result, police had to design technical solutions which meant they needed an extension of the court order, and this has delayed the process. The communications among the suspected terrorists have not been obtained. The case is still under investigation.

Case 7: Digital chatter unreadable

RCMP obtained warrants to conduct surveillance on a group of people in Eastern Canada suspected in a terrorism conspiracy in 2014. Police discovered the main suspect's phone was connecting to multiple different cellular networks, none of which was technically equipped to intercept the suspect's text and Internet traffic. The Mounties spent two months and $250,000 to engineer a custom tool that would intercept the target's communications, only to discover all of it was encrypted and unreadable. The individuals remain under investigation.

Case 8: Interception too costly

The RCMP seized kilos of cocaine and arrested low-level members of an alleged drug and human trafficking organization in Eastern Canada. After obtaining a warrant to monitor suspects' communications, investigators determined it would cost hundreds of thousands of dollars to install interception hardware at the targets' Internet service provider (ISP). Police abandoned the effort and resorted to using undercover officers and agents. The alleged criminal bosses and organization are still operational.

Case 9: Laptops, phones blocked

The RCMP, working with foreign intelligence agencies, obtained warrants to intercept residential and cellular traffic of a group of suspected "high-risk travellers" in a city in Western Canada. Police believed they were planning to join extremist groups overseas. Investigators attempted to intercept more than 30 laptops, cellphones and computers being used by the group but could only "successfully infiltrate" two of them. While those two devices delivered a bounty of intercepted evidence - 4.4 million pieces of data, including videos, images, web pages, text messages and emails - some of the data was encrypted and unreadable.

Case 10: Aaron Driver's encrypted chats

The RCMP was unable to read Daesh supporter Aaron Driver's encrypted messages in 2015 to and from other suspects involved in attacks in Texas and Australia. Despite suspicions, RCMP say encryption thwarted their ability to understand how far along Driver may have been in his bomb plot. He was killed in August 2016 outside his home in Strathroy, Ont., after police were tipped off to a martyrdom video Driver had made. The FBI alerted Canadian police to an "imminent" attack. He was killed amidst police gunfire and the partial detonation of a bomb he was carrying.

New York Times
Secret Backdoor in Some U.S. Phones Sent Data to China, Analysts Say
Tuesday, 15 November 2016
Byline: Matt Apuzzo, Michael S. Schmidt

Washington - For about $50, you can get a smartphone with a high- definition display, fast data service and, according to security contractors, a secret feature: a backdoor that sends all your text messages to China every 72 hours.
Security contractors recently discovered preinstalled software in some Android phones that monitors where users go, whom they talk to and what they write in text messages. The American authorities say it is not clear whether this represents secretive data mining for advertising purposes or a Chinese government effort to collect intelligence.

International customers and users of disposable or prepaid phones are the people most affected by the software. But the scope is unclear. The Chinese company that wrote the software, Shanghai Adups Technology Company, says its code runs on more than 700 million phones, cars and other smart devices. One American phone manufacturer, BLU Products, said that 120,000 of its phones had been affected and that it had updated the software to eliminate the feature.

Kryptowire, the security firm that discovered the vulnerability, said the Adups software transmitted the full contents of text messages, contact lists, call logs, location information and other data to a Chinese server. The code comes preinstalled on phones and the surveillance is not disclosed to users, said Tom

Karygiannis, a vice president of Kryptowire, which is based in Fairfax, Va. "Even if you wanted to, you wouldn't have known about it," he said.

Security experts frequently discover vulnerabilities in consumer electronics, but this case is exceptional. It was not a bug. Rather, Adups intentionally designed the software to help a Chinese phone manufacturer monitor user behavior, according to a document that Adups provided to explain the problem to BLU executives. That version of the software was not intended for American phones, the company said.

"This is a private company that made a mistake," said Lily Lim, a lawyer in Palo Alto, Calif., who represents Adups.

The episode shows how companies throughout the technology supply chain can compromise privacy, with or without the knowledge of manufacturers or customers. It also offers a look at one way that Chinese companies -- and by extension the government -- can monitor cellphone behavior. For many years, the Chinese government has used a variety of methods to filter and track internet use and monitor online conversations. It requires technology companies that operate in China to follow strict rules. Ms. Lim said Adups was not affiliated with the Chinese government.

At the heart of the issue is a special type of software, known as firmware, that tells phones how to operate. Adups provides the code that lets companies remotely update their firmware, an important function that is largely unseen by users. Normally, when a phone manufacturer updates its firmware, it tells customers what it is doing and whether it will use any personal information. Even if that is disclosed in long legal disclosures that customers routinely ignore, it is at least disclosed. That did not happen with the Adups software, Kryptowire said.

According to its website, Adups provides software to two of the largest cellphone manufacturers in the world, ZTE and Huawei. Both are based in China.

Samuel Ohev-Zion, the chief executive of the Florida-based BLU Products, said: "It was obviously something that we were not aware of. We moved very quickly to correct it."

He added that Adups had assured him that all of the information taken from BLU customers had been destroyed.

The software was written at the request of an unidentified Chinese manufacturer that wanted the ability to store call logs, text messages and other data, according to the Adups document. Adups said the Chinese company used the data for customer support.

Ms. Lim said the software was intended to help the Chinese client identify junk text messages and calls. She did not identify the company that requested it and said she did not know how many phones were

affected. She said phone companies, not Adups, were responsible for disclosing privacy policies to users. "Adups was just there to provide functionality that the phone distributor asked for," she said.

Android phones run software that is developed by Google and distributed free for phone manufacturers to customize. A Google official said the company had told Adups to remove the surveillance ability from phones that run services like the Google Play store. That would not include devices in China, where hundreds of millions of people use Android phones but where Google does not operate because of censorship concerns.

Because Adups has not published a list of affected phones, it is not clear how users can determine whether their phones are vulnerable. "People who have some technical skills could," Mr. Karygiannis, the Kryptowire vice president, said. "But the average consumer? No."

Ms. Lim said she did not know how customers could determine whether they were affected.

Adups also provides what it calls "big data" services to help companies study their customers, "to know better about them, about what they like and what they use and there they come from and what they prefer to provide better service," according to its website.

Kryptowire discovered the problem through a combination of happenstance and curiosity. A researcher there bought an inexpensive phone, the BLU R1 HD, for a trip overseas. While setting up the phone, he noticed unusual network activity, Mr. Karygiannis said. Over the next week, analysts noticed that the phone was transmitting text messages to a server in Shanghai and was registered to Adups, according to a Kryptowire report.

Kryptowire took its findings to the United States government. It plans to make its report public as early as Tuesday.

Marsha Catron, a spokeswoman for the Department of Homeland Security, said the agency "was recently made aware of the concerns discovered by Kryptowire and is working with our public and private sector partners to identify appropriate mitigation strategies."

Kryptowire is a Homeland Security contractor but analyzed the BLU phone independent of that contract.

Mr. Ohev-Zion, the BLU chief executive, said he was confident that the problem had been resolved for his customers. "Today there is no BLU device that is collecting that information," he said.

Reuters
Snowden warns of increase in U.S. domestic spying after Trump victory
Tuesday, 15 November 2016
Byline: Staff report

Buenos Aires - Donald Trump's election as U.S. president raises concern that Washington may increase the intrusiveness of domestic intelligence gathering, former U.S. spy agency contractor Edward Snowden said on Monday, warning that democratic checks and balances were losing ground to authoritarianism.
Snowden lives in Moscow under an asylum deal after he leaked classified information in 2013 that triggered an international furor over the reach of U.S. spy operations. He spoke at a teleconference hosted by Buenos Aires University's law school.

"We are starting to substitute open government for sheer authoritarianism, a government based not upon the principle of informed consent granted by people who understand its activities but rather a trust in personalities, a trust in claims, a trust in the hope that they will do the right thing," Snowden said.

Washington pledged not to engage in indiscriminate espionage following Snowden's 2013 disclosures. But Snowden questioned if that policy could be modified by new officials "who have a very different set of values and can govern in the dark."

"If government does actually win our trust, because they go for some years and they do operate in a way that we should support, what happens when it changes?" he asked.

"This is kind of the challenge that we're facing today in the United States with the result of the last election."

Supporters see Snowden as a whistleblower who boldly exposed government excess. But the U.S. government has filed espionage charges against him for leaking intelligence information.

Trump, who scored an upset win over Democrat Hillary Clinton in last Tuesday's election, broke with many in his own Republican Party during the campaign and emphasized his success as a businessman and reality TV show star. He promised sweeping security measures to deal with the threat of attacks on the United States.

His election was greeted with concern from the American Civil Liberties Union over statements he made during the campaign supporting increased surveillance of U.S. Muslims, mass deportation of illegal immigrants, reauthorization of waterboarding and changing libel laws to increase press restrictions.

Snowden, asked if he thought the election of Trump, who has praised Russian President Vladimir Putin as a strong leader, might increase chances of him being pardoned by the U.S. government, responded: "Who knows?"

Deutsche Welle

German Constitutional Court rules out access to NSA's 'selectors' list
Tuesday, 15 November 2016
Byline: Staff report

Berlin - The Constitutional Court in Karlsruhe on Tuesday delivered a verdict, saying the government in Berlin did not need to transfer its secret list of spy targets to the commission investigating the US' spy agency NSA's activities in Germany.
The government's need to keep certain data confidential outweighed the NSA commission's desire for more details on the issue in this case, judges said in an October decision that was made public on Tuesday.

The verdict also said that releasing the "selectors" list without approval from the United States could endanger the functioning of intelligence agencies and jeopardize Germany's effectiveness in matters of national security.

Green party politician Konstantin von Notz, who is on the parliamentary committee investigating NSA issues, expressed disappointment at Tuesday's verdict. "Large portions of the illegal BND practices conducted over years will remain in the dark," he said in Berlin, adding that because of the way the systems worked, further scandals and rights violations were "pre-programmed."

Tuesday's ruling was a response to a complaint by the Greens and left-wing party "Die Linke" members as well as the leaders of the NSA fact-finding commission, lodged after the German government denied them access to the list.

The "selectors" list details search criteria like telephone numbers, email addresses and IP addresses of people, including European politicians and heads of corporations, who were monitored by the NSA, with the help of Germany's foreign espionage agency, the BND. Targets also included many European political leaders, including German Chancellor Angela Merkel. The scandal dates back to the intelligence leaks mainly attributable to former NSA contractor Edward Snowden, now living in self-imposed exile in Russia.

Instead of handing over the list to the commission, the ruling coalition in Berlin appointed an administrative judge, Kurt Graulich, as a "person of trust." Graulich analyzed the list and then briefed the investigative commission on its contents, but judges at the constitutional court said this did not give the body any right to demand exact information.

The judges applauded the German government for passing on some information in this way. In justifiying its ruling, it said that the selectors list was "more of a general political interest," rather than being central to the welfare of the state or the government's capacity to function, criteria that might have prompted a different decision.

China Daily
Cybersecurity Law aims to 'protect people's interests'
Tuesday, 15 November 2016
Byline: Cao Yin

Beijing - Cybersecurity and related issues have been hot topics among internet and judicial experts since China's first Cybersecurity Law was adopted earlier this month.
The law and its related topics, including how to put coordination of government departments into practice and how to review products and services before they are made available on the internet, will also be heated topics of discussion at the World Internet Conference, experts said.

Li Yuxiao, secretary-general of the Cybersecurity Association of China, said that he will go to Wuzhen, Zhejiang province, to participate in the third WIC, which runs from Wednesday to Friday, adding that one of his focuses will be legal issues.

"It's good to see that our nation has finally drawn up and adopted its first Cybersecurity Law," Li said.

"It's the guide when we draft some other cybersecurity-related rules, and I think its adoption has brought more confidence to internet and judicial professionals," he said. "I'd like to share the law with foreign guests and listen to their opinions at the conference."

The law, with 79 articles, was approved by the Standing Committee of the National People's Congress, China's top legislature, on Nov 7, and will be effective on June 1, 2017.

"The lawmaking is to maintain State security and protect people's interests," said Yang Heqing, deputy director of the office for economic law under the NPC Standing Committee's Legislative Affairs Commission.

The law also aroused public attention overseas, as some foreigners have a great concern about one article - online products and services that could form China's key internet infrastructure or affect State security must pass a governmental review to enter the Chinese market.

In response to the concern, Zhao Zeliang, head of cybersecurity for the Cyberspace Administration of China, said: "The article of the law does not mean that we'll block foreign web products and services."

Zhao denied the article is a trade barrier, saying there is some misunderstanding overseas.

Wang Sixin, a law professor specializing in cybersecurity at the Communication University of China, suggested guests from home and abroad at Wuzhen should discuss it to reduce misunderstanding.

"The review is a necessity, as some products with security risks may harm the internet," Wang said. "If we cannot find them quickly, the damage will be more serious."

The review also targets every product or service that tends to be in the market, no matter where they are from, he said, adding that similar checks are also being conducted in the United States and the European Union.

He said the conference is a good opportunity and platform to communicate and reach consensuses, saying that the more discussion there is on the law, the better it can play a role in cyberspace governance.

Zuo Xiaodong, vice-president of the China Information Security Research Institute, said the law is a milestone.

"It's a progress that the law clarifies the responsibilities of governments, enterprises and individuals in cyberspace, and measures on how to deal with cyber emergencies," Zuo said.

Press Association
Amber Rudd orders Lauri Love extradition to US on hacking charges
Monday, 14 November 2016
Byline: Staff report

London - The home secretary, Amber Rudd, has signed an order for the extradition of a British man to the US, where his lawyers believe he could face up to 99 years in prison if convicted of computer hacking charges.
Lauri Love is accused of stealing large amounts of data from US government agencies such as the Federal Reserve, the army, the Department of Defence, Nasa and the FBI in a spate of online attacks in 2012 and 2013.

The 31-year-old activist, who has Asperger's syndrome, lost his legal challenge to avoid extradition in September, and on Monday the Home Office said the necessary order allowing his removal had been signed after Rudd "carefully considered all relevant matters".

The Home Office said Love "has been charged with various computer hacking offences which included targeting US military and federal government agencies". He has 14 days to appeal against the order and is expected to do so.

Love, who also has depression and eczema, had argued that his health means a jail term in the US could drive him towards a mental breakdown or suicide.

However, the district judge Nina Tempia said in her ruling on 16 September that Love could be cared for by "medical facilities in the United States prison estate".

She said he faced "extremely serious charges" and, while she accepted he suffered from "both physical and mental health issues", she believed provision for his condition was adequate in the US.

US authorities have been fighting for Love to face trial there. He could face proceedings in three different US jurisdictions. Rudd had been given a deadline of 16 November to decide whether or not to order his extradition.

It is alleged that between October 2012 and October 2013, Love placed hidden "shells" or "backdoors" within networks, allowing for confidential data to be stolen. He is accused of causing millions of dollars' worth of damage.

Love's father, Alexander, said in response to Rudd's decision: "It was going to happen - it was inevitable - but it's still painful. I cannot begin to express how much sorrow it causes me. All we are asking for is British justice for a British citizen."

Barry Sheerman, one of more than 100 MPs who signed a letter calling on Barack Obama to block Love's extradition, said he was "deeply disappointed".

"We are still keeping up the pressure. We are getting more and more MPs to sign the letter to President Obama," the Labour MP for Huddersfield said. "The pressure continues, we won't give up."

Reuters
Bangladesh's central bank hopes to recover $30 million stolen in cyber heist
Tuesday, 15 November 2016

Dhaka - Bangladesh's central bank hopes to retrieve $30 million more of the $81m stolen from its account at the New York Federal Reserve in February, two bank officials said on Monday.
Hackers used stolen Bangladesh Bank credentials to try to send three dozen SWIFT messages to transfer nearly $1 billion from its Fed account. They succeeded in transferring $81m to four accounts at Rizal Commercial Banking Corp in Manila.

Most of the money was laundered through casinos in Manila. On Friday, Philippine authorities began the process of handing over $15.25m to Bangladesh.

"We are hoping to get back around $30m which remains frozen," Bangladesh Bank deputy governor Abu Hena Mohammad Razee Hassan, who heads its financial intelligence unit, told Reuters.

A Bangladesh team is likely to visit the Philippines at the end of the month to accelerate the process, he said.

"We are expecting to get a favourable verdict from Supreme Court of the Philippines as it has already been proved that $81m is our money," said another Bangladesh Bank official, who asked not to be identified because he was not authorised to talk to the media.

Times of Israel
Elbit Systems unveils New Anti-Drone System
Tuesday, 15 November 2016

Jerusalem - Elbit Systems will reveal at the Israel HLS & Cyber Conference, taking place this week in Tel Aviv, Elbit Systems EW and SIGINT Elisra's ReDrone system, a solution for protection of closed air spaces, national infrastructures and other critical areas against hostile drones penetrating the protected perimeter.
ReDrone is designed to detect, identify, track and neutralize different types of drones that are flown within a range of radio frequency communication protocols. The system will be presented at the conference along with Elbit Systems' SupervisIR, an infra-red wide-area persistent ISTAR (information, surveillance, target acquisition and reconnaissance) system. SupervisIR can be integrated and operated within the ReDrone system thus enabling full-scale Signal Intelligence (SIGINT) and thermal imaging detection capabilities of hostile drones.

The ReDrone's open system architecture allows multiple hardware configurations, including an array of controllers and sensors for target detection, tracking and engagement. The system is also capable of separating a drone's signals from its operator's remote control signals, as well as pinpointing both the drone and the operator's directions. The detection system provides 360-degree perimeter protection and complete, up-to-the- minute situational awareness. It can also deal with a number of different drones simultaneously. Due to its passive detection features, ReDrone also enhances environmental protection and supports the safety of civilians and air platforms inside the secured airspace.

After detecting a target, the ReDrone system disrupts the drone's communication with its operator, blocks its radio and video signals and GPS positioning data, and sends it off track, preventing it from carrying out an attack.

Gulf Times
Vodafone shares its expertise in tackling cyberwarfare
Tuesday, 15 November 2016

Doha - Vodafone shared its global expertise in tackling cyberwarfare at the Qatar Central Bank's (QCB) recent 3rd annual 'Information Security Conference' for the financial sector.
This is also the second time that Vodafone participates as a sponsor of the event. The event was held at the Sheraton under the patronage of HE the Prime Minister and Minister of Interior, Sheikh Abdullah bin

Nasser bin Khalifa al-Thani, in the presence of HE the QCB governor, Sheikh Abdullah bin Saoud al-Thani; and HE the Minister of Transport & Communications, Jassim Seif Ahmed al-Sulaiti.

Vodafone Qatar's director (Information Security) Shaik Abdulkhader delivered a presentation on cyberwarfare and showcased Vodafone's cyber security portfolio for both the consumer and enterprise segments such as its DDoS Mitigation Service and Secure Device Management.Vodafone's chief business officer Mahmud Awad said, "Cyberwarfare is the number-1 national security threat ahead of terrorism and espionage with cyber-attacks continuing to evolve in the region, and show a continuation of extremely high volume of attacks posing a huge risk to organisations and governments.

Vodafone is committed to bringing our global expertise and leading edge technology to Qatar to help protect organisations and people whilst contributing to the development of a knowledge based economy."

Vodafone, a founding member of the IoT Security Foundation, was the first service provider globally to offer a managed DDoS mitigation service protecting its customers from DDoS attacks since 2004. Vodafone was also the first company in Qatar to offer 'Secure Device Management' to help businesses better protect their company data.

Khaleej Times
Cyberspace security, power building and geopolitical impact up for debate at ADSD
Tuesday, 15 November 2016

Abu Dhabi - As the world today shows great concerns and interests pertaining to Cyberspace Security, the "Third Abu Dhabi Strategic Debate 2016" gave a special focus to the issue and designated a panel to address the threats linked to a phenomena gaining powerful impact on governments and organisations across the globe.
Speakers of the panel included Barry Pavel, Vice President, Arnold Kanter Chair, and Director, Brent Scowcroft Center on International Security at the Atlantic Council, Josh Corman, Director of the Cyber Statecraft Initiative at the Atlantic Council and Moderator Dr. Zaid Eyadat, Prof. of Political Science at UCONN, Georgetown and EPC adviser.

Barry Pavel, Vice President, Arnold Kanter Chair, and Director, Brent Scowcroft Center on International Security at the Atlantic Council, said "We're at the beginning of a new age in history and we require strategic foresight to imaging what's coming in the future of cyberspace. This age is experiencing a functioning and a functional internet. We need to communicate, operate and in the security sphere. It's global in every aspect".

"Cyber is mastered by some of the major actors such as Russia. On the technical side.The system is getting increasingly complex although the US and Russia seem to be on the same level of advancement

We should give more importance in foreign policy and defense to cyber security. We can close on ISIS on the field, but if we don't do so online then we cannot defeat them", Pavel stressed.

Josh Corman, Director of the Cyber Statecraft Initiative at the Atlantic Council, emphasized "It's important to bridge the technical community with the international one. The private sector is far more concerned with the ability to defend and protect individuals from attacks and breaches. It's less about the big data and technology nowadays".

"In the Arab region there is tremendous investment in future smart technology. If we can raise the cyber hygiene enough, we can protect ourselves better from attacks". Corman added.

The cyber security threat is now widely understood to be real and growing, and increasingly touches on every facet of our connected world.

Saudi Gazette
Beware of hackers, IT expert tells Saudis
Tuesday, 15 November 2016
Byline: Staff Report

Dammam - Educational and cultural awareness programs through schools and social networking sites have contributed greatly to reducing cases of hacking electronic gadgets and websites of Saudis from 70 percent in 2014 to 25 percent in 2016, said an expert.
Speaking to Al-Watan Arabic daily, Khaled Abu Ibrahim, executive director of Saudi IT Consulting Co., said hacking of Saudis' electronic devices reached its peak in 2014, hitting 70 percent and it reduced to 45 percent in 2015 and 25 percent this year as a result of awareness programs.

He said some people break into social media accounts of individuals without any specific purpose. "It has been noticed that some hackers break into Facebook, Twitter and other social media accounts as well Internet websites regularly," he told Al-Watan Arabic daily.

Sociologist Latifa Bin Humaid spoke about the negative impact of hacking electronic sites on the society as it leads to many crimes. "People try to get secret information and make use of them for their vested interests. They will also tamper with databank of companies and organizations."

Stealing money from bank accounts and transferring money from one account to another are other crimes committed by hackers. Hackers also engage in impersonation, blackmailing, threatening and break into the websites of major government departments and corporations.

IT engineer Abu Ibrahim urged individuals and companies to be cautious about hackers who get into their websites and social media accounts. Hackers use various methods to break into their sites despite advanced security firewalls and systems, he added.

"They often get into our devices and websites by promoting news of celebrities and major commercial firms," he pointed out. "Saudis have achieved tremendous progress in using computer systems but still they fall into the traps of hackers," he added.

He described the Internet as a double-edged sword. "Some unknown people send messages through the Internet for various purposes. There are some companies that want to collect various information about Arab youth and we don't know their hidden objectives."

Abu Ibrahim urged Saudi youth to use the Internet carefully to enhance their knowledge and interact with other people and they should be cautious about people and agencies that try to influence and change their religious faith and values.

"Hackers use WhatsApp to get into personal information of users as they forward news of celebrities and companies and promise fake prizes in order to entrap users of the popular social media. People should check links before opening them to avoid hacking," he explained.

The National (UAE)
Abu Dhabi security conference sets focus to cyber threats
Tuesday, 15 November 2016
Byline: Caline Malek

Abu Dhabi - How to stay ahead of online threats and combat them will be at the heart of discussions at a cybersecurity conference that kicks off in the capital on Tuesday.
Defining a new security roadmap, the current state of electronic security, advanced threat detection and risk management are some of the topics that will be discussed by more than 1,000 security experts and officials at the two-day RSA conference.

The predominant concern for the UAE is the transition to smart cities. "The UAE has experienced a growth of digitalisation, smart cities and smart government," said Scott Manson, cybersecurity leader for the Middle East and Turkey at Cisco.

"We're seeing through this innovation age a lot more need for more security and a huge amount of cybertechnology."

He said if the UAE continued to grow and benefit from digitalisation, the way forward would be to continue to oversecure its intellectual property and key data.

Fifty sessions will tackle critical infrastructure, cybercrime and threats and analytics as well as incident response.

"As the smart city grows, more people will share data, on a personal and professional level - hence there are more concerns around security and privacy," said Ibrahim Almallouhi, vice president of security operations at telecoms company du.

He said that cybersecurity was not only critical to the UAE, but also to the whole world.

"In the UAE, we are working with the Government to bring the country's smart city ambitions to life," Mr Almallouhi said. "As connectivity continues to proliferate, it is incumbent on us to ensure that data and compliance is protected the right way."

Experts say the Middle East is rapidly recognising its level of vulnerability to cyberattacks.

"As more systems become interconnected with the internet, they can be targeted," said Faisal Al Bannai, founder of UAE cybersecurity company DarkMatter. "The areas of concern for the region are information theft and cyberextortion, where cybercriminals are leveraging threats to disrupt or deny service if a ransom is not paid."

Two-time Formula One champion Mika Hakkinen will speak about risk management in his sport. Hakkinen said drivers have turned to data acquisition, analysis and predictive analytics to better manage risk.

"We have developed a fully connected digital communications environment, which means that for a driver we can make better real decisions to protect ourselves."

Linda Martin, the conference's general manager, said one of the major drivers of technology was people's desire to connect.

"The internet has allowed us to do that so easily, but the downside is a proliferation of attackers," she said. "The conference gives the region that platform to come together and share knowledge."

New Straits Times
Darknet makes IS more dangerous
Tuesday, 15 November 2016
Byline: Shahzeb Ali Rathore

Kuala Lumpur - Terrorist and non-state actors have used different modes and mediums to spread their message and communicate with their comrades. The dawn of the Internet has also provided such groups with unparalleled opportunities to establish communications and operational links that were not possible before. Starting from websites, terrorist groups moved to more interactive mediums like chatrooms and forums. Social media platforms, Facebook and Twitter, truly revolutionised how

militants, terrorists and non-state actors communicated with each other, recruited sympathisers and supporters, and disseminated their propaganda.
The Islamic State perfected the use of social media, which became the preferred source for the "jihadists" or "soldiers of the Caliphate". In response, technology companies have been compelled to take down Facebook and Twitter accounts affiliated with IS. Because of these supporters, sympathisers and members of jihadist groups have moved into the deep web and the darknet.

Deep web and darknet are interchangeably used, but they are two different things. The deep web includes all those web pages that a search engine, such as Google, cannot find. This includes web pages that are password-protected, all webmail, private Facebook accounts, user databases and pages behind paywalls. Websites that are not indexed by Google are also part of the deep web. The surface web is all that Google has indexed and a user can access it using any search engine.

It is said that the surface web is only the "tip of the iceberg" and the deep web comprises more than 90 per cent of the total Internet, almost 500 times of what Google can see.

The darknet is a part of the deep web, but there is an important distinction. We access the deep web every day when retrieving our emails, checking bank statements online or logging into Facebook account. However, we cannot enter the darknet through a regular browser. The darknet is accessed using "dot onion" software and not a "dot com" one. Dot com browsers, such as Google Chrome and Mozilla Firefox, cannot access 'onion' websites. The Tor browser is used for this.

Tor is an onion browser that sends the user through an unusual route to access a web page. For instance, if a user wishes to access a website using Tor, the browser will wrap the request through numerous layers, which will keep bouncing off different domains in different countries. The layers of the onion (hence the name) ensures anonymity and makes it almost impossible to trace the user's footprints. This makes the Tor browser and dot onion web pages attractive for those wishing to maintain their secrecy.

Indeed, anonymity does not mean that the darknet is a dangerous place. Individuals, especially journalists, use such avenues to hide themselves from prying eyes of authoritarian states and dictators. Similarly, Tor is used by those who wish to protect their privacy. However, illegal practices can, and do, happen because of the anonymity that is guaranteed by Tor and the darknet.

The darknet has provided criminals, non-state actors and terrorists tools and avenues that are absent in the surface net. For instance, a webpage by the name of "Silk Road" functioned like the Amazon.com for illegal activities, including the sale of drugs, weapons, fake passports and even hitmen. Criminals were comfortable dealing on this platform because of the anonymity in the darknet. The owner and founder of Silk Road, Ross Ulbricht, was caught by the Federal Bureau of Investigation in 2013.

Another attractive market in the darknet is that of hacking tools. IS and its United Cyber Caliphate has conducted several cyber-attacks in the last one year, usually in the form of defacing websites or hacking

Twitter and Facebook accounts. The hacking tools and malware toolkits such as keyloggers and Remote Access Trojans are available in the darknet.

IS is known for its innovations and ability to adapt to changing environments. When law enforcement agencies started snooping around social media, IS migrated to mobile applications WhatsApp and Telegram. They have become attractive modes of communication because of their end-to-end encryption, which prevents any "peeping" by intelligence and law enforcement.

Now, a pro-IS deep web forum user has recommended that the group migrate to Tor and stop using virtual private network services to ensure greater anonymity.

The 9/11 attack was the biggest terrorist attack which changed the complexion of global security. The American leadership and public never expected that an attack of this scale could happen in the homeland. Yet, it did. Today, the attack that defined Osama bin Laden's notorious legacy seems less possible because of all the security measures and precautions that have been taken by countries around the world.

The lack of imagination before was the serious shortfall of security analysts and counter-terrorism specialists who failed to predict or anticipate 9/11. If IS wants to surpass 9/11, it will conduct a cyber-9/11. This is not an impossible task considering the lax cybersecurity measures. The recent hacks of the Democratic National Committee emails and leaks to Wikileaks signify the vulnerability of private information. The DoS attacks by hacking groups such as Anonymous further underline the capacity of non- state actors to inflict damage.

A terrorist organisation that is anonymous and possesses an army of hackers is already becoming a reality. The world is increasingly becoming more connected via the Internet. With or without IS, the next wave of terrorism is most likely to be cyber terrorism. Rather than reacting to an attack in the future, the international community must pre-empt this threat now and take necessary steps.

Ottawa Citizen
Bell Canada hacker sentenced to nearly four years in US prison
Wednesday, 16 November 2016
Byline: Andrew Seymour

Ottawa - An American man who hacked login and password combinations for thousands of Bell Canada customers and then posted the information online has been sentenced to nearly four years in a U.S. prison.
The 45- month sentence handed down in a Chicago courtroom this month to the 22-year- old Tennessee man is in stark contrast to the one received by a 15-year-old Canadian teen who avoided jail after helping to perpetrate that cyber attack and several others on U.S. businesses, universities and government departments between October 2012 and April 2014.

The pair were members of a hacking collective calling themselves NullCrew. The two boasted online that they hacked into the personal information as a "public service" to expose how easily personal information that should have been protected could be accessed. The 22-year-old's identity cannot be published as a result of a publication ban placed on the Canadian teen's court case.

Canadian prosecutors said million of files were exfiltrated during the Bell Canada hack and 300,000 of them contained client information. The U.S. hacker posted about 12,700 logins and passwords and Tweeted a link to the data.

It was only after the Feb. 1, 2014, hack that the RCMP learned from the FBI that an investigation had been underway for more than a year and that the suspects had long since been identified.

The hack was carried out using an undercover FBI server that NullCrew had been given access to through a confidential FBI informant. The American man continued using the undercover server to carry out hacks on a university and two other companies following the Bell hack, all while the FBI watched.

Dominic Lamb, the Ottawa lawyer for the Canadian teen, accused the FBI during a sentencing hearing for his client of putting the public at risk and questioned whether its tactics amounted to entrapment.

After pleading guilty to unlawful use of a computer, the Canadian teen received a conditional discharge and was ordered to perform 100 hours of community service, ordered to stay off Internet cloud storage devices, and to stop hacking.

The teen - who discovered the vulnerability that allowed the hack on Bell - was sentenced under Canada's Youth Criminal Justice Act. Unlike adult sentencing hearings, a judge in a youth court must consider all reasonable alternatives to jail and arrive at a sentence that puts a young offender's rehabilitation first.

The U.S. Attorney's office said the hacks caused at least $792,000 in monetary losses for the victim companies, schools and government agencies, and violated the privacy and security of thousands of innocent people whose usernames, email accounts and passwords were exposed online.

The U.S. man pleaded guilty last year to one count of intentionally damaging a protected computer without authorization.

Toronto Star
Julian Assange now hero of the alt-right
Wednesday, 16 November 2016
Byline: Rosie DiManno
Section: column

Publish and be damned, Julian Assange declared from diplomatic asylum on election day in America. So damn you, Julian Assange.

Darling of the left, Assange has transformed himself into a hero of the alt-right. They've been singing his hosannas since the drip-drip-drip release of hacked emails and internal memos that served to vilify Hillary Clinton and the Democratic Party, most harmfully in the final weeks leading up to Nov. 8.

WikiLeaks, the raw data site of which Assange is founder and executive editor, purports to be a cipher for truth and transparency, ideologically neutral. But the mission has been warped irredeemably, as evidenced by the glee heaped upon its unfiltered disclosures by Team Donald Trump and his coalition of the haters.

In the annals of overt political interference, Assange has forever secured himself a place amongst rogues and reprobates, mutilating citizen activism into partisan pitch-forking, more concerned with influencing the electorate against Clinton than neutral enlightenment.

"I love WikiLeaks," Trump proclaimed at an October rally in Pennsylvania. And why would he not champion this cannon of loose fodder who conservative commentators had earlier demanded be prosecuted for treason? A berserk ally now in the change-lobsters-and-dance Internet wars that fostered demonization of Clinton on social media masquerading as journalism. On the morning after Trump's victory, trending on Twitter was an email allegedly released by WikiLeaks hashtagged #SpiritCooking. While "spirit cooking" apparently refers to performance artist Marina Abramovic's "cookbook" of recipes to promote thoughts and ideas, WikiLeaks tweeted that it involved "blood, sperm and breast-milk," with many on Twitter pouncing on the definition to accuse Clinton of devil worship. That's how kooky this election has been.

Nothing goes out on WikiLeaks without Assange's approval. He has shown his colours.

One of Trump's key "unofficial" advisers, Roger Stone, admitted to NBC News a month ago that he had advance warning about the last tranche of emails through "back-channel communications with WikiLeaks" via an Assange "mutual friend." This is the same Stone who claimed Ted Cruz's father was involved in the Kennedy assassination and said Bernie Sanders should be shot for treason.

While cleaving to the high road of a whistle-blowing Robin Hood, Assange himself made no secret of his anti-secrecy organization's strong tilt against Clinton, making it abundantly clear in a June interview with Britain's ITV network that he hoped to damage the Democratic candidate's chances of winning the presidency.

Australian-born Assange, engaged in a long-running battle with the Obama administration, described the then-pending email splash (Part I) just before the Democratic convention, as "great" stuff, strongly suggested he opposed Clinton's candidacy on policy grounds and, further, viewed her as a personal foe. He accused Clinton, specifically, as being among those who connived to indict him after WikiLeaks spewed out a quarter-million diplomatic cables while she was secretary of state. (Those were the cables leaked by Pvt. Chelsea Manning, then known as Bradley Manning, who is now serving a 35-year sentence for Espionage Act violations.)

But Assange - while not physically setting foot outside the Ecuador Embassy in London where he was granted asylum more than four years ago after breaking the house-arrest conditions attached to an international warrant for alleged sexual assault in Sweden - has travelled a long road from the paragon of virtue he once espoused to be, just as WikiLeaks has strayed far from its founding principles.

The last batch of hackery installments were emails - some 58,000 in all - stolen from the accounts of John Podesta, Clinton's campaign chair. Though the documents disclosed some of the nastiness inside the campaign - only political naïfs would be shocked - and were cringe-inducing in their exposure of fawning by journalists to gain insider access, there was in fact no bombshell as Assange had advertised. Embarrassing and candid, yes, at their worst confirming that Clinton had been lucratively paid for private speeches delivered to banks and other Wall Street institutions. But no malfeasance, no corruption and certainly nothing criminal.

They did feed into Trump's false narratives, however, which many are convinced was Assange's core intent, unloaded without fact-checking, nuance or context to sway voters. What should have boomeranged more damagingly, but didn't, was the likelihood that the material arrived at WikiLeaks courtesy of sinister forces. U.S. authorities have concluded that the digital files were taken by hackers "affiliated and associated with Russian intelligence and security agencies."

That puts Assange and WikiLeaks in collusion with a foreign government to influence the American election. On election eve, Assange felt the need to defend himself, claiming he'd come under "enormous pressure" to stop publishing the Clinton campaign documents.

"Millions of Americans have pored over the leaks and passed on their citations to each other and to us," he wrote. "It is an open model of journalism that gatekeepers are uncomfortable with, but which is perfectly harmonious with the First Amendment." He has denied any links to Russia in obtaining the material but hasn't said where or how WikiLeaks came into possession.

In his jaw-dropping megalomania, Assange has cast himself, instead, as "the gatekeeper." Not one word about Trump on WikiLeaks. Never once has Assange taken ownerships of the site's grievous misdeeds. As U.S.-based scholar Zeynep Tufekci wrote in the New York Times last week, WikiLeaks has "fuelled viral misinformation on social media."

"Data dumps by WikiLeaks have outed rape victims and gay people in Saudi Arabia, private citizen's emails and personal information in Turkey, and the voicemail messages of Democratic National Committee staff members. Mass data releases, like the Podesta emails, conflate things that the public has a right to know with things we have no business knowing."

Ecuador was so concerned by what its government saw as a blatant attempt to impact the election that the embassy shut off Assange's Internet access a month ago. "The Government of Ecuador respects the principle of non-intervention in the internal affairs of other states," it said in an Oct. 18 statement. "It does not interfere in external electoral process, nor does it favour any particular candidate."

A little late and a whole lot short. But the Ecuadorans are palpably sick of the Assange deadlock; probably rue giving him sanctuary at the embassy.

For the past two days, it was an Ecuadoran prosecutor putting questions to Assange at his bolt-hole, queries pre- submitted by Swedish deputy chief prosecutor Ingrid Isgren.

It's been six years since Assange was accused of rape by a woman in Stockholm (a second alleged sexual assault was dropped because of delay deadline.) This is the format Assange demanded. Isgren, according to agreements between the two countries, was permitted to ask for clarification of answers but could not put fresh questions to the accused.

Assange has not been formally charged with any offence and has claimed his innocence throughout. Taking refuge in the embassy was his way of avoiding what he feared would be extradition from Sweden to the U.S. over the WikiLeaks dissemination of classified documents.

It is for the Swedes to decide whether the fugitive should stand trial on the sexual assault charge, should the embassy ever jettison their "guest." But in the world of misinformation manipulation, Julian Assange is manifestly no innocent.

CBC News and Toronto Star

'I don't know that we can help you': RCMP boss 'consumed' with 'inability' to investigate in digital world
Wednesday, 16 November 2016
Byline: Dave Seglins, Robert Cribb and Chelsea Gomez

Ottawa - The RCMP is lobbying the Prime Minister's Office for new powers to bypass digital roadblocks in cases where national security threats and other "high priority" suspects hide online and operate anonymously beyond the reach of police.
"I can safely say that there's criminal activity going on every day that's facilitated by technology that we aren't acting on," RCMP Commissioner Bob Paulson told CBC News and the Toronto Star in an exclusive interview.

The problem is a major focus for Paulson, and one that only gets more urgent as technology advances and suspects find new ways to cover their digital tracks.

"Because of our inability -- and the future inability -- to protect Canadians, both from garden variety criminality and from the national security threat, I see that as really significant," Paulson said. "I'm consumed with trying to make sure that we're able to mitigate the threat."

But privacy advocates and civil liberties groups remain unconvinced that effort requires expanded investigative powers for police.

Canada 'lagging'

On June 23, the RCMP sent Prime Minister Justin Trudeau's national security adviser a briefing note that says Canada lacks strategies and laws to address the technological limitations of police investigations.

The RCMP argues the U.S., Australia, the U.K. and New Zealand -- members of our Five Eyes intelligence alliance - - do much more than Canada to help their police forces deal with high-tech obstacles like encryption, and interception and storage of digital information.

"It's a challenge," Paulson said. "I think we're lagging."

The RCMP briefing note closely mirrors four policy ideas floated in the federal government's green paper on national security, which is open for public consultation.

The RCMP and other police leaders say aside from requests for basic subscriber information, these additional powers would be used only in targeted investigations and would require a warrant from a judge.

Paulson directed his force to provide CBC News and the Toronto Star access to ongoing "high prioirity" investigative case files to demonstrate what police call "going dark" -- the digital barriers to tracking suspects and gathering evidence.

"If you've got a complaint of criminality on the internet, you're going to have to think about where you go with that complaint because I don't know that we can help you," he said. "And that's a terrible thing for a person who's in charge of a police force to say when citizens, when companies, when corporate Canada, or indeed the government comes to us and says, 'Hey, we've been victimized on the internet.'"

Paulson fully expects he'll be criticized by civil libertarians and privacy advocates, but he insists Canadians need to understand the growing digital challenges police face and that our laws need to be updated.

"I think Canadians need to be asked, 'What do you expect the police to be able to do in this digital world? What do you expect?'"

What's unreasonable?

He says privacy is increasingly being understood as a right to complete anonymity online.

"In other words, absolute privacy is everybody's right," he said. "And for me to sit here and say, 'OK, hold on, that's not right,' immediately I get dismissed as someone who doesn't respect privacy.

"That's the space that we need to talk about. What's reasonable, what's unreasonable."

One of Paulson's top priorities may also be the most controversial.

"I've been consistently advocating for a warrantless access to subscriber information. I often get dismissed as, you know, as a troglodyte that doesn't understand people's privacy."

He's adamant Canada must return to a system that allows police easier access to basic phone and internet subscriber information.

In 2014, the Supreme Court ruled in a child pornography case that police had violated the suspect's expectation of online privacy when investigators requested the basic subscriber information (BSI) linked to the IP address he was using. The ruling says absent a reasonable law, the request for the suspect's BSI constituted a search and therefore police should have first obtained a warrant.

Before the ruling, police didn't hesitate to request BSI directly from telecom companies. In fact, the federal privacy commissioner released data that showed law enforcement made nearly 1.2 million such requests in 2013 alone.

Police now must apply for a warrant every time they want to look up a user's BSI. They say it takes time and paperwork, and when police are at the beginning of an investigation and want to look up an IP address, they don't always have sufficient grounds to obtain a warrant.

Paulson says the system causes delays and occasionally forces police to abandon investigations. He says the public and policy-makers don't fully understand the consequences of the ruling.

"We can query licence plates and get the subscriber of a car on the basis of the fact that the police are engaged in enforcement of the Traffic Act or another criminal investigation. We keep records of all that and we're accountable for that," he said. "I don't think it's unreasonable."

Paulson and many other police leaders across the country are hoping the Liberal government will draft a new "reasonable law" to create a system of "administrative access" to BSI that could be overseen by senior police or prosecutors -- not the courts.

'Not a trivial ask'

But critics say police must first provide far greater evidence that investigations are being abandoned.

They also say basic subscriber information can actually be extremely revealing.

"When it is connected to an IP address, [BSI] reveals an incredible amount of information about the things that you do online," said Brenda McPhail, director of the Privacy and Technology Surveillance Project at the Canadian Civil Liberties Association.

McPhail says with a simple IP address police can discover a user's identity, where they live and build a profile based on online activity.

"Let's face it, we live half of our lives online these days, so it is not a trivial ask."

Christopher Parsons, a technology and privacy researcher with the Citizen Lab at the University of Toronto's Munk School of Global Affairs, says any new law must protect against abuses.

"The solution is not to say, 'It's very hard for police, just trust us and let us sign off on our own warrants.' Turning to other jurisdictions such as the U.S., we know it doesn't work. We know that police will over-exercise that power."

Paulson has mixed views on the other policy proposals discussed in the government's green paper.

For example, he disagrees with the Canadian Association of Chiefs of Police that courts should be able to order suspects to hand over their passwords and/or encryption codes.

He says he struggles with the idea of compelling suspects to potentially incriminate themselves.

"It's fraught," he said. "I don't see a state where the police are ordering people to give up information. It would be like ordering a statement. That's at odds with how I understand what we do. I don't see that happening."

But the commissioner does support proposals to require communications providers to build intercept and data-retention capabilities into their networks

He insists access to a suspect's private data or communications would require a warrant authorized by the courts.

"We are not at all interested in surveilling citizens, except to the extent that we can demonstrate to others that they're engaged in criminal activity that threatens Canadians."

Paulson says public debate on these issues is urgently needed because police are increasingly hitting digital dead ends in terrorism and child exploitation investigations.

"I feel responsible for the safety and security of Canadians in the face of this challenge."

Toronto Star and CBC News
Mounties lobbying for more power
Wednesday, 16 November 2016
Byline: Robert Cribb and CBC staff

Ottawa - The RCMP is lobbying Prime Minister Justin Trudeau for more powers - including access to digital information without warrants - to investigate suspects who are hiding behind uncrackable encryption on their digital devices, a Toronto Star/CBC investigation has found.
"I can safely say that there's criminal activity going on every day that's facilitated by technology that we aren't acting on," RCMP Commissioner Bob Paulson told the Toronto Star and CBC in an exclusive interview. "We're losing our ability, if we haven't lost it entirely, to bring the traditional investigative response to technologically facilitated crime because of the misunderstanding, in my view, of the privacy threat."

The RCMP has reached a point, Paulson said, that Canadians should "think about where you go with that complaint because I don't know that we can help you."

"And that's a terrible thing for a person who's in charge of a police force to say when citizens, when companies, when corporate Canada, or indeed when the government comes to us and says, 'Hey, we've been victimized on the Internet.'"

An RCMP briefing document sent June 23 to Trudeau's national security adviser compares Canadian law enforcement's digital investigative capabilities with four western countries - and Canada stands alone.

The country lacks police powers in six categories, including legal remedies for cracking encryption, intercepting communications and accessing suspects' identities.

The other countries - Australia, the U.K., the U.S. and New Zealand - are, with Canada, members of the Five Eyes intelligence alliance.

"When we come up against impediments to getting evidence ... that's demoralizing," Paulson said.

The Star/CBC investigation comes as the federal government is engaging in public consultation on Canada's anti- terror act, including a problem police call "going dark" - the gradual disappearance of evidence behind digital brick walls.

It's a deeply polarized debate.

Police are calling for laws that would force suspects to provide access to their encrypted devices and compel telecommunications companies to create interception and data retention capabilities to assist investigations.

Privacy advocates call these demands an "evidence-free" infringement of basic privacy rights.

"If we plan every law around a hypothetical ticking time bomb, it will be used in a lot of non-time-bomb scenarios," says Christopher Parsons, a technology and privacy researcher at the Citizen Lab at the University of Toronto.

"We know powers that are passed, often under the auspices of terror or something of that nature, are immediately used for potentially serious but far less serious crimes."

The most controversial item on Paulson's wish list would allow police to collect basic subscriber information - such as names and addresses - from telecommunications companies without having to go to court for a warrant.

Police view such searches as a basic investigative tool - the first step in launching investigations into suspected terrorists, pedophiles or organized crime figures.

"I'd like to see the ability of the police to call an Internet Service Provider or communications provider ... and get the basic subscriber information," he said.

Paulson concedes that such requests are dismissed by privacy advocates who cast him as a "troglodyte who doesn't understand people's privacy."

Paulson's argument for warrantless access to basic subscriber information has already been heard - and rejected. A 2014 Supreme Court ruling found Canadians have a reasonable expectation of online privacy in basic information, such as names, addresses and IP addresses.

In the absence of a law to the contrary, the ruling concludes, police should have to obtain a warrant.

Police, who were previously able to get the information almost immediately, call that ruling a game-changer. Many officers say obtaining a warrant is a bureaucratic process that is so time- consuming it can undermine investigations.

"I don't think the consequences of that decision on policing and security (are) completely understood," Paulson said. "The consequences are delayed, and sometimes, abandoned investigative efforts because we haven't been able to meet a threshold."

He points to what happens when police run licence plate numbers and get the owner's name and address. Police want the same kind of ease searching ISP records.

"We keep records of all that and we're accountable for that. I don't think it's unreasonable."

Privacy advocates reject the comparison.

"Basic subscriber information, which is connected to an IP address, reveals an incredible amount of information about the things that you do online," said Brenda McPhail, director of the Privacy and Technology Surveillance Project at the Canadian Civil Liberties Association.

"It is not a trivial ask to say we just want warrantless access without any sort of supervision to this information, which we have already shown in court to be sensitive and personal."

Any powers handed to police come with the risk of abuse, said Citizen Lab's Parsons.

"The solution is not to say, 'It's very hard for police, just trust us and let us sign off on our own warrants,'" he said. "We know that police will over-exercise that power."

In recent weeks, two cases of law enforcement overreaching their powers made scandalous headlines.

Two weeks ago, a Federal Court judge denounced the Canadian Security Intelligence Service's monitoring and retention of information on thousands of Canadians' and, in Quebec, police forces admitted to intercepting and tracking cellphones belonging to at least 10 journalists.

"I can't sit here and say that it's going to be a perfect," Paulson said.

But when abuses occur, those responsible are held accountable, he said.

"Canadians can be persuaded that there is a reasonable, reliable administrative oversight mechanism, that it can be seen externally."

Paulson is more cautious than many of his policing colleagues on the idea of compelling suspects to open up their phones or computers for police review - a proposal tabled by the Canadian Association of Chiefs of Police.

"It's fraught," he said. "I'm not a lawyer, but I do know the dangers of conscripted evidence ... Given the current state of concerns and misunderstanding around privacy, I think we're likely not to win too many arguments there."

Yesterday, the Star and the CBC, which were given unprecedented access, reported the details of investigations that the RCMP say have been stonewalled by encrypted devices. Those disclosures and Paulson's interview are part of the force's attempt to get its message to Canadians about what he calls a high-stakes debate.

"I feel I need to be educating folks to a fair understanding of what the challenge is," Paulson said. "But more importantly, I feel responsible for the safety and security of Canadians in the face of this challenge."

Toronto Star
Spy agency kept court in the dark about data
Wednesday, 16 November 2016
Byline: Alex Boutilier

Ottawa - Canada's electronic spies were asked to brief the Federal Court on their intelligence-gathering activities, the Star has learned.
But the Communications Security Establishment (CSE) declined to meet with federal judges earlier this year, saying an ongoing constitutional challenge prevented them from doing so.

The request came from the same judge that found CSE's partner agency, the Canadian Security Intelligence Service (CSIS), illegally kept information on innocent people for almost a decade.

In a strongly worded ruling released this month, Justice Simon Noël found CSIS kept the court in the dark about a program to retain and analyze data about innocent people between 2006 and 2016.

The ruling gave an unprecedented look at CSIS's Operational Data Analysis Centre, which for years had been storing data about "non-threat" individuals. While the information was intercepted legally, the court ruled it was illegal for CSIS to keep and analyze it indefinitely.

The ruling came out of a briefing on the program by Noël for judges who approve CSIS warrants. In documents obtained by the Star, CSE chief Greta Bossenmaier was told that Noël requested a general educational briefing from her agency around the same time.

But because of a constitutional challenge launched by the B.C. Civil Liberties Association (BCCLA) against CSE's intelligence activities, currently before the court, the agency declined Noël's invitation.

"A briefing to the Federal Court could have reasonably led to the perception from the public and the BCCLA that CSE may be attempting to influence the (court's) judgment or opinion as it related to this ongoing case," Lauri Sullivan, a spokesperson for the agency, said an email to the Star.

"It is important to note that CSE has provided briefings to Federal Court designated judges in the past, and would consider doing so again in the future (provided any conflict concerns are addressed as they relate to the ongoing BCCLA case)."

That case, launched in 2013 after U.S. whistleblower Edward Snowden's disclosures about mass surveillance programs, challenged CSE's bulk collection of metadata - commonly described as "data about data," such as mobile phone numbers, IP addresses, duration and locations of phone calls and unique identifiers of mobile devices.

The BCCLA contends the very nature of bulk collection puts Canadians' privacy rights at risk, according to the advocacy group's policy director Micheal Vonn. The case is proceeding behind closed doors, while a judge determines how much information about CSE's methods and techniques can be made public. But Vonn expects that process to wrap up this year, meaning public arguments could be heard in early 2017.

A spokesperson for the Federal Court, Andrew Baumberg, said Justice Noël's request to CSE was for a general educational briefing about their operations. Baumberg said there are no plans for future briefings, whether general in nature or specifically related to metadata collection.

The Star requested comment from Defence Minister Harjit Sajjan, the minister responsible for CSE, including whether he had any concerns about the agency declining to brief the judges, or any indication CSE data could have ended up in CSIS's illegal database.

In an email, a spokesperson for Sajjan said the minister is in regular communication with Bossenmaier about the agency's operations.

"The minister has regular conversations with the CSE chief and stays informed of CSE activities through these discussions, as well as through departmental briefings, and updates from the CSE Commissioner," wrote Jordan Owens.

"I am sure you understand that CSE can't get into specifics on operations, including data sharing. However, CSE's mandate allows for information sharing with Government of Canada partners under (those partners') lawful authority."

Motherboard
The RCMP Is Using the Media to 'Create Moral Panic' About Encryption
Wednesday, 16 November 2016
Byline: Jordan Pearson

The Royal Canadian Mounted Police has turned to two of the country's top media outlets to make their case for new surveillance capabilities in what critics say is a PR play orchestrated to sow public worry about privacy-boosting technology.
Police in Canada have long pushed for broadened surveillance powers that would force people to unlock their phones, for example, or force telecommunication companies to provide real- time access to subscriber information. No such laws currently exist, but to show why the police believe they need them to do their jobs, the country's federal force worked with two of Canada's most respected media entities.

The RCMP gave the CBC's David Seglins and the Toronto Star's Robert Cribb security clearance to review the details of 10 "high priority" investigations--some of which are ongoing--that show how the police is running into investigative roadblocks on everything from locked devices to encrypted chat rooms to long waits for information. The Toronto Star's headline describes the documents as "top-secret RCMP files."

The information sharing was stage-managed, however. Instead of handing over case files directly to the journalists, the federal police provided vetted "detailed written case summaries," according to a statement from Seglins and Cribb. These summaries "[formed] the basis of our reporting," they said. The journalists were given additional information on background, and allowed to ask questions, according to the statement, but "many details were withheld."

The stories extensively quote RCMP officials, but also include comment from privacy experts who are critical of the police agency's approach.

"On the one hand, the [RCMP] do have a serious problem," said Jeffrey Dvorkin, former vice president of news for NPR and director of the University of Toronto Scarborough's journalism program. "But to give information in this way to two respected media organizations does two things: it uses the media to create moral panic, and it makes the media look like police agents."

"It would have been better if the RCMP launched its own PR campaign to get the public to understand that they're in a difficult position," Dvorkin continued.

When asked if the Star and the CBC had any say in which cases they reviewed, Seglins and Cribb wrote that they did request details on a "handful of individual cases of interest," they said, and police complied "in some cases," denying access to one file because of sensitivities surrounding an ongoing investigation.

In the CBC and Star reports, RCMP officials repeatedly refer to the problem of "going dark," a term that law enforcement frequently uses to describe their supposed difficulties in solving cases due to the use of encryption technology. A green paper prepared by the government in the lead-up to an ongoing national security consultation also notes that police have identified encryption as a roadblock. Critics say the consultation and green paper risk broadening Canadian police's already-expanded powers.

A joint investigation by Motherboard and VICE News earlier this year revealed that the RCMP possessed a key that allowed them to decrypt communications on all consumer BlackBerry devices. The RCMP also has the ability to "crack" the encryption on certain phones, reports have shown.

Critics of police attempts to undercut encryption technology via the law note that ordinary people--journalists, protesters, and professors--also use encryption, and banning it would hurt them too, not just criminals.

"This is obviously part of a concerted PR attempt on the part of the RCMP in particular, which has been ongoing for some time," said privacy lawyer David Fraser. "The wording in these articles is mostly the police's version of things, and we need a reality check."

"If ordinary Canadians don't have access to technology to protect their privacy," Fraser said, "bad guys would be able to very easily, online, get the same tools that they're using today to encrypt their communications. Overall, we would be no safer, and in fact less safe."

The CBC and the Toronto Star's story is part one of a five-part series on the debate over privacy and police powers in Canada, with a second installment to come on Wednesday.

Xinhua News Agency
President Xi stresses int'l cooperation in cyberspace governance
Wednesday, 16 November 2016
Byline: Staff reporter

Beijing - Chinese President Xi Jinping on Wednesday called for increased international cooperation in cyberspace governance and the building of a cyberspace community of common destiny.
Noting that Internet development has no boundaries, Xi said China is willing to work with the international community for the common welfare for all people, to uphold the concept of cyberspace sovereignty and to make the global cyberspace governance system fairer and more reasonable.

Xi made the remarks while giving a speech via video at the opening ceremony of the third World Internet Conference (WIC) in the riverside town of Wuzhen, east China's Zhejiang Province.

Liu Yunshan, a member of the Standing Committee of the Political Bureau of the Communist Party of China (CPC) Central Committee, attended the opening ceremony of the WIC and delivered a speech.

The Internet is changing the global economic and security situation, so that building a cyberspace community of common destiny is a pressing demand in an information-led world, Liu said.

China is willing to strengthen policy coordination and cooperation with other countries, Liu said, calling for the improving of cyberspace governance rules, respecting cyberspace sovereignty and safeguarding all countries' equal rights in developing, joining and governing cyberspace.

Liu also called for the building of a multilateral and transparent global Internet governance system, cooperation in Internet innovation, and network popularization, in a bid to make the Internet benefit all peoples of the world.

Cooperation should be strengthened in coping with cyberspace security challenges, in a bid to safeguard state security, public interests and citizens' legitimate rights, according to Liu.

Themed "Innovation-driven Internet Development for the Benefit of All -- Building a Community of Common Future in Cyberspace," the third WIC runs from Wednesday to Friday.

Over 1,600 Internet entrepreneurs, opinion leaders, experts, officials and heads from over 110 countries and regions as well as international organizations attended.

South China Morning Post
Beijing wants to have it both ways with internet
Wednesday, 16 November 2016
Byline: Jane Cai and Mandy Zuo

Beijing - Liu Yunshan, the No 5 in the Politburo Standing Committee and in charge of ideological control, doesn't look like a man who can influence the future of the internet.
Yet the 69-year-old senior cadre will be the keynote speaker at the third World Internet Conference, an event organised by the Chinese government.

He will instruct leading figures in China's internet industry and guests from dozens of developing countries on how to build "a -community of common future in cyberspace".

At last year's conference, President Xi Jinping voiced the idea of "cyberspace sovereignty", an unambiguous announcement that Beijing would step up its -censorship and control of the internet.

The Communist Party is trying to match its social control in the real world in the virtual world.

The country has a huge online police team patrolling the internet and is enhancing the "Great Firewall" as a border control line to keep foreign websites such as Google and Twitter out.

But the internet is also a booming business and a way of life in China, a country of 1.3 billion -people.

Literally everyone is now connected via their phones, and online shopping, cashless payment, mobile taxi-hailing and virtual entertainment services in Beijing and Shanghai are as widespread and sophisticated as in New York and Tokyo.

It is against this backdrop that Communist Party leaders hope to allow a booming business-wise internet while maintaining rigid ideological control.

"China will continue to pursue a leadership role in global cyberspace governance," Zhang Lifan, a Beijing-based historian, said.

"But China is unlikely to achieve concrete results, since most developed countries are shunning the internet conference. Those with underdeveloped internet infrastructure are more interested in the economic benefits, rather than internet control."

Most overseas guests will be from developing countries, from Cambodia in Asia to Comores in Africa. There will be a conspicuous absence of speakers from big-name global internet firms like Google, Apple or Twitter.

This year's conference starts today in Wuzhen, Zhejiang (??) province. It has sessions on cybersecurity, smart health care and China's "One Belt, One Road" infrastructure scheme.

China has been trying in the past few years to strike a deal with conference participants on "cyber governance". Such an agreement would give international recognition to the way Beijing manages the internet, but observers are not optimistic that such common ground can be found.

Huang Chengqing, vice-chairman of the Internet Society of China, said it was unlikely Beijing could achieve any kind of agreement with participating countries during the summit.

"It's an issue of seeking balance for each country. Different countries have different understandings on what is harmful information, as they have different religions and values, or are at a different phase of growth."

Mother Jones Magazine

NSA Chief: WikiLeaks Hacks of Democrats' Emails Were a "Conscious Effort by a Nation-State"
Wednesday, 16 November 2016
Byline: Kanyakrit Vongkiatkajorn

New York - The WikiLeaks release of internal emails from the Democratic National Committee and the Hillary Clinton campaign constituted a "conscious effort by a nation-state to attempt to achieve a specific effect," the head of the National Security Agency said Tuesday.
"There shouldn't be any doubt in anybody's mind," NSA Director Michael S. Rogers said in an interview with the Wall Street Journal on Tuesday. "This was not something that was done casually, this was not something that was done by chance. This was not a target that was selected purely arbitrarily." Rogers acknowledged in October that Russians were behind the hacks.

News that the DNC had been compromised broke earlier this June, when hacker Guccifer 2.0 released a trove of documents containing campaign emails and memos--most notably emails implying that the committee favored Clinton over Sen. Bernie Sanders during the Democratic primary. The release of the emails led to the resignation of DNC chair Debbie Wasserman-Schultz.

WikiLeaks also published thousands of emails from John Podesta, Clinton's campaign chair. Though Russia was long suspected of being behind the hacks, US officials did not formally accuse the Russian government of orchestrating the cyber attacks until October. In November, just four days before the election, DNC officials told Mother Jones they had found evidence that the DNC headquarters may have been bugged and had submitted a report to the FBI.

London Daily Telegraph
Teenage hacker in data breach at TalkTalk was 'just showing off '
Wednesday, 16 November 2016
Byline: Lydia Willgress

London - The head of the telecoms giant TalkTalk fell victim to blackmail by cyber criminals after a teenage boy hacked into its website then boasted about it online, a court has heard.
The boy, aged 17, who cannot be named for legal reasons, used hacking software to identify TalkTalk's vulnerabilities. He then posted the details online, which resulted in the website being targeted more than 14,000 times, Norwich Youth Court was told.

The teenager, who also targeted data held by Manchester University and Oxford University, admitted seven hacking offences and told magistrates: "I didn't really think of the consequences at the time. I was just showing off to my mates."

TalkTalk eventually fell victim to a "significant and sustained" attack in which the personal data of nearly 160,000 people was compromised. It was branded a "car crash" earlier this year by the then information commissioner Christopher Graham.

The TalkTalk attack prompted an investigation by the Metropolitan Police Cyber Crime Unit and the teenager was arrested in Norwich on Nov 3 2015 and charged with breaching the Computer Misuse Act 1990.

Laura Tams, prosecuting, said he used a "legitimate software" program, SQL map, which is a tool to identify vulnerable web security. But it should only be used if the website consents.

Ms Tams said that in the days before the TalkTalk hack, the youth had gained access to data on 693 staff and students at Manchester University, gleaning details which a "more capable hacker would be able to use for wider criminality".

He then attacked a library website for Cambridge University.

She said the boy had claimed in an online conversation that he "could potentially have everyone on TalkTalk" and then mentioned "wiping and nuking his digital devices".

Chris Brown, in mitigation, reminded the court that it was not the prosecution's case that what happened at TalkTalk "lies solely at the teenager's door". But that a third party took advantage of the situation.

"That's someone acting completely apart from him [the teenager]. That person used the vulnerability in TalkTalk days later to demand things and emailed the chief executive with blackmail efforts," Mr Brown said.

"You're dealing with someone who at the time was just 16 years old, who created a number of personas online," said Mr Brown. "Personas that talked about his abilities as a hacker."

"The thrill was in the chase," Mr Brown added. "It was not in damaging their website or causing loss to them. It was playing."

Sentencing was adjourned to Dec 13, but the chairman of the bench, Jean Bonnick, said magistrates may be minded to spare the teenager jail.

Le Figaro
Mégafichier : Cazeneuve sur le gril au Sénat
Wednesday, 16 November 2016
Byline: Jean-Marc Leclerc

Paris - Après l'audition du ministre de l'Intérieur, la Haute Assemblée craint que Beauvau ne recule sans apporter les garanties espérées.

Sécurité Bernard Cazeneuve connaîtra-t-il, avec la polémique sur le mégafichier national d'identité, la même déconvenue que Michèle Alliot- Marie avec le défunt fichier de renseignement Edwige ? Une chose est certaine : le Sénat ne veut pas être complice de ce qui se trame au ministère de l'Intérieur dans ce dossier. Rappelons que le fichier sur le point de naître doit réunir dans une seule et même base informatique les données d'identité (nom, couleur des yeux, domicile, photo, empreintes digitales...) de près de 60 millions de Français. Cela ne mérite-t-il pas un minimum de concertation ?

Mardi matin, à l'issu de l'audition du ministre de toutes les polices devant la commission des lois devant la Haute Assemblée, le président Les Républicains de cette instance, Philippe Bas, a tenu à rappeler qu'il fut le premier à réclamer des éclaircissements au gouvernement sur le texte qui fait aujourd'hui scandale.

Par un courrier en date du 18 octobre, le sénateur de la Manche a en effet demandé à l'hôte de Beauvau de lui communiquer « le projet de décret créant un fichier centralisé des données personnelles recueillies pour la délivrance des passeports et des cartes d'identité » . Il souhaitait, écrivait-il, « rassurer (les) collègues » qui l'avaient alerté sur les intentions du gouvernement.

Le 27 octobre, le ministre lui a répondu que toutes les garanties avaient été prises ; il a signé son décret le lendemain, pour une publication du texte le 30, un dimanche, en pleines vacances de la Toussaint. Avec le résultat que l'on sait : conflit ouvert avec Axelle Lemaire, secrétaire d'État au Numérique, qui a aussitôt dénoncé un décret « pris en douce par le ministère de l'Intérieur » et un « dysfonctionnement majeur » ; vive protestation dans la société civile également, sur les réseaux sociaux, avec recours annoncé devant le Conseil d'État, selon l'association La Quadrature du Net.

Ce n'est pas tout : la Commission nationale de l'informatique et des libertés (CNIL) rappelle qu'elle avait conseillé au gouvernement un débat préalable au Parlement. Même le Conseil national du numérique, organisme indépendant dont les membres sont nommés par le chef de l'État en personne, a appelé à « suspendre » le fichier controversé.

Voici donc Bernard Cazeneuve contraint de « rétropédaler » , ce mardi, devant les sénateurs. « J'en conviens » , un débat « n'a pas eu lieu en amont (...) dès lors qu'il est souhaité, nous l'organisons » , a-t-il déclaré. « Nous pensons bien faire » , nous « prenons toutes les précautions » pour garantir les libertés, a-t-il réitéré. « Nous n'avons rien à redouter » et « sollicitons nous-mêmes le débat » public. En guise de « débat » , le ministre a tenu à expliquer, ce mardi à l'Assemblée nationale, que son fichier serait bien sécurisé pour empêcher tout piratage.

D'autres concessions, sachant que, sur le fond, il ne retire pas son texte ? Il a, en tout cas, affirmé que les Français « pourront s'opposer » au « transfert numérique de leurs empreintes » digitales « dans la base » de ce fichier, comme il l'avait déjà indiqué vendredi. Cohabiteront donc un grand fichier numérique et un autre, manuel, à l'ancienne.

Et c'est là que là que le bât blesse. « Une fois de plus, comme avec la loi El Khomri, le gouvernement avance et recule, en dénaturant l'essence même d'un projet qui avait pourtant un intérêt, puisqu'il s'agit de lutter en priorité contre le fléau des usurpations d'identités , regrette Philippe Bas. Si vous permettez aux gens de refuser que leur photo ou leurs empreintes digitales y figurent, ce fichier sera incomplet » , a-t-il réagi.

« Pourquoi s'accrocher dès lors à un dispositif bancal ? » , interrogent en substance nombre de sénateurs. « Il aurait fallu uniquement répondre sur le terrain des garanties et des contrôles » , estime le patron de la commission des lois du Sénat. En pleine campagne présidentielle, l'affaire du mégafichier relève de l'exercice de haut vol pour Bernard Cazeneuve.

Les Echos
Des téléphones Android espions ?
Wednesday, 16 November 2016
Byline: Frédéric Schaeffer

Non identifié - La société de sécurité informatique Kriptowire a repéré qu'un logiciel préinstallé dans certains téléphones tournant sous Android surveillait secrètement les utilisateurs.
Vous être l'heureux propriétaire d'un smartphone tournant sous Android acheté pas trop cher ? Vos SMS, vos contacts, la liste de vos appels téléphoniques ou encore vos données de déplacement sont peut-être en train d'être analysés à Pékin. La société de sécurité informatique Kriptowire a, en effet, repéré qu'un logiciel préinstallé dans certaines téléphones tournant avec le système d'exploitation de Google. Il surveillait secrètement les utilisateurs et envoyait même l'intégralité des textos et autres données sur un serveur basé en Chine. Et ce, au rythme de toutes les 72 heures !

Les téléphones prépayés et bas de gamme seraient les plus vulnérables mais le nombre de produits concernés reste encore flou, indique le New York Times qui révèle l'information. Le logiciel mis en cause a été créé par la société chinoise Shanghai Adups Technology, qui prétend être présent sur plus de 700 millions de téléphones, voitures et autres appareils connectés. Cette société a des partenariats avec de grands constructeurs chinois comme Huwei et ZTE. Au moins une société américaine, Blu Products, serait concernée, avec 120.000 terminaux équipés du logiciel mais une mise à jour aurait rapidement permis d'éliminer la fonctionnalité en cause, précise le groupe.

Exploitation de données secrètes à des fins publicitaires ou un effort des autorités de Pékin pour recueillir des renseignements ? Les autorités américaines hésitent encore, indique le quotidien américain. « Ce n'est pas une vulnérabilité, c'est une fonctionnalité », insiste la société de sécurité informatique Kryptowire interrogé par le site Theverge.com. Adups a déclaré que le logiciel n'était pas destiné aux téléphones américains mais à aider un fabricant chinois désireux d'analyser les comportements de ses clients.

La fonctionnalité d'envoi des SMS et aux données en Chine aurait été appliqué par inadvertance sur les appareils Blu Products. Un porte- parole de Google a déclaré que la société n'était pas au courant de la question jusqu'à ce qu'il ait été contacté par Kryptowire. La liste des téléphones concernés n'ayant pas été publiée par Adups, il est bien difficile de savoir quels sont les clients concernés.

BDNews24
Internet freedom 'declined' in Bangladesh in one year (Canada).
Wednesday, 16 November 2016
Byline: News Desk

Dhaka - Bangladesh has gone backward in achieving internet freedom in past one year, according to US-based observer and analyst Freedom House.
It has put Bangladesh under 'Partly Free' category among 65 countries reviewed in its Freedom on Net 2016 report.

The report, published on Monday, says Bangladesh scored 56 out of 100, up four points from last year. This means the opportunity to use the internet freely has narrowed by four points in one year.

Estonia and Iceland are the most free countries in the use of the internet, scoring only six points, the report said.

China is at the bottom of the list with 88 points while Canada, US, Germany, Australia, Japan, UK, France, and Georgia are among the top 10.

Among Bangladesh's neighbours, India and Sri Lanka are ahead in the report with 41 and 44 points respectively. Myanmar and Pakistan have scored 61 and 69 points respectively.

In the Bangladesh chapter, Freedom House mentioned the murders of LGBTI activist Xulhaz Mannan, Faisal Arefin Dipan, a publisher of books authored by slain blogger Avijit Roy, and the murder of blogger Niladri Chattopadhyay Niloy, as a reason behind the country's 'bad performance'.

It also mentioned the arrest of journalist Probir Sikdar under the ICT Act for publishing a comment about a minister on his Facebook page and the blocking of social networking sites for an hour in November last year in its report. It has changed Bangladesh's Press Freedom Status from 'Partly Free' to 'Not Free'.

Indo-Asian News Service
New York consulate latest of Indian diplomatic web sites hit by hacker
Wednesday, 16 November 2016

New York - The Indian consulate's website is the latest Indian diplomatic websites to be hacked by a person claiming to be a 17-year-old student in Tokyo who asserts that it was a well-intentioned attempt to show the vulnerabilities that "even kids could exploit".
The person, using the identity Kapustkiy, who had earlier hacked the web sites of seven Indian diplomatic missions in Europe and Asia, posted on a public web site the partial personal information of 418 people registered with the consulate said to be taken by penetrating its website.

Last week web sites of Indian diplomatic missions in South Africa, Libya, Malawi, Mali, Italy, Switzerland and Romania were hacked and non-public information were posted publicly.

In an interview over Twitter on Monday, Kapustkiy said: "It took me only three seconds to gain access to their database."

"Even the kids could exploit it," he said of the vulnerabilities in the way the programing language, SQL or Structured Query Language, was used on the web sites. SQL is used by web sites to manage databases.

His method was different from the hacking of Indian defence, business and media sites exposed last year by a Silicon Valley cybersecurity firm, FireEye, which said it was likely by China.

Those penetrations required more elaborate efforts like planting spying software in emails sent to people using those sites. But Kapustkiy's methods appeared to be simpler and more direct, exposing more dangerous vulnerabilities.

The list said to be from the New York consulate was posted on a website, pastebin.com, which is open for public posting of information. The list was still on the site Monday night, even though the earlier postings from other Indian missions have been removed.

The consulate did not respond as of Monday night, New York time, to a request emailed to the press section for comments.

The web site says that it is powered by Ardhas Technology India Private Limited, which has its registered office in Erode, Tamil Nadu. A request to it for comment had not received a response by Monday night.
Kapustkiy said: "I don't describe myself as a hacker or something, but as a security pentester."

Pentester is short for penetration testers who examine the weaknesses of internet sites to intrusions.
On his Twitter account he also describes himself as a "cyber detective".

The hack did not affect functioning of the consulate's website while the non-public data was being extracted from it. "I didn't want to do any damage, but [only] to let administrators to pay attention [to the vulnerabilities]," Kapustkiy said.

"I could've leaked around 7,500 entries of people," he said. "But I decided to leak only 400 entries which belong to the employees and not to the people. I could also leak there real address and zip code. But I didn't do that."

However, the partial list seen by IANS appeared to be information about people who had registered with the consulate rather than employees.

Kapustkiy said that he first reported the problems to the web site administrators but didn't get a response. "After all the media attention I gain they started to fix it," he added. He said that Indian officials have not contacted him.

Around 20 domains connected to the Indian missions were hacked in the past and although they have been patched, he said, "there were still some domains that were vulnerable to exploit. You could find the vulnerability in three secs".

About his future plans, he said, "I think that I will continue look at vulnerables in important websites in Asia." Asked about his nationality, he said, "I don't want to tell where I'm from, but most media are claiming that I'm from the Netherlands.

Times of Israel
Using AI, Israel's Aperio protects infrastructure from hackers
Wednesday, 16 November 2016
Byline: Shoshanna Solomon

Jerusalem - Israel's APERIO Systems said it has developed the cyber industry's first technology that identifies, sends out alerts and takes real time corrective action when hackers try to artificially manipulate data to damage critical infrastructures, such as electricity grids or water supply networks. "For real impact hackers need to create a dangerous state in which operators of the critical systems get messages that all systems are functioning well whereas they are actually being damaged or destroyed," said Michael Shalyt, APERIO's VP Product. "Data forging is when you give the impression that things are working as they should, but they are actually not."

Shalyt, a 29-year old former researcher and team leader in an elite IDF intelligence unit, brings as an example an unfolding bank robbery in which video feed to the guard is hijacked to transmit not a real-time feed but that of the previous day, showing that everything is fine.

The Stuxnet malicious worm that sabotaged Iran's nuclear program "was operating for 18 months and the control room felt all was well, but it was all fake," Shalyt said. "This kind of forgery can cause lasting physical damage because if a turbine, for example, is rendered dysfunctional without an operator being aware of the fact it could be months before the damage is repaired and the system is up and running again."

"Many companies are trying to achieve our same goal, but our approach is different. We are a different breed of cyber company," said Shalyt, who previously led the malware research team at Check Point Software Ltd. "We are a lie detector for machines."

And this is the niche -- data forgery protection -- in which APERIO operates, with its team of former Israeli army intelligence veterans, electronic engineers, physicists and signal processing experts.

APERIO said it secured seed funding from a consortium of private investors, including cybersecurity veterans Doron Bergerbest-Eilon, Liran Tancman, and Shlomi Boutnaru. Bergerbest-Eilon helped establish the agency charged with protecting all critical infrastructures in Israel and is the former director of the security and protection division of the Shin Bet security agency. Tancman and Boutnaru, who played key roles in building Israel's cybersecurity capabilities, founded predictive cybersecurity startup CyActive, which was acquired by PayPal in 2015.

APERIO, founded in January this year, targets its new product, which is actually a server, to industrial control systems (ICS) of anything from the temperature of turbines in a power plant to pharmaceutical or food manufacturing plants and gas flow at a petroleum refinery.

Through the use of algorithms, APERIO's technology scours the systems and alerts users to forgeries by monitoring the machinery and seeking inconsistencies in physical realities compared to their historical performance. Any mismatches generate an alert and APERIO Systems pinpoints the attacked equipment and faked process data.

Then, using a sophisticated combination of physics and state-of-the-art machine learning techniques, APERIO Systems reconstructs the real values of the forged operational data and reverts it to its original state in real time -- establishing operational resilience.

"A fan, when operating, tends to emit a high pitch when it rotates fast. The noise is a side effect of the fan's operation," he said. "But if suddenly I notice that the fan is operating but is not emitting a noise, then that is strange. We learn the physical models and what they should be. Then we look for inconsistencies, based on past experiences."

The company uses several methods for verification, all of which are based on physical signs. "It all has to make sense," Shalyt said.

APERIO's servers are already being used by several big gas pipelines across Israel, said Yevgeni Nogin, the CEO of APERIO. The company recently won a cybersecurity competition run by Italy's Enel, a multinational energy producer and Europe's largest utility by market cap, and will be deploying its servers at their plants.

The huge expansion of computer inteconnecitvity and the global dependence on data has increased the risks and severity of cyberattacks, spurring a need for more efficient and effective defensive measures.The cybersecurity market will likely grow at an annual rate of almost 11 percent to to $202 billion by 2021 from $122 billion in 2016, according to MarketsandMarkets, a research company.

Nogin, 28, is a graduate of the elite Talpiot IDF military academy who served over nine years in elite intelligence and R&D units of the IDF. "We are targeting our product to any controlled systems, whether they are cars, airplanes and services that are critical in our everyday life," Nogin said.

Jerusalem Post
Did Uri Ariel pass sensitive security technology to Russia?
Wednesday, 16 November 2016
Byline: Yossi Melman

Jerusalem - The Israeli government is embarrassed and fears that a unilateral decision by Agriculture Minister Uri Ariel to transfer sensitive technology with US-made components to Russia could damage security ties with the US and Spain.
Russian Prime Minister Dmitry Medvedev visited Israel last week and met with many government officials, including Ariel. Medvedev paid a visit to the Agriculture Ministry's Volcani Center in Rishon Lezion, where he took a shining to a small drone that was on display.

Despite clear instructions from the Defense Ministry that any transfer of unmanned vehicles to foreign countries requires an export license, Ariel didn't ask for one, and offered the drone to Medvedev on the spot.

The Russian president gladly accepted the gift and sent two members of his delegation to collect the small helicopter and load it onto his plane.

The Israeli media focused on the cost of the "toy" - NIS 200,000 - and the violation of government procedures that occurred. But The Jerusalem Post has learned that the transfer was also in violation of Israeli security export instructions and most probably was done without the approval of the manufacturers.

The drone was produced by the Spanish company Alpha Unmanned Systems, and one of its essential components is the thermal camera installed.

The camera is produced by the US giant Flir, which makes most of its cameras for military or dual use. According to the company website, its products require an export license by the US Department of Commerce. It is unlikely that such a license was given to either the Spanish company or Israel to transfer it to Russia, which is under US and NATO sanctions because of its invasion of Ukraine and the annexation of the Crimean peninsula more than two years ago.

In the past, Israel has been reprimanded by the United States for transferring US technology and equipment to China without permission.

All parties involved - Ariel's office, the Agriculture Ministry, the Volcani Center, the Prime Minister's Office, the Alpha and Flir companies and the US Embassy - declined to comment. The Defense Ministry said Ariel's decision "was not coordinated with us."

Jerusalem Post
Cyber concerns bring leaders from across globe to Tel Aviv
Wednesday, 16 November 2016
Byline: Anna Ahronheim

Jerusalem - Thousands of top decision-makers, along with senior government and law enforcement officials from 80 countries, gathered in Tel Aviv this week for the fourth International Homeland Security and Cyber Conference.
The conference, which runs November 14 to November 17 at Tel Aviv's Convention Center, focuses on the ever-changing challenge of protecting data from the merging of physical and cyber crime.

Israel is a leader in cyber security. More than 300 companies had sales of $4b. in 2015 alone, and the conference is showcasing hundreds of those companies tops in the field of homeland and cyber security.

Speakers will discuss how and why the increased number of terror attacks worldwide has led to government strategies to better protect their strategic assets, including citizens.

Chief information security officer at Barclays Bank, Troles Oerting, said, "When the rules of the game have changed, we have to change as well." That sentiment was echoed by Meir Hayun, chief superintendent and head of the national cyber crime unit of the Israel Police, who said there needs to be a "change in how we think of intelligence today."

As part of the conference's main focus on cyber security, a discussion was held on the significant role played by social media in radicalization and encouragement of terrorism.

In a world of constant change, new threats arise on a daily basis. One game-changer is the threat posed by robots on social media, where decisions must be made if inciteful material on sites such as Twitter and Facebook were posted by human beings or "bots."

As the influence of social media grows, so does concern about its effect on vulnerable youth, especially in regard to Islamic extremism.

Former chief of Shin Bet Yoram Cohen talked about the large number of third-generation Muslim immigrant youths who did not integrate into European society and "underwent an identity crisis which caused them to become disenfranchised with the state." These predominantly male youth from lower-economic households often turned to radical Islam and terror in order to atone for what they perceive as past crimes or sins, usually involving drugs.

"When they can't make it to the Middle East, they carry out attacks at home. And those who do make it often serve as role models for those who remain in Europe," Cohen said, "posing an additional threat to law enforcement."

Salafi, or fundamentalist, Jihadi terrorism can also found among Palestinians, Cohen said. While there is limited support within that sector, the rise of its popularity and influence of the Islamic State create worries to, among others, Palestinian authorities.

According to Cohen, while most Palestinians don't support or identify with Islamic State, there has been an increase in ISIS-influenced cells, caught at the end-stages of planning attacks on Israeli targets, before plans could be carried out.

In his second public appearance since leaving Shin Bet, Cohen told the crowd that "the reality of mass terror cannot be expected to change in our favor any time soon," and pointed to online incitement as a major player in the process of radicalization and terrorism.

Gulf News
Cyber security consultancy firm Dark Matter to expand operations (Canada).
Wednesday, 16 November 2016
Byline: Fareed Rahman

Abu Dhabi - Abu Dhabi-headquartered cyber security consultancy firm Dark Matter is planning to expand operations as cyber security threats grow, the chief executive officer of the company said on Tuesday.
"As part of our expansion plans we will be opening a managed security operations centre in the first quarter of next year that will enable us to monitor the IT network of different entities all the time and prevent it from cyberattacks," said Faisal Al Bannai, addressing the media.

He did not give a total investment figure in building the new centre but said investments will be huge.

The company launched in 2014 has offices in Dubai, Abu Dhabi, Canada, China and Finland. It has a large number of customers ranging from government entities to private firms.

"It's been an interesting journey in the last two years. We grew from 100 team members last year to more than 400 employees at present. The biggest accomplishment has been the kind of people we could attract in the last two years. We have a team from different parts of the world."

He said there is a heavy demand from entities, governments and individuals to secure themselves. "The industry is large and growing and looking for innovative solutions. The aim of Dark Matter is not to serve the UAE or GCC market but to become a global player using UAE as a hub."

The products which the company is developing currently include Securecom, blockchain technology, crypto development and big data analytics.

"We are developing securecom that will enable secure email, secure chat, secure voice and secure file share. There is a whole host of securecom portfolios which we will be announcing at the end of the quarter and next year."

Blockchain technology improves efficiency and processes and Big data analytics can be used for smart city deployment where you can integrate everything from traffic feeds, to camera feeds to electricity feed to social media feed, he said.

According to the company, European Union security agency has identified a number of cybercrime trends. They include payment fraud, the criminal use of data, online child sexual abuse, ransomware, among various other online crime activities.

Khaleej Times
UAE responding to cyber threats
Wednesday, 16 November 2016
Byline: Ashwani Kumar

Abu Dhabi - The UAE is evolving and seriously looking to tackle the challenges of cyber security, an official said on the sidelines of the RSA Conference - the world's leading information security conference and exposition - in Abu Dhabi on Tuesday.
"The UAE, in terms of security, is pretty good. There is recognition. They are willing to do more about handling the challenges. They are spending so much on industry. If we look at stats, the UAE in 2014 spent $5.7 billion, but by 2019 they will be spending $9.56 billion. That is a 13 per cent rise in term of index, so there is recognition," RSA (Europe, Middle East and Africa) advanced cyber defence practice director Azeem Aleem said. "But are they evolving with the threat? They are not advancing," Aleem noted.

"It's evolving but they are still using traditional tools. Criminals are now very specifically picking targets. They are evolving whereas we are not. There is no skills sector problem. We can't have one fix-solution for all problems," he added.

"We are seeing the industry control system in the Middle East is vulnerable. We have seen evidence in Iran, Saudi Arabia and Ukraine," Aleem added.

The conference, held in partnership with UAE National Electronic Security Authority (NESA), saw five keynote speeches, 22 track sessions and over 35 companies showcasing their latest capabilities.

Adelaide Advertiser
ID fraud linked to terrorism
Wednesday, 16 November 2016
Byline: Staff reporter

Adelaide - New research shows Australians are falling victim to identity crime at the rate of one every 20 seconds.
Justice Minister Michael Keenan will also reveal today that people convicted of terrorism offences in Australia have used false identities to assist in planning terrorist attacks.

"This includes purchasing ammunition and chemicals to make explosives and prepaid mobile phones to communicate anonymously," he told The Advertiser yesterday.

Mr Keenan said a new $50 million biometric identification system would help police and other agencies crack down on identity fraud."The Government made this investment because we realise that biometric data sources, such as fingerprints and facial images, offer a degree of accuracy and assurance in identity verification processes," he said.

Sydney Morning Herald
Airports warned of 'terrorist infiltration'
Wednesday, 16 November 2016
Byline: Rachel Olding

Sydney - Australian airports are "extremely vulnerable" to infiltration by terrorists who could launch catastrophic attacks from within, one of the world's leading cybercrime and counter-terrorism experts has warned.
Jim Kent, an adviser to the United Nations who pioneered digital investigation techniques as a British police officer, said recent events have highlighted the potential for terrorists to infiltrate airports by corrupting airport officials or hacking digital systems.

In May, Fairfax Media uncovered widespread and unprecedented corruption among Australian border security workers in Melbourne and Sydney who have been assisting organised crime rings and drug smugglers for years.

Last week, the Australian Federal Police revealed that air traffic control broadcasts at Melbourne had been hacked over several weeks by a hoaxer and there have been warnings from the Australian Criminal Intelligence Commission that links between crime gangs and terrorists are growing.

Dr Kent, who spoke to Fairfax Media in Sydney ahead of briefings with the federal government, said the risk was greater when large agencies operated in silos.

"Airports are still extremely vulnerable to infiltration ... by terrorist groups because critical monitoring of unusual activity and enforcement of security measures is rarely joined up," he said.

"Terrorist groups could still work their way into an airport like a virus, for example by covertly infiltrating baggage handlers, immigration staff, freight drivers, pilots and cabin crew."

He said the risk of infiltration was not confined to airports. It also affected nuclear reactors, utilities, transport companies and financial institutions.

As the global head of security and intelligence for data investigation company Nuix, he has briefed several companies this week on using systems that pick up on seemingly innocuous pieces of information among employees and collate it to detect patterns. He has observed terrorist cells recruit employees by "hammering" them with Facebook requests or targeting those with money troubles. He said recruitment happens over two to three years.

But Clarke Jones, a counter-terrorism adviser who worked in aviation security before the Sydney Olympics, said Australian extremists lack the capability for such attacks.

"The level of sophistication is just not there," he said.

Kit Bennetts, a former intelligence officer, policeman and airline executive, said Australia does a good job at airport security but it would be "certainly feasible" to infiltrate it.

"Terrorist organisations ... watch and learn," said Mr Bennetts, a Southern Cross University lecturer in aviation management. "You only have to pick up a spy book from the '60s to learn about recruitment and gradual involvement [or] about penetration operations."

He said investigators can follow the money trail when it comes to organised crime but ideological crime was harder to detect.

Sydney and Melbourne Airports referred questions to the Department of Border Protection and Immigration, which didn't respond by deadline.

Intelligent Risks chief executive Neil Fergus, who conducted a government review into airport security, said Dr Kent's assertion was not "grounded in fact or in any apparent understanding of the checks, controls and systems that mitigate against such developments".

He said the corruption scandals showed detection systems were working.

Wall Street Journal
NSA Chief: 'Uneven' Cooperation Between Public, Private Sectors Impedes Cyber Defenses
Wednesday, 16 November 2016
Byline: Alan Cullison

New York - The head of the U.S. National Security Agency said "uneven" cooperation between the government and private sector has hampered the fight against a "literal onslaught" of cyber attacks from criminal and state-supported hackers.
Speaking at The Wall Street Journal CEO Council, Adm. Michael S. Rogers said the host of hackers is "so large and so diverse" that perpetrators are difficult to identify. About two-thirds are criminals or criminal groups looking to steal personal information for financial gain, and the balance are state-sponsored hackers, he said.

He said company leaders need to take a personal interest in cyber security, which has become too important a matter to be delegated entirely to network security specialists.

"You need to shape the discussion," he said. "I don't pretend that this needs to totally dominate your life, but there is a significant role for you to play."

The appeal for greater cooperation challenges the abiding suspicion in the private sector about government intentions.

In a poll of executives at the conference, 9% of the respondents said they would never sufficiently trust the government with information to work with it during a cyber attack.

Another 34% said they would cooperate with the government only if their own company was being attacked, while the 57% said they would readily cooperate.

Adm. Rogers, who also heads the U.S. Cyber Command that coordinates U.S. military networks, said the traditional understanding of private and public property hampers cooperation.

"My point is that cyber does not recognize these arbitrary lines that we have drawn -- it doesn't recognize the geography," he said. "Network structures in the world wide web [are] not organized that way. Our adversaries don't work that way."

Although the U.S. is trying to defend networks within its borders, it cannot effectively do so without the help of U.S. companies that need to reveal something about their networks, he said.

"If you want me to defend something, I can't do it from the outside," he said. "I can't defend something if I don't have access to the network structure - it's like fighting with one hand tied behind your back."

Adm. Rogers said the government worked productively with Sony Pictures Entertainment Inc. after the company reported that a hacker group released a trove of data looted from its networks. That included personal information about employees and their families, e-mails, salaries at the company, and copies of then- unreleased Sony films. The U.S. government determined the attack was sponsored by the government of North Korea. Pyongyang denied the accusation.

After realizing the seriousness of the hack, he said, Sony officials contacted the U.S. government for help determining the perpetrators of the hack and developing a plan to prevent further intrusions.

He said he explained to Sony officials that government investigators would need full access to Sony networks to do an effective post-mortem, something that the company allowed only after the government promised to explain what the government was doing and why.

Toronto Star and CBC News
Canadians support more investigative powers for police -- with a catch
Thursday, 17 November 2016
Byline: Robert Cribb and CBC Staff

Ottawa - Nearly 70 per cent of Canadians are willing to give police greater powers to investigate suspects cloaked by online anonymity - as long as their actions are monitored by a judge, a Toronto Star/CBC national poll has found.
While 2,500 respondents to the poll were split down the middle on Canadians' right to complete digital privacy, most said that right should not extend to suspects in a serious crime investigation.

"The vast majority of Canadians . . . are willing to accept certain conditions . . . if it means that public safety is put first and their own families or personal safety is protected because police and intelligence agencies have these tools," said David Coletto, CEO of Ottawa-based Abacus Data, which conducted the polling on behalf of the Toronto Star and CBC News.

"When a judge is involved, when a warrant is needed, we find broad support. It's only when you take away that judicial oversight that you see a much more divided population."

The findings are part of a Toronto Star/CBC investigation into policing in the digital age, a topic under debate in national security public consultations. Top RCMP officials warn that serious crimes are increasingly unpunished because evidence is disappearing behind sophisticated encryption or being purged from the servers of telecommunications companies. The poll has an error margin of plus or minus two percentage points, 19 times out of 20.

Perhaps the most striking finding is that Canadians are open to a police proposal for a law allowing authorities to compel a suspect in a criminal investigation to hand over the password or encryption key to investigators.

Initially, nearly half of respondents - 49 per cent - agreed police should have the ability to access personal devices. With the addition of a judge's authorization, support jumps to 77 per cent.

"There's broad support . . . which I think was an interesting finding," Coletto said.

"Canadians - and I've seen this in other research we've done on other controversial issues - are open-minded. They're willing and open to being persuaded about public policy questions."

There is a notable gender gap in the responses with men taking a distinctly stronger privacy position than women.

For example, 55 per cent of men agreed that every Canadian has the right to complete digital privacy versus 40 per cent of women.

For suspects in serious crime investigations, 30 per cent of men insist on complete digital privacy as a right. Only 17 per cent of women demand that right for crime suspects.

Other key findings include:

19 per cent of Canadians are "privacy purists" who oppose any infringement on their digital privacy, even if they are suspected of committing a serious crime. The purists are 71 per cent male and are much more likely to use encryption. They are also less trusting of law enforcement, security, or legal institutions.

47 per cent of Canadians are "conditionalists" who are split on the complete right to digital privacy but agree that suspects in serious criminal investigations would lose the right if a judge issues a warrant.

19 per cent of Canadians are "security firsters" who believe Canadians do not have a right to complete digital privacy, especially for those suspected of committing a serious crime. Security firsters are 61 per cent female, older (57 per cent are 45 years or older) and are more trusting of law enforcement and intelligence institutions.

The initial polling of 1,500 people was completed Oct. 20 to 22.

A second phase of polling took place Nov. 7 to 9, after reports that a Federal Court judge found that Canada's intelligence agency, CSIS, had illegally gathered Canadians' private information and that Quebec police intercepted and tracked the cellphones of at least 10 journalists to discover their sources.

An additional 1,000 Canadians were polled in this second phase.

The results showed almost no meaningful change.

There was very little or no change among different age groups (young people share many of the same opinions as older respondents) and political persuasions.

Police in Canada - including RCMP Commissioner Bob Paulson - are calling for access to the basic identifying information without requiring a warrant from a judge.

That's where Canadians draw a line.

More than three-quarters of respondents say police should be required to get a warrant from a judge every time they search a suspect's basic digital information.

Even when presented with law enforcement's argument that the time and red tape involved in obtaining a warrant can slow down and even entirely undermine an investigation, only 35 per cent supported a law that would allow warrantless access.

Canadians are split on the police proposal for a law that would require telecommunications companies to retain data for two years so police could access data.

Forty-one per cent agree, 39 per cent disagree and 19 per cent are unsure.

But agreement rises to 66 per cent if a warrant is obtained.

"That check actually makes people who were initially uncomfortable, far more accepting of the police having that ability to use that data when they think it's important for their investigation," Coletto said.

The only question that produced near consensus asked Canadians if police and intelligence agencies already have the ability to monitor Internet activities.

Ninety-four per cent said they believe authorities can already do so surreptitiously.

Nearly half of respondents said they believed their Internet activity is monitored by police or intelligence agencies.

"These two data points suggest that even though . . . a significant portion believes they have a right to digital privacy, very few think that it's possible for them to be completely anonymous online," Coletto said.

They are right, said former provincial information and privacy commissioner Ann Cavoukian.

"This type of activity has been going on for a long time," she said.

"This is something we need to be very concerned about. To me, freedom is absolutely critical. Preserving that freedom now and well into the future will take all of our efforts."

Robert Cribb can be reached at rcribb@thestar.ca

19% of respondents are "security firsters," who believe Canadians do not have a right to complete digital privacy

Source: Abacus Data poll for the Toronto Star/CBC

iPolitics.ca

Surveillance watchdog says C-22 not likely to be abused
Thursday, 17 November 2016
Byline: Amanda Connolly

Ottawa - The man in charge of overseeing Canada's electronics surveillance agency says there is no reason to believe the government would abuse controversial provisions in its national security committee legislation that give ministers the power to refuse to disclose requested information.
"I don't see why they would do that unless they are in bad faith, and I assume that everybody is in good faith unless the contrary is proven to me," said Jean-Pierre Plouffe, commissioner of the Canadian Security Establishment. "The fears we have are seldom realized to the same extent we had thought. Yes, it is a restriction, but it is a reasonable one."

Bill C-22, currently being studied at the House of Commons public safety committee, would create a nine-member committee of parliamentarians tasked with monitoring and scrutinizing the activities of all government departments and agencies that engage in national security activities.

While it would bring Canada up to speed among the Five Eyes intelligence allies (we are currently the only one without such a committee), opposition critics have raised red flags over several key components of the bill.

First, the legislation would allow the government to appoint a chair of the committee as well as all of its members rather than allowing parliamentarians to vote to confirm them or allow committee members to elect their own chair.

Second, the bill contains what some national security experts have dubbed "potential Mack truck exemptions" when it comes to giving ministers the power to refuse to disclose information the committee has requested.

Third, it requires the committee to submit any reports it produces to the prime minister for vetting and requires that the committee scrub the report for issues the prime minister flags as potentially jeopardizing national security before the report can be presented to Parliament.

There is no recourse mechanism for the committee to challenge required redactions or ministerial refusals to disclose information.

The government says the committee would have the power to complain publicly when it feels it is being censored and the public backlash would be a powerful mechanism for motivating a government not to refuse or redact unless absolutely necessary.

However, the lengthy battle of trying to force the former Conservative government to disclose information related to the Afghan detainee scandal in 2010 often comes up in discussions among committee members who suggest "national security" could encompass pretty much anything the

government doesn't want to make public and also cannot be challenged or evaluated in an objective way.

The creation of a committee tasked with national security oversight was a key campaign promise by the Liberals and also part of their plan to reform national security in light of the controversial bill C-51, passed by the former government.

That bill sparked a huge public backlash after it was perceived as going too far in allowing for expanded information sharing among government departments, enhancing the powers of the Canadian Security Intelligence Service, and lowering the legal threshold for who can be surveilled by law enforcement.

Ian McPhail, chair of the RCMP's Civilian Review and Complaints Commission, was also at the committee and stressed the need for a continued discussion around the balance of privacy and civil liberties, and suggested the committee can play a leading role in leading that conversation for Canadians.

"There is a constant tension between our commitment to civil liberties but also to the protection of Canadians in terms of national security issues," he said. "Exactly how that balance should be reached I would see as being one of the key purposes of this committee because the review bodies aren't able to perform that function. The committee, provided there's not undue partisanship, should be able to do so."

The committee is working to complete hearings and move to clause-by-clause consideration by November 23.

Once complete, the bill will head back to the House of Commons for third reading.

CBC News and Toronto Star
Canadians want judicial oversight of any new digital snooping powers for police: Poll
Thursday, 17 November 2016
Byline: Dave Seglins, Robert Cribb and Chelsea Gomez

Most Canadians feel strongly about their right to privacy online, but a new poll shows the vast majority are willing to grant police new powers to track suspects in the digital realm -- so long as the courts oversee the cops.
Nearly half of the respondents to an Abacus Data survey of 2,500 Canadians agreed that citizens should have a right to complete digital privacy. But many appeared to change their mind when asked if an individual suspected of committing a serious crime should have the same right to keep their identity hidden from police.

"The vast majority of Canadians ... are willing to accept certain conditions ... if it means that public safety is put first and their own families or personal safety is protected because police and intelligence agencies have these tools," Abacus CEO David Coletto said.

"When a judge is involved, when a warrant is needed, we find broad support. It's only when you take away that judicial oversight that you see a much more divided population."

The survey, conducted on behalf of CBC News and the Toronto Star, asked Canadians about their views on three specific proposals to expand police powers, which are raised in a federal discussion paper that's part of a review of Canada's Anti-Terrorism Act.?

Police across the country say they need expanded powers to track crime suspects and national security threats who use encryption and other high-tech tricks to hide their digital tracks.

RCMP Commissioner Bob Paulson put it this way:

"If you've got a complaint of criminality on the internet, you're going to have to think about where you go with that complaint because I don't know that we can help you. And that's a terrible thing for a person who's in charge of a police force to say when citizens, when companies, when corporate Canada, or indeed the government comes to us and says, 'Hey, we've been victimized on the internet.'"

Passwords and encryption codes

Respondents were evenly split on whether police should be able to demand suspects or witnesses hand over passwords or codes to unlock devices and encrypted data.

But support for granting police this authority increased to 77 per cent if a judge is required to first approve a warrant.

Phone and internet user data

Less than half of respondents agreed communications providers should be forced to keep text, email, phone and internet records for two years to assist potential criminal investigations.

But support jumped to 66 per cent if access to the stored information is protected and police would need a judge's order before accessing a suspect's records.

"Under the right conditions, there is broad support for this across political lines, across gender and even across generation," Coletto said.

Paulson says access to this information is crucial.

"That's a very important data set that we would only access with a warrant, but it has to be there," the top Mountie told CBC News and the Toronto Star. "Because there's nothing worse than trying to go and recreate somebody's movements through cell sites or to deduce who the offender is and the data's all been destroyed."

Easy access to subscriber info

Opposition was strongest to the third proposed new power for police: access to basic subscriber information (such as a user's name and IP address) without authorization from a judge.

Most respondents (78 per cent) said police should need judicial approval to ask a communications company for a person's basic digital identity, and only 35 per cent said they'd support a system where a senior police officer or prosecutor could sign off.

Police used to request subscriber information hundreds of thousands of times a year, but that changed in 2014, when the Supreme Court ruled that in the absence of a specific law, police requests to phone and internet companies amount to a search and therefore require a warrant.

Police compare it to looking up licence plate information, which doesn't require permission from a judge.

Plus, Paulson says, Canada lags behind its allies the U.S., Australia, New Zealand and the U.K., which allow senior police officers or prosecutors to oversee the requests.

But again, Coletto says, judicial oversight is clearly important to Canadians.

"Even when we give both sides of the argument, we find Canadians are more likely to oppose a new law that would give police that authority or administrative authorization than those that would support it."

Abacus Data surveyed 1,500 Canadians in October, before two major news stories broke about privacy and authority. The first found CSIS had violated court orders and the other revealed Montreal police got approval from a justice of the peace to track the cellphones of six journalists.

CBC and the Toronto Star had Abacus survey another 1,000 Canadians after the stories made headlines.

Coletto says the overall results remained identical, but he cautions the stories could still affect public trust.

"Awareness of these stories has not reached a saturation point," he said.

"Support for expanding powers is tied to judicial oversight. If these organizations don't follow the court orders, then we might see public acceptance of expanded powers deteriorate."

Globe and Mail
Canadian journalists push for 'shield law' to protect sources
Thursday, 17 November 2016
Byline: Daniel Leblanc

Ottawa - Journalists and parliamentarians are putting pressure on the Liberal government to enhance the protection of reporters and confidential sources, calling for quick legislative changes instead of rhetorical support for the freedom of the press.
The calls flow from recent cases in which police spied on journalists to obtain information on their sources, raising questions across Canada about the quality of the judicial process for obtaining warrants.

At a news conference in Ottawa on Wednesday, two journalists who are in legal battles with police authorities backed a proposal for a "shield law" that allows reporters to protect the identity of their sources and confidential information.

"Mine is just one of many cases of the growing erosion of press freedom in Canada," said Ben Makuch, a journalist for Vice News who is refusing to provide information from a confidential source to the RCMP.

Mr. Makuch faces a possible jail sentence for refusing to comply with a court order. He said the RCMP's actions have created "irreparable damage" to journalists' ability to win the trust of sources.

Patrick Lagacé, a journalist at La Presse, recently learned that the Montreal police service had obtained judicial approval to consult his phone records, tap his phone and trigger the GPS on his mobile device to track his meetings with sources. He said the Liberal government is saying all the right words in the defence of journalistic freedom, but that police officers need to face tougher requirements to go after a journalist's sources.

"The mentality of police officers is not different whether you are in Saskatchewan or British Columbia or Quebec," Mr. Lagacé said. "I am convinced that other police agencies, if they can have access to this type of information, will try to do so without asking themselves any questions."

Also present at the news conference were journalist and author Mohamed Fahmy, who was imprisoned for more than a year in Egypt because of his reporting, and Tom Henheffer, the executive-director of Canadian Journalists for Free Expression. Mr. Henheffer said he distrusts agencies such as the RCMP and CSIS that have increased means to monitor electronic communications, and that new laws are needed to curtail their powers.

"The fact is the state apparatus and the surveillance capabilities of the state are absolutely enormous, and we cannot fully protect ourselves against them," he said. "That is why there needs to be a change at the legislative level in order for us to really enjoy a free press in Canada. I don't fully trust government

agencies because there is a lack of accountability, but all of that can be fixed with simple legislative changes."

Prime Minister Justin Trudeau has expressed his concerns over the recent revelations involving Mr. Lagacé, and Public Safety Minister Ralph Goodale has said his government is open to toughening the rules that govern how and when the federal government can investigate members of the media. "All of the safeguards in place at the federal level are being reassessed to make sure they are strong enough," he said in the House of Commons. "We are welcoming any input from journalists, lawyers or others if they have suggestions to make about how the law needs to be improved."

The NDP is arguing the government needs to go further and launch a public inquiry into the protection of sources at the federal level.

"The government certainly talks a better game than the previous [Conservative government], but at the end of the day, it's the legislation that matters," NDP MP Matthew Dubé said.

Washington Post
In our new Cold War, deterrence should come before detente
Tuesday, 15 November 2016
Byline: David Ignatius

Column - The White House sent a secret "hotline"-style message to Russia on Oct. 31 to warn against any further cyber-meddling in the U.S. election process. Russia didn't escalate its tactics as Election Day approached, but U.S. officials aren't ready to say deterrence worked.
The previously undisclosed message was part of the high-stakes game of cyber- brinkmanship that has been going on this year between Moscow and Washington. How to stabilize this relationship without appearing to capitulate to Russian pressure tactics is among the biggest challenges facing President-elect Donald Trump.

The message was sent on a special channel created in 2013 as part of the Nuclear Risk Reduction Center, using a template designed for crisis communication. "It was a very clear statement to the Russians and asked them to stop their activity," a senior administration official said, adding: "The fact that we used this channel was part of the messaging."

According to several other high-level sources, President Obama also personally contacted Russian President Vladimir Putin last month to caution him about the disruptive cyberattacks. The senior administration official wouldn't comment on these reports.

The private warnings followed a public statement Oct. 7 by Director of National Intelligence James Clapper and Secretary of Homeland Security Jeh Johnson charging that "Russia's senior-most officials" had authorized cyberattacks that were "intended to interfere with the U.S. election process."

The senior administration official said Russia gave a "noncommittal" response to the Oct. 31 message, neither acknowledging the U.S. charges nor denying them. But the official confirmed reports by other high-level sources that after the public and private warnings, Russia did not increase its cyber-activity and may have reduced it.

"We did not see an escalation of Russian cyber-activity aimed at either trying to disrupt the election process or trying to influence the process, in the month leading up to the election," said one senior official. A second senior official cautioned, however, that it was too early to say "whether the Russians were deterred" from additional activity.

The White House feared a last-minute Russian cyber-onslaught right up to Nov.?8, but it apparently never came. "We saw no evidence of any systematic attempt to disrupt the election on Election Day," the first official said.

These disclosures about secret U.S.-Russia contacts are the latest chapter in the story of heightened confrontation between the two countries -- a process that Putin and Trump say they are seeking to reverse. Putin phoned Trump on Monday to discuss ways to improve current "unsatisfactory" relations after Trump takes office and seek a "partner-like dialogue," according to a Kremlin statement.

The Obama administration has grappled with how to establish norms of deterrence in cyberspace that check destabilizing actions by an aggressive, risk-taking Russia. The White House thought it was making progress with a joint statement at the November 2015 G-20 summit in Antalya, Turkey, which affirmed that "international law applies to state behavior in cyberspace." The United States argues that this commitment includes observing laws of armed conflict that require proportionality and limited collateral impact in whatever battlespace. But the Obama administration fears Russia is ignoring these limits.

The Obama administration is ready to explore these issues further with Russia through a little-known "working group" created under a defunct "presidential bilateral commission." The working group last met in April in Geneva. At that meeting, according to the White House, "both sides discussed the possibility of expanding the quantity and scope of information sharing about malicious activity occurring on the networks of both countries."

Those words ring hollow now, in light of alleged Russian activities this year.

Russia experts in the Obama administration caution their successors: "It will be very difficult for the next administration .?.?. to know what Russia's intentions are and whether you can have confidence that they will live up to their commitments," said the second official. Russia has shown "increasing willingness to take risky actions," and "old assumptions about the careful, calculating, risk-averse nature of Russian leadership .?.?. seem to be shifting."

Republican Sen. John McCain (Ariz.), a longtime critic of Russia, issued a similar warning Tuesday about Putin's professed desire for "partner-like" relations. "We should place as much faith in such statements as any other made by a former KGB agent who has plunged his country into tyranny, murdered his political opponents, invaded his neighbors, threatened America's allies and attempted to undermine America's elections," he said.

A new Cold War has begun in cyberspace. Trump seems to want detente. But first he should think carefully about how to establish clear norms of deterrence in this new domain.

New York Times
The World Needs WikiLeaks
Thursday, 17 November 2016
Byline: Sarah Harrison

Op-ed from Berlin - My organization, WikiLeaks, took a lot of heat during the run-up to the recent presidential election. We have been accused of abetting the candidacy of Donald J. Trump by publishing cryptographically authenticated information about Hillary Clinton's campaign and its influence over the Democratic National Committee, the implication being that a news organization should have withheld accurate, newsworthy information from the public.
The Obama Justice Department continues to pursue its six-year criminal investigation of WikiLeaks, the largest known of its kind, into the publishing of classified documents and articles about the wars in Iraq and Afghanistan, Guantánamo Bay and Mrs. Clinton's first year as secretary of state. According to the trial testimony of one F.B.I. agent, the investigation includes several of WikiLeaks founders, owners and managers. And last month our editor, Julian Assange, who has asylum at Ecuador's London embassy, had his internet connection severed.

I can understand the frustration, however misplaced, from Clinton supporters. But the WikiLeaks staff is committed to the mandate set by Mr. Assange, and we are not going to go away, no matter how much he is abused. That's something that Democrats, along with everyone who believes in the accountability of governments, should be happy about.

Despite the mounting legal and political pressure coming from Washington, we continue to publish valuable material, and submissions keep pouring in. There is a desperate need for our work: The world is connected by largely unaccountable networks of power that span industries and countries, political parties, corporations and institutions; WikiLeaks shines a light on these by revealing not just individual incidents, but information about entire structures of power.

While a single document might give a picture of a particular event, the best way to shed light on a whole system is to fully uncover the mechanisms around it -- the hierarchy, ideology, habits and economic forces that sustain it. It is the trends and details visible in the large archives we are committed to

publishing that reveal the details that tell us about the nature of these structures. It is the constellations, not stars alone, that allow us to read the night sky.

There are two contradictory myths about how we operate: on one hand, that we simply dump whatever comes to us into the public's arms; and on the other, that we pick and choose material to harm our alleged political enemies.

We do neither. Yes, we believe in the integrity of source material, in the value of conserving pristine collections of documents, and we strive to make this historical record accessible to the public. We publish in full, in an uncensored and uncensorable fashion. But we also research, validate and contextualize the submissions we receive. While it can be difficult to balance the needs of the public to have timely access to large archives with individual privacy, such concerns have mostly been disingenuous.

At times we receive individual documents, but we have come to specialize in large collections. Over the last decade we have vetted, indexed and published an average of 3,000 documents per day, including over 300,000 reports covering the wars in Iraq and Afghanistan, more than two million emails from Syrian political figures and over 120,000 documents from the Saudi Arabian Ministry of Foreign Affairs. We also curate the Public Library of United States Diplomacy, the world's largest collection of diplomatic cables (nearly three million).

WikiLeaks has transformed more than 10 million documents into a unique searchable archive, not only making our website the world's largest online library for suppressed information, but also enabling greater contextualization through relationships across publications.

Some have accused us of being pawns of the Russian government, but this misrepresents our principles and basic operations. WikiLeaks relies on our editor's invention of a secure anonymous online submission system to protect sources' identities. This technology has become a standard for many media outlets around the world. We prefer not to know who our sources are; we do not want to, and usually do not need to. What matters to us is the authenticity of the documents.

This has always been our position and approach, whether we were publishing material about the George W. Bush administration's wars or corruption within the Democratic Party. The establishment media was happy to work with us on the former, but turned against us when it came to the latter, calling into question our intentions and those of Mr. Assange. CNN has even suggested, wrongly, that readers may have legal troubles if they download documents from our site.

While we have no institutional bias and can publish only what we receive, we are happy to publish documents about any presidential candidate, at any time, anywhere for a globally significant election.

We publish without fear or favor, bringing transparency to powerful factions and secretive institutions, not taking any sides except that of the truth. We believe in the democratization of information and the power that knowledge gives to people to further peace, accountability and self-determination.

WikiLeaks will continue publishing, enforcing transparency where secrecy is the norm. While threats against our editor are mounting, Mr. Assange is not alone, and his ideas continue to inspire us and people around the world.

Note: Sarah Harrison is a journalist and editor for WikiLeaks.

Reuters
Trump cyber security team, policy slow to take shape: officials
Thursday, 17 November 2016
Byline: Dustin Volz, Mark Hosenball

Washington - President-elect Donald Trump's transition team has not announced a point person dedicated to cyber security policy or staffing in his administration, an omission that could make the United States more vulnerable to threats and worsen a government cyber talent shortfall, current and former national security officials said.
They and multiple sources involved with the Trump transition organization said they were unaware of any person in the Trump orbit who is dealing specifically with cyber security, and that there has been minimal contact with federal agencies.

The apparent lack of expertise or prioritization coincides with U.S. intelligence agencies, including the CIA, having pivoted to digital warfare to address the growing national security and economic threats that nation-states and extremist groups pose in cyberspace.

In response to a request for comment, a Trump spokeswoman referred to a cyber-security "vision" on Republican Trump's campaign website, which calls for an immediate review of U.S. cyber defenses and vulnerabilities and lists high- profile hacks as "key issues" without further explanation.

It did not mention cyber attacks on Democratic Party political organizations during the election campaign that the U.S. government said were carried out by Russia to interfere with the Nov. 8 vote. Trump praised WikiLeaks for publishing leaked emails from his opponent Hillary Clinton's campaign and also questioned whether Russia was responsible for the hacks.

A former National Security Agency (NSA) official who reviewed the "vision" statement said it was short on detail.

Kellyanne Conway, a senior advisor to Trump who managed his campaign, told reporters in the lobby of Trump Tower Wednesday that reports of a rocky transition process were false.

"You don't form a federal government overnight," she said.

The ousting of former Republican lawmaker Mike Rogers from Trump's transition team on Tuesday left a void of expertise on cyber and intelligence matters for the president-elect, officials said.

Rogers, who chaired the House Intelligence Committee while in Congress was talked about in Washington as a potential CIA Director or Director of National Intelligence.

Former Defense Intelligence Agency Director Michael Flynn and retired lieutenant general Ronald Burgess are part of Trump's transition team. They were focused on intelligence and security matters, according to a Trump team document that has circulated among Washington trade and lobbying organizations in the week since the New York businessman's stunning election victory.

Flynn is a contender to be the next Director of National Intelligence or White House National Security Adviser, according to people close to him and multiple media reports. A less likely possibility, according to the people, is Flynn would be named head of the National Security Agency.

But neither Flynn nor Burgess are experts on cyber security, nor have they indicated an interest in the subject to Obama administration officials, sources close to the Trump and Obama teams said.

TALENT GAP

The federal government has struggled for years to keep pace with the rising need for cyber talent.

A July memo from the White House's Office of Management and Budget found a critical shortage of talent across the country was worsened in government, caused in part by an inability to compete with lucrative salaries in the private sector.

James Norton, a former George W. Bush administration official who helped set up the Department of Homeland Security's first cyber security team, said that Trump's transition team may be waiting to move forward on the issue until after cabinet-level security posts are filled.

"Cyber will be a priority," said Norton, now president of Washington-based consulting firm Play-Action Strategies LLC. "There's a little bit of fog, but I think that will clear once the names of the nominees are out."

But finding and retaining qualified technical people to serve in government may become even more difficult under a Trump presidency because of disagreements with his policies and politics, three former national security officials said.

The president-elect's bombastic statements on the campaign trail frequently alarmed tech companies and at times elicited public mockery, such as when Trump called for closing off parts of the Internet to limit militant Islamist propaganda or urged his supporters to boycott Apple when it refused to help the FBI unlock an iPhone tied to one of the San Bernardino, Calif., shooters.

Susan Hennessey, a former attorney in the office of the general counsel at the NSA, said she has been urging people in the intelligence community to keep working in Trump's administration because their expertise will be necessary to protect the country and resist potential abuses of executive power on issues such as surveillance.

"In candor, I'm sad to be asking former colleagues whom I respect to consider setting aside their conscience in order to serve their country," said Hennessey, who now serves as managing editor of the national security blog Lawfare. "I can't and don't blame anyone who feels they can't stay."

A current national security official who has been approached by the Trump transition team said all or most political appointees in the Obama administration are expected to be sent packing after Trump's inauguration on Jan. 20. He predicted that as much as five to 10 percent of the federal workforce also might leave.

Richard Clarke, a former senior White House advisor on counterterrorism and cyber security in both the Bill Clinton and George W. Bush administrations, said Trump's election presents an opportunity to civil servants to help shape or resist the president-elect's opinion on policy matters. He said many of the same concerns about Trump existed within the federal bureaucracy when former President Ronald Reagan was elected in 1980.

"These people like Reagan and Trump are not well-grounded in policy," Clarke said. "They don't have a lot of firm beliefs that stem from years of analysis and experience," Clarke told Reuters. "You can change their mind if you do it subtly, if they trust you. And you may not even know you've changed their mind, because they don't know what their mind is."

Some parts of government are more effective than others at "slow-rolling" the president's impulses, Clarke said. But "you can't slow-roll work that needs to be done," such as improving cyber security and addressing cyber threats, he said.

New York Times
White House Confirms Pre-Election Warning to Russia Over Hacking
Thursday, 17 November 2016
Byline: David E. Sanger

Washington - Over the past month, President Vladimir V. Putin of Russia has received two starkly different messages about hacking into American computer networks from the current and future presidents of the United States: Don't you dare, and don't worry, we're not even sure it was you. The White House confirmed in a statement on Wednesday that eight days before the presidential election, the United States "contacted the Russian government directly regarding malicious cyberactivity" that was "targeting U.S. state election-related systems." It sent the message over a rarely used system: a hotline connecting the Nuclear Risk Reduction Centers in both countries, which they had agreed three years ago could also be employed to deal with major cyberincidents.

The pre-election warning -- only the latest after verbal cautions by President Obama, his defense secretary and the director of national intelligence -- was reported by The Washington Post.

The warnings to Russia against further hacking into polling or registration systems, or any further effort to affect the outcome of the election, are being hailed by the Obama administration as a success in deterrence. After all, they argue, a year and a half of Russian hacking activity seemed to slow, or halt, and there is no evidence that voting or counting of ballots was disrupted on Election Day.

But more than a few experts in deterring cyberattacks take a more skeptical view. They say the Russians had already achieved their main goal: to demonstrate how they could disrupt the American electoral process with the leak of hacked emails, including from the Democratic National Committee and Hillary Clinton's campaign chairman, John D. Podesta.

Mr. Putin suffered nothing worse than a warning, they note -- no sanctions, no counter cyberstrikes, no embarrassing revelations engineered by the United States. And he now has the satisfaction of dealing with President-elect Donald J. Trump, who during the campaign praised him, promised to build a more productive relationship with Russia and maintained there was no evidence that the Russians were behind the hacking.

"Anytime anything wrong happens they like to" blame the Russians, Mr. Trump said in an Oct. 10 debate with Mrs. Clinton. "She doesn't know if it's the Russians doing the hacking. Maybe there is no hacking."

Mr. Trump contended that the allegations of Russian activity were intended to "tarnish me" for advocating a new relationship with Moscow. He frequently repeated similar sentiments in the last weeks of the campaign, suggesting the hacking was a fabrication. The leaks of emails worked largely to his advantage, embarrassing Democratic leaders like Representative Debbie Wasserman Schultz of Florida, who was forced to resign as the chairwoman of the Democratic National Committee.

Mr. Trump's larger strategic message is that the United States and Russia need to cooperate on a range of issues.

But for now the situation underscores the uncertainty around the world about the direction of American foreign policy and gives Mr. Putin the opportunity to exploit differences between the current president

and his successor until Mr. Trump is inaugurated on Jan. 20. It is also raising the question of whether the Obama White House pushed back hard enough when American intelligence agencies concluded on Oct. 7 that "only Russia's senior-most officials could have authorized these activities."

James A. Lewis, a computer expert at the Center for Strategic and International Studies in Washington, dismissed the administration's claim that it had deterred Russia's hacking.

"It seems a little bold to claim this is a success for deterrence, since the Russians weren't deterred from doing anything," he said. "Their hacking work was mostly complete. The issue now is whether they will be deterred in the future, and the guessing is they will not. Strong private warnings aren't enough to constitute deterrence."

In fact, the Russians appear to have paid less of a price for their hacking around the election than North Korea did for its attack on Sony Pictures Entertainment in 2014. That attack melted down about 70 percent of Sony's computers and servers at its studios, wreaking considerable damage, and embarrassed many Sony executives. It was in response to the release of a movie, "The Interview," that imagined a C.I.A. plot to kill Kim Jong-un, the North Korean leader.

After the Sony episode, the United States issued more sanctions against North Korea and encouraged China to limit the North's internet access, all of which runs through Chinese switching centers. Many experts had expected the White House to follow a similar path with Russia.

Instead, the White House concluded that the warnings, and the unstated suggestion that the United States had the power to reach inside Russian networks and see the origin of attacks, might suffice. It is not clear if the administration plans any other actions against Russia before Mr. Obama's departure from office, but that seems less and less likely.

The Oct. 31 warning did not deal with the hacking of the Democratic National Committee or Mr. Podesta's account, which James R. Clapper Jr., the director of national intelligence, had previously said was conducted with the knowledge of the Russian leadership. Instead, it referred only to the concerns about hacking around the election process itself, and the fear it was originating from Russian territory, though it stopped short of saying it was a state-sponsored attack.

China Daily
Xi: Share internet governance
Thursday, 17 November 2016
Byline: Cao Yin and Zhang Zhihao

Wuzhen, Zhejiang - President Xi Jinping, who addressed a meeting of global internet experts on Wednesday, called for all countries to have independence in managing their own internet industry and equality among nations in participating in global information industry governance.

In a keynote speech via video at the opening of the third annual World Internet Conference in Wuzhen, Xi said that China would like to work together with the international community to "ensure the common well-being of humanity, uphold cyberspace sovereignty and also promote more fair and equitable global internet governance".

The three-day internet conference in the ancient Zhejiang province township has attracted more than 1,600 attendees from 110 countries and regions.

Xi applauded the great progress that has come with the internet, and discussed its new challenges and opportunities. "The development of the internet has no national boundaries. To take advantage of, promote and govern it, we must call for closer international cooperation and joint efforts to build a community of a common future in cyberspace," he said.

"A gentleman puts basic principles first, which will illuminate the way forward," he quoted a Chinese proverb as saying.

Liu Yunshan, a member of the Standing Committee of the Political Bureau of the Central Committee of the Communist Party of China, who attended the opening ceremony, said that China, a large internet country with more than 700 million netizens, is willing to strengthen policy coordination and cooperation with other countries.

To benefit all people of the world, "we should build a multilateral and transparent global internet governance system," Liu said.

Cooperation should be strengthened in coping with cyberspace security challenges, aiming to safeguard State security, public interest and citizens' legitimate rights, he said.

Del Christensen, chief of global business development for the Bay Area Council, a business- sponsored, public policy advocacy group based in San Francisco, said after listening to Xi that there should be "some standard that the world should abide by forge better cooperation and trade."

"The internet is not a lawless zone. Every other subject like finance, military and medicine all have rules. The internet should be no different," he added.

Global Times
Threats from cyberspace 'pressing and vital' in China: top State secret official
Thursday, 17 November 2016
Byline: Staff reporter

Beijing - Security threats coming from cyberspace are pressing and vital and China must increase its efforts to improve security technology to safeguard national interests, said a top official from the State secret administration.
"A series of Internet leaks in China and other countries show the threats coming from cyberspace are pressing and vital, and the technology to safeguard information security needs to be reliable, self-developed and controllable," Tian Jing, director of the National Administration for the Protection of State Secrets, told the People's Daily in an interview that was published on the newspaper's website on Wednesday.

Over 70 percent of leaked information classified as national secrets was passed on via the Internet, according to a 2014 report from the Internal and Judicial Affairs Committee of the National People's Congress.

China's top legislator adopted a revision to the Law on Guarding State Secrets in 2010 which defines a "State secret" as "information concerning State security and interests," the Xinhua News Agency reported.

Though China has established a system of security technology that covers a wide range of areas and is mutually supportive, information security technology still cannot meet the current requirements, and China must improve its technology effectively and innovatively, said Tian.

R&D talents and resources from academic institutes, universities and information security companies must be integrated into the country's efforts to safeguard State secrets with increasing government support, Tian noted.

Whoever steals, spies on, or unlawfully supplies State secrets or intelligence to overseas agencies may face punishments including the death penalty, according to China's Criminal Law.

Kyodo News
Japanese ICT solutions providers gearing up for Thai digital economy
Thursday, 17 November 2016
Byline: Silpchai Prasarnsuklarp

Bangkok - Japanese companies providing information and communication technology solutions are gearing up to meet increasing demand for digital services among Thai businesses, as the government is attempting to drive forward the country on the strength of the digital economy.
Japan's Ministry of Internal Affairs and Communications signed agreements Monday with two Thai government organizations in a bid to encourage bilateral ICT collaboration.

One agreement was inked with the National Broadcasting and Telecommunications Commission, Thailand's telecom regulator, for the purpose of telecom and broadcasting exchanges, while the other

accord was signed with the newly established Ministry of Digital Economy and Society for ICT development cooperation covering disaster risk management, cyber security and postal services.

Atsuko Tominaga, deputy manager at the Global Business Division of Internet Initiative Japan Inc., a leading cloud service provider, said IIJ has seen growing demand for data centers in Thailand due to government efforts to enhance the ICT sector by promoting the digital economy.

The company is planning to provide a modular data center and its procedural knowledge to the Thai side in the near future, she added.

IIJ has set up a joint venture with a Thai partner, T.C.C. Technology Co., which provides hosting and data center services, to offer local companies cloud solutions.

IIJ's cloud services, launched in the Thai market in October, have received good feedback from entrepreneurs who need cloud computing technology to help them run businesses, Tominaga said, adding the joint venture, Leap Solutions Asia Co., now has nearly 100 clients, both Thai and Japanese.

Veerapol Paisarnsupnimit, sales director at NTT Data (Thailand) Co., a subsidiary of Japan's Nippon Telegraph and Telephone Corp., said the company also sees potential for digital economy development in Thailand and plans to widen its customer base to small and medium-sized enterprises next year by collaborating with NTT's offices in Singapore and Malaysia.

Moreover, the company will pay more attention to serving non- Japanese corporations rather than focusing on Japanese multinational businesses. It is aiming to even the ratio of Japanese and non-Japanese customers, compared with 60:40 at present.

The Australian Financial Review
Infrastructure may fall victim to cyber attack
Thursday, 17 November 2016
Byline: Yolanda Redrup

Canberra - A former FBI special agent who oversaw the bureau's investigation of the 9/11 terrorism attacks says nation states are at risk of cyber terrorism attacks, with many foreign nations already having the capability to take down a foreign country's infrastructure assets.
But Mary Galligan, who is visiting Australia as part of her role as managing director of Deloitte & Touche's Cyber Risk Services practice, said the real risk would arise if these offensive measures were to fall into the hands of terrorists or rogue nations.

"Right now the way terrorists use the internet is highly concentrated on how they can radicalise individuals. They've figured out how to use the internet and click media campaigns to get individuals around the world to become radicalised and travel around the world," she said.

"But we can never talk enough about what could happen. Looking at history we've been criticised for not having done this enough. But it ends up coming back to the response ... so we also need to talk about having resilience to technical issues, regardless of where it comes from or how it's caused."

Ms Galligan spent 25 years with the FBI, with the first half of her career spent in the terrorism division combating al-Qaeda, before becoming the head of cyber and crisis management, where she responded to high-level cyber threats involving the financial services industry, media, hotels and retailers.

She joined Deloitte after leaving the FBI in 2013 and since then has provided cyber briefings to more than 60 boards of major US private and public companies.

The ASX and the Australian Investments and Securities Commission launched cyber "health checks" for the ASX top 100 firms last week, and Ms Galligan said firms that do not undertake risk assessments end up ill-equipped to deal with cyber threats.

"Organisations who do not take the time to do a cyber risk assessment and then come up with a strategy have often found themselves not being about to find out how much they should spend in each area, or they spend way too much in one area [of protection]," she said.

"Like any other part of the business, if you don't do an assessment, you don't have a strategy to follow."

The ASX's health checks, which form part of the government's cyber security strategy, were developed alongside professional services firms such as Deloitte, EY, KPMG and PwC.

Deloitte head of cyber governance and strategy in Australia, Tommy Viljoen, said the health checks for Australia's biggest businesses were just the first part of a larger strategy that would eventually see them rolled out to smaller companies.

"We have to start with the biggest organisations. It's about getting an independent view of how healthy the top 100 are, and then over time we'll cascade that down," he said.

"We've done a number of these reviews in the past 12 months, following the United State's National Institute of Standards and Technology (NIST) framework with organisations on a voluntary basis ... and I'm yet to see an organisation that has reached the level of cyber maturity that they'd like to be at."

Mr Viljoen said even though big businesses had more resources, they knew they still had room for improvement on cyber security.

"They're still not 100 per cent comfortable with where they're at."

The Intercept
TITANPOINTE
Wednesday, 16 November 2016
Byline: Ryan Gallagher, Henrik Moltke

New York - They called it Project X. It was an unusually audacious, highly sensitive assignment: to build a massive skyscraper, capable of withstanding an atomic blast, in the middle of New York City. It would have no windows, 29 floors with three basement levels, and enough food to last 1,500 people two weeks in the event of a catastrophe.
But the building's primary purpose would not be to protect humans from toxic radiation amid nuclear war. Rather, the fortified skyscraper would safeguard powerful computers, cables, and switchboards. It would house one of the most important telecommunications hubs in the United States -- the world's largest center for processing long-distance phone calls, operated by the New York Telephone Company, a subsidiary of AT&T.

The building was designed by the architectural firm John Carl Warnecke & Associates, whose grand vision was to create a communication nerve center like a "20th century fortress, with spears and arrows replaced by protons and neutrons laying quiet siege to an army of machines within."

Construction began in 1969, and by 1974, the skyscraper was completed. Today, it can be found in the heart of lower Manhattan at 33 Thomas Street, a vast gray tower of concrete and granite that soars 550 feet into the New York skyline. The brutalist structure, still used by AT&T and, according to the New York Department of Finance, owned by the company, is like no other in the vicinity. Unlike the many neighboring residential and office buildings, it is impossible to get a glimpse inside 33 Thomas Street. True to the designers' original plans, there are no windows and the building is not illuminated. At night it becomes a giant shadow, blending into the darkness, its large square vents emitting a distinct, dull hum that is frequently drowned out by the sound of passing traffic and wailing sirens.

For many New Yorkers, 33 Thomas Street -- known as the "Long Lines Building" -- has been a source of mystery for years. It has been labeled one of the city's weirdest and most iconic skyscrapers, but little information has ever been published about its purpose.

It is not uncommon to keep the public in the dark about a site containing vital telecommunications equipment. But 33 Thomas Street is different: An investigation by The Intercept indicates that the skyscraper is more than a mere nerve center for long-distance phone calls. It also appears to be one of the most important National Security Agency surveillance sites on U.S. soil -- a covert monitoring hub that is used to tap into phone calls, faxes, and internet data.

Documents obtained by The Intercept from the NSA whistleblower Edward Snowden do not explicitly name 33 Thomas Street as a surveillance facility. However -- taken together with architectural plans, public records, and interviews with former AT&T employees conducted for this article -- they provide

compelling evidence that 33 Thomas Street has served as an NSA surveillance site, code-named TITANPOINTE.

Inside 33 Thomas Street there is a major international "gateway switch," according to a former AT&T engineer, which routes phone calls between the United States and countries across the world. A series of top-secret NSA memos suggest that the agency has tapped into these calls from a secure facility within the AT&T building. The Manhattan skyscraper appears to be a core location used for a controversial NSA surveillance program that has targeted the communications of the United Nations, the International Monetary Fund, the World Bank, and at least 38 countries, including close U.S. allies such as Germany, Japan, and France.

It has long been known that AT&T has cooperated with the NSA on surveillance, but few details have emerged about the role of specific facilities in carrying out the top-secret programs. The Snowden documents provide new information about how NSA equipment has been integrated as part of AT&T's network in New York City, revealing in unprecedented detail the methods and technology the agency uses to vacuum up communications from the company's systems.

"This is yet more proof that our communications service providers have become, whether willingly or unwillingly, an arm of the surveillance state," said Elizabeth Goitein, co-director of the liberty and national security program at the Brennan Center for Justice. "The NSA is presumably operating under authorities that enable it to target foreigners, but the fact that it is so deeply embedded in our domestic communications infrastructure should tip people off that the effects of this kind of surveillance cannot be neatly limited to non-Americans."

The NSA declined to comment for this story.

The code name TITANPOINTE features dozens of times in the NSA documents, often in classified reports about surveillance operations. The agency uses code names to conceal information it deems especially sensitive -- for instance, the names of companies it cooperates with or specific locations where electronic spying is carried out. Such details are usually considered "exceptionally controlled information," a category beyond top secret and thus outside the scope of most of the documents that Snowden was able to obtain.

Secret NSA travel guides, dated April 2011 and February 2013, however, reveal information about TITANPOINTE that helps establish its connection to 33 Thomas Street. The 2011 guide, written to assist NSA employees visiting various facilities, discloses that TITANPOINTE is in New York City. The 2013 guide states that a "partner" called LITHIUM, which is NSA's code name for AT&T, supervises visits to the site.

The 33 Thomas Street building is located almost next door to the FBI's New York field office -- about a block away -- at Federal Plaza. The 2011 NSA travel guide instructs employees traveling to TITANTPOINTE to head to the FBI's New York field office. It adds that trips to the site should be coordinated with AT&T (referenced as "LITHIUM") and the FBI, including an FBI "site watch officer."

When traveling to TITANPOINTE, NSA employees are told to hire a "cover vehicle" through the FBI, especially if they are transporting equipment to the site. In order to keep their true identities secret while visiting, agency employees are instructed not to wear any clothing displaying NSA badges or insignia.

Upon arrival at TITANPOINTE, the 2011 travel guide says, agency employees should ring the buzzer, sign in, and wait for a person to come and meet them. The Intercept visited 33 Thomas Street and found a buzzer outside its entrance and a sign-in sheet on a desk in the building's lobby, which is manned by a guard 24 hours a day. There are also parking bays in front of the skyscraper designated "AWM," a traffic code for federal agencies.

A 1994 New York Times article reported that 33 Thomas Street was part of AT&T's "giant Worldwide Intelligent Network, which is responsible for directing an average of 175 million phone calls a day." Thomas Saunders, a former AT&T engineer, told The Intercept that inside the building there were at least three "4ESS switches" used to route calls across phone networks. "Of the first two, one handled domestic long-distance traffic and the other was an international gateway," said Saunders, who retired from his role at the company in 2004. The NSA's documents describe TITANPOINTE as containing "foreign gateway switches" and they state that it has a "RIMROCK access." RIMROCK is an NSA code name for 4ESS switches.

The NSA's documents also reveal that one of TITANPOINTE's functions is to conduct surveillance as part of a program called SKIDROWE, which focuses on intercepting satellite communications. That is a particularly striking detail, because on the roof of 33 Thomas Street there are a number of satellite dishes. Federal Communications Commission records confirm that 33 Thomas Street is the only location in New York City where AT&T has an FCC license for satellite earth stations.

The man behind the design of 33 Thomas Street, John Carl Warnecke, was one of the most prominent architects in the U.S. between the 1960s and 1980s.

Warnecke's high-profile projects included producing designs for the U.S. Naval Academy in Maryland, the Hart Senate Office Building in Washington, D.C., and the Hawaii State Capitol. In 1962, President John F. Kennedy's administration commissioned Warnecke to preserve and restructure buildings at Lafayette Square, across from the White House. And following Kennedy's assassination, Warnecke was asked to design the president's eternal flame and gravesite at Arlington National Cemetery. He also helped construct a new embassy complex in Washington for the Soviet Union, in which the Soviets claimed they found eavesdropping equipment embedded in the walls.

But it was not only governments that trusted Warnecke -- who died in 2010, aged 91 -- with major construction projects. He cultivated a close relationship with telecommunications companies, too, possibly helped by family ties to the industry. Warnecke's father-in-law had been a director at Pacific Bell, a California-based AT&T subsidiary. In the 1960s, Warnecke was asked to design a telephone

exchange building for Pacific Bell in Oakland. He would subsequently receive a series of other major commissions from AT&T: Aside from the 33 Thomas Street building, he also designed a telephone exchange in Williamsburg, Brooklyn, and an AT&T facility in Bedminster, New Jersey.

Some of Warnecke's original architectural drawings for 33 Thomas Street are labeled "Project X." It was alternatively referred to as the Broadway Building. His plans describe the structure as "a skyscraper to be inhabited by machines" and say that it was "designed to house long lines telephone equipment and to protect it and its operating personnel in the event of atomic attack." (At the time the building was commissioned and built, amid the Cold War, there were genuine fears in the U.S. about the prospect of a Soviet nuclear assault.)

It is not clear how many people work at 33 Thomas Street today, but Warnecke's original plans stated that it would provide food, water, and recreation for 1,500 people. It would also store 250,000 gallons of fuel to power generators, which would enable it to become a "self-contained city" for two weeks in the event of an emergency power failure. The blueprints for the building show that it was to include three subterranean levels, including a cable vault, where telecommunications cables likely entered and exited the building from under Manhattan's bustling streets.

After it was built, the unusual style of 33 Thomas Street attracted a lot of attention. Its dark, somewhat dystopian appearance contrasted dramatically with other buildings in lower Manhattan. Yet it proved popular, particularly among architecture buffs.

In a 1982 piece in the New York Times, architecture critic Paul Goldberger praised 33 Thomas Street as "one of the neighborhood's few pieces of good modern architecture," adding that it "blends into its surroundings more gracefully than does any other skyscraper in this area."

"Other telephone company buildings from that era, designed solely for equipment, all look like horrible boxes," Goldberger told The Intercept. "This one has an allure of its own to it. ... There's something about that shape. You see it and you don't see it at the same time."

In 1975, just a year after Warnecke's 33 Thomas Street building was completed, the NSA became embroiled in one of the biggest scandals in the U.S. intelligence community's history. Following revelations about domestic surveillance operations targeting anti- Vietnam War activists, a congressional select committee began investigating the alleged abuses.

The inquiry, led by Democratic Sen. Frank Church, published its findings in April 1976. It concluded that U.S. intelligence agencies had "invaded individual privacy and violated the rights of lawful assembly and political expression." Surveillance programs operated by the NSA through this period, it was later revealed, had targeted "domestic terrorist and foreign radical" suspects, including a host of eminent Americans, such as the civil rights leaders Martin Luther King and Whitney Young, the boxer Muhammad Ali, Washington Post columnist Art Buchwald, and New York Times journalist Tom Wicker.

The Church Committee recommended that new and tighter controls be placed on intelligence gathering. And in 1978, Congress approved the Foreign Intelligence Surveillance Act, requiring the executive branch to request warrants for spying operations from a newly formed court.

Through this tumultuous time for American spies, the NSA established a new surveillance program under the code name BLARNEY, which was first exposed in a Snowden-leaked slide published in 2013. According to a previously unpublished document provided to The Intercept by Snowden, BLARNEY was established in the early 1970s and, in mid-2013, remained one of the agency's most significant initiatives.

BLARNEY leverages "commercial partnerships" in order to "gain access and exploit foreign intelligence obtained from global networks," the document states. It carries out "full take" surveillance -- a term that refers to the bulk collection of both content and metadata -- under six different categories: counterproliferation, counterterrorism, diplomatic, economic, military, and political.

As of July 2010, the NSA had obtained at least 40 court orders for spying under the BLARNEY program, allowing the agency to monitor communications related to multiple countries, companies, and international organizations. Among the approved targets were the International Monetary Fund, the World Bank, the Bank of Japan, the European Union, the United Nations, and at least 38 different countries, including U.S. allies such as Italy, Japan, Brazil, France, Germany, Greece, Mexico, and Cyprus.

The program was the NSA's leading source of data collection under the Foreign Intelligence Surveillance Act, an April 2013 document disclosed, and information gleaned from the communications it intercepted was a top contributor to the president's daily briefing.

Notably, TITANPOINTE has played a central role in BLARNEY's operations. NSA documents dated between 2012 and 2013 list the TITANPOINTE surveillance facility among three of BLARNEY's "core sites" and describe it as "BLARNEY'S site in NYC." Equipment hosted at TITANPOINTE has been used to monitor international long-distance phone calls, faxes, voice calls routed over the internet (known as Voice-Over-IP), video conferencing, and other internet traffic.

In one case that may have involved 33 Thomas Street, NSA engineers with the BLARNEY program worked to eavesdrop on data from a connection serving the United Nations mission in New York. This spying resulted in "collection against the email address of the U.N. General leading the monitoring mission in Syria," an April 2012 memo said.

Mogens Lykketoft, former president of the U.N.'s general assembly, criticized the surveillance. "Such spying activities are totally unacceptable breaches of trust in international cooperation," he told The Intercept.

At the TITANPOINTE site, the NSA equipment is stored inside a secure room, known as a "Sensitive Compartmented Information Facility." Top-secret diagrams dated April 2012 show that within the

secure space there is "NSA controlled" equipment linked to the routers of its "access partner," referring to AT&T. Intercepted internet data was collected from the "backbone," then processed at TITANPOINTE, before being passed to NSA for storage. Phone calls that were intercepted were collected from TITANPOINTE's "foreign gateway switches" before being routed through the partner's "call processor." They were then forwarded to NSA's headquarters in Maryland through an interface shared with the partner.

Much of the surveillance carried out at TITANPOINTE seems to involve monitoring calls and other communications as they are being sent across AT&T's international phone and data cables. But the site has other capabilities at its disposal. The NSA's documents indicate that it is also equipped with powerful satellite antenna -- likely the ones located on the roof of 33 Thomas Street -- which monitor information transmitted through the air.

The SKIDROWE spying program focuses on covertly vacuuming up internet data -- known as "digital network intelligence" -- as it is passing between foreign satellites. The harvested data is then made accessible through XKEYSCORE, a Google-like mass surveillance system that the NSA's employees use to search through huge quantities of information about people's emails, chats, Skype calls, passwords, and internet browsing histories.

Fletcher Cook, an AT&T spokesperson, told The Intercept that the company does not "allow any government agency to connect directly to or otherwise control our network to obtain our customers' information. Rather, we simply respond to government requests for information pursuant to court orders or other mandatory process and, in rare cases, on a legal and voluntary basis when a person's life is in danger and time is of the essence, like in a kidnapping situation."

Cook added that NSA representatives "do not have access to any secure room or space within our owned portion of the 33 Thomas Street building." When pressed on whether any room within 33 Thomas Street contains equipment used for the purposes of NSA surveillance, an AT&T spokesperson pointed to a 1983 deed and declaration filed with New York City indicating that Verizon's predecessor company maintained ownership of three floors and a basement floor in the building. The New York City Department of Finance said the predecessor company has an easement for the space and pays utility taxes, but insisted that AT&T owns the whole building. The AT&T spokesperson declined to comment further.

The NSA's documents do not state that it can "connect directly to" or "otherwise control" AT&T's networks, but they do make clear that the agency has placed its own equipment inside TITANPOINTE to tap into phone calls and internet data. It may be the case that the secure room where the equipment is installed is overseen by AT&T's own engineers or technicians who have a security clearance. One NSA document dated from March 2013 suggests such a relationship, noting that the "corporate sites" the agency collects data from "are often controlled by the partner, who filters the communications before sending to NSA."

As in 1983, AT&T may not be completely alone at 33 Thomas Street. Earlier this year, a technician working at the building -- who did not want to be named because he was not authorized to speak to the media -- told The Intercept that a handful of Verizon employees were still based inside. However, the NSA's documents do not suggest that Verizon is implicated in the surveillance at the TITANPOINTE facility, and instead only point to AT&T's involvement. Verizon declined to comment for this story.

AT&T is far from the only company that has a relationship with the NSA. The agency has established what it calls "strategic partnerships" with more than 80 corporations. But some companies are more cooperative than others.

Historically, AT&T has always maintained close ties with the government. A good example of this came in June 1976, when a congressional subcommittee served AT&T with a subpoena demanding that it hand over information about its alleged role in unlawful FBI wiretapping of phone calls. President Gerald Ford personally intervened to block the subpoena, stating that AT&T "was and is an agent of the United States acting under contract with the Executive Branch." Ford said the company was in a "unique position" with respect to telephone and other communication lines in the U.S., and therefore it had been "necessary for the Executive Branch to rely on its services to assist in acquiring certain information necessary to the national defense and foreign policy." The details sought by the committee could not be shared, Ford asserted, because they could expose "extremely sensitive foreign intelligence and counterintelligence information."

In more recent decades, as the New York Times and ProPublica reported last year, AT&T has allowed the NSA to access billions of emails, exhibiting what the agency called its "extreme willingness to help." These revelations were foreshadowed in 2006 by allegations made by Mark Klein, a former AT&T technician. Klein stated that the company had maintained a "secure room" in one of its San Francisco offices, which was fitted with communications monitoring equipment apparently used by the NSA to tap into phone and internet traffic. Klein's claims formed the basis of a lawsuit brought by the Electronic Frontier Foundation on behalf of AT&T customers (Jewel v. NSA), which remains ongoing today.

Coincidentally, between 1981 and 1990, Klein also worked for AT&T at 33 Thomas Street. "I wasn't aware of any NSA presence when I was there, but I had a creepy feeling about the building, because I knew about AT&T's close collaboration with the Pentagon, going way back," he told The Intercept. When presented with the details linking 33 Thomas Street to NSA's TITANPOINTE, Klein added: "I'm not surprised. It's obviously a major installation. ... If you're interested in doing surveillance, it's a good place to do it."

According to the Snowden documents, AT&T has installed surveillance equipment in at least 59 U.S. sites. And on any given day, NSA employees may be working at the company's facilities. Classified memos dated from April 2013 describe one- to four-day deployments of NSA technical staff to TITANPOINTE and other buildings. Most AT&T personnel at these locations, however, are unlikely to have knowledge of the agency's presence. NSA staff are encouraged to wear clothes that make them "blend in to the environment." Even the car hire company the agency uses for its trips to AT&T facilities

is kept in the dark. "Some personnel are aware of the FBI link," states the agency's travel guidance, "but [they] have no knowledge of NSA's involvement."

Straits Times
Banks in Singapore must give cyber security high priority: ABS, ministry
Thursday, 17 November 2016
Byline: Rachael Boon

Singapore - Industry and government leaders on Thursday (Nov 17) urged financial institutions to step up cybersecurity efforts even as they seek innovation and digitise, at a technology risk conference by the Association of Banks Singapore (ABS) and the Monetary Authority of Singapore (MAS).
ABS chairman Wee Ee Cheong told the audience at the Sands Expo and Convention Centre that the focus is no longer just to defend against cyber threats, "but to respond promptly".

The idea is to use tools such as machine learning and big data analytics to aid in such efforts, "to be agile in responding to cyber threats" and move from being reactive in defence to being proactive.

Mr Aubeck Kam, Permanent Secretary of the Ministry of Communications and Information, said the Government is already working on its cyber security strategy, and hoped this would encourage financial institutions to deepen their own plans.

He noted that even as the industry embraces innovative fintech solutions, it has to give thought to keep security on top of the organisation's agenda, especially when the financial sector plays an important role here.

Jerusalem Post
Security expert: Pressure social media to block terrorist incitement
Thursday, 17 November 2016
Byline: Yonah Jeremy Bob

Jerusalem - Countries grappling with terrorists who use Facebook and Twitter to incite should unite together to formulate new international standards against such activity, INSS national security expert Col. (res.) Gabi Siboni recently told The Jerusalem Post.
Even national efforts in democratic countries to restrain terrorism and incitement via social media are only at their earliest stages, making Siboni's idea an innovative and potentially game-changing solution, though the challenges in accomplishing it are probably at least as great as the positive potential.

The INSS expert did emphasize that the initiative - what he calls fighting on the "cognitive warfare" plane - should be carried out in consultation with the leading social media giants.

His initiative is part of a larger multifaceted plan he is proposing for addressing the challenge of terrorists' brilliant use of online propaganda to hound Israel and the West.

Regarding Israel, he adds that a leading problem from Israeli adversaries, some linked to terrorists and some well-meaning human rights activists who downplay the challenge terrorism poses to Israel, is the power of social media to delegitimize Israel and "limit its freedom to act in self-defense."

Even if the media has delegitimized Israel's use of force in self-defense situations against terrorists (especially with television coverage of victims of IDF strikes), Siboni explains that social media has increased the breath of that delegitimization exponentially.

Besides using social media to delegitimize Israel, its right to self-defense and to encourage the worldwide Boycott Divestment and Sanctions campaign against Israel, he said that social media is also used to actively incite lone wolves into attacking Israelis.

These two distinct but related trends mean that terrorists are using social media to incite violence against Israel at the same time that human rights defenders are using it to limit Israel's ability to fight back.

Siboni said Israel has improved its efforts to counter suicide bombers and is beginning to improve tracking the social media pages of potential lone wolves in order to catch them before they act. Yet, he suggests Israel must act to proactively block terrorists' use of social media and to reduce the impact of incitement before it turns disgruntled but benign persons into lone wolf attackers.

At the same time, he explained that Israel must continue and double its efforts in the legal and public relations sphere to cope with the propaganda impact of social media delegitimization of Israel.

Specifically, he added that ways should be found where possible to go on the legal offensive against those trying to delegitimize Israel.

Returning to his idea of international efforts, he suggested that a paradigm-shift in how the top social media conceive of themselves and operate can be achieved far better with a united international front pressing media platforms to change and developing better technologies to deal with their drawbacks.

In order to coordinate all such efforts, Siboni said Israel must establish a new situation room for networking all of the military, intelligence, diplomatic, legal and public relations efforts, specifically fighting the negative impact of social media propaganda. He said coordination with Jewish organizations globally was also critical.

Part of the program would also include additional training for IDF commanders to be prepared for how social media can frame their activities and impact the IDF's overall ability to use force. Even as they may

already have some exposure to such issues, he implied that continued education regarding social media's evolving challenges is imperative.

Finally, he said, it is necessary for a surge in investing funds in developing new technologies to fully address these new challenges.

Jerusalem Post
Rafael seeks to bring Iron Dome technology to civilian market
Thursday, 17 November 2016
Byline: Anna Ahronheim

Jerusalem - Iron Dome might be known best for its precision in intercepting incoming rockets, but now one of the principal designers of the system is hoping to use that technology in the civilian market. Rafael Advanced Defense Systems subsidiary mPrest, located in Petah Tikva, is responsible for developing the algorithms that direct the missile defense system, but the underlying technology has a variety of other uses.

Now, with the increased threats posed by terrorism, including cyber terrorism, mPrest is hoping to use Iron Dome technology to protect government buildings and civilian infrastructure such as airports, major tourist spots, ports and other strategic installations.

mPrest is well known for their work in the field of command and control systems and already offers solutions for smart cities, allowing organizations to use its generic software platform to connect several sensors at any time with unrivaled flexibility and obtain real-time situational awareness.

New York State's Power Authority bought a system developed by mPrest which detects malfunctioning power transformers, automatically shutting them down or rerouting the power before they might cause larger problems on the electrical grid.

mPrest CEO and founder Col. (res.) Natan Barak told The Jerusalem Post that the company "comes with a new approach in how to manage the huge amount of data and sensors that thousands of organizations are using. We are giving total asset management to our clients for the process of increasing productivity, efficiency and energy as well as the safety and security of the organization."

Most importantly, Barak added, mPrest "gives our clients the power to change any rules in the system on a daily basis, in real time without the need to go through the whole development cycle again."

The asset management system was developed on the basis of the command and control system of Iron Dome, but uses a unique IoT (Internet of Things) platform interface with several sensors and systems. The system provides a "robust protection layer" which gives organizations full control and allows for a

lightning-fast response while controlling, processing, and transferring all the information to the appropriate authorities.

In a statement to the press, Barak said "IOT technology enables organizations to control many interfaces by placing sensors that monitor activity on a regular basis and produce an updated assessment of the situation at any given moment.

"The mPrest system will allow enterprises, cities and states to face the challenges in the coming years in terms of raising productivity, improving processes and boosting real-time information sharing between all officials and fulfilling tasks in the best way possible," Barak added.

Gulf News
Data of 34 million Keralites leaked in massive breach
Thursday, 17 November 2016
Byline: Mazhar Farooqui

Dubai - Confidential personal records of over 34 million residents in the Indian state of Kerala have been compromised in one of the biggest data breaches in the world.
The breach occurred last fortnight when an Indian man living in Tokyo hacked the Kerala government's civil supplies department website and uploaded the sensitive information of all of Kerala's 8,022,360 Public Distribution System (PDS) beneficiaries and their family members on Facebook.

The data reveals names, addresses, birth dates, gender, monthly incomes, electoral card details, consumer numbers of power and cooking gas connections. The massive leak has sparked fears that the information could fall into the wrong hands if it hasn't already.

A cyber security expert in Dubai fears the breach can have dangerous consequences. "The data could be used to duplicate SIM cards or reset net banking passwords. It's very serious." Tokyo-based IT consultant N.T.R. who hacked the website civilsupplieskerala.gov told XPRESS he took the extreme step to expose the security flaws in the site after attempts to draw attention towards them [weaknesses] fell on deaf ears. The website is designed, developed and hosted by India's National Informatics Centre (NIC).

"I wrote to the NIC several times pointing to the vulnerabilities and even called the civil supplies office warning them about a possible breach, but they ignored me. I had no option but to make the information public in a Facebook post," N.T.R., a native of Thiruvananthapuram, said from Tokyo.

He said breaking into the website was easy as the government had made a major gaffe by posting the entire list of PDS beneficiaries online.

Prepared as part of the Food Security Act 2013, the list was released just last month. According to reports, the Kerala government put the list online so that residents could verify their personal data and apply for corrections before new ration cards are printed in 2017.

"It was foolish on their part to put all ration card numbers on the website. All I had to do was make a data set of these numbers and then fetch the corresponding data for each number. It was simple as the security methods on the website were primitive. It took me just one week to access and transfer around 100GB of data. I am appalled no one raised the red flag despite the fact that I used the same IP address to make over 30 million requests," said N.T.R. Significantly, most servers block multiple requests originating from the same IP address.

The National (UAE)
Twitter to clamp down on abusive content following persistent criticism
Thursday, 17 November 2016
Byline: John Everington

Abu Dhabi - Twitter has announced new features to curb abusive content, as the social network seeks to increase advertiser engagement on its platform as a means of boosting profitability.
Twitter today said it was making it easier for users to report "hateful conduct" directed at them or others, had retrained its staff to better deal with improper conduct, and extended the service's "mute" function to include notifications of selected keywords, phrases and conversations.

"Twitter is an open public platform where the vast majority of people have a really positive experience," Bruce Daisley, Twitter's vice president for Europe the Middle East and Africa, said in a telephone interview today.

"Obviously some of the attention goes on the negative experiences, and that's why we're foc-using our energies on ensuring that we deal with the negatives so that the positives of an open platform like Twitter can benefit everyone."

Twitter has faced persistent criticism for not doing enough to curb racist, sexist and religiously motivated abuse on the platform.

Ghostbusters star Leslie Jones abandoned the platform temporarily in July after being inundated with racist and sexist hatred, with a large rise in online abuse in the run-up to this month's presidential elections.

Twitter's perceived failure to deal effectively with such abuse cases was reportedly a factor in suitors including Salesforce and Disney declining to submit bids for the company last month.

"There's no single platform that can say they've got everything right," said Mr Daisley. "We've set up a safety council and worked with a lot of users to try and understand what their big issues are."

"These battles are never won, but most people who look at our response and the way we deal with [online abuse] say we've made more progress in the last six months than we've done up to that point."

Newsweek
Donald Trump Can Either Continue the Shadow War With Vladimir Putin or End Sanctions
Thursday, 17 November 2016
Byline: Owen Matthews

New York - The telegram was one of the first to arrive from a world leader. On the morning of November 9, the Kremlin announced that Russian President Vladimir Putin had sent a message to U.S. President-elect Donald Trump expressing "his hope they can work together toward the end of the crisis in Russian-American relations, as well as address the pressing issues of the international agenda and the search for effective responses to global security challenges." Just minutes before, the Russian State Duma had erupted in applause when its members learned that Trump had won the election.
Putin appeared to be taking his lead from repeated comments Trump has made suggesting the two would get along: "I would treat Vladimir Putin firmly, but there's nothing I can think of that I'd rather do than have Russia friendly, as opposed to the way they are right now, so that we can go and knock out ISIS with other people," the then-candidate of the Republican Party said on July 28, referring to the Islamic State militant group.

But the blossoming bromance between the two men may come to a sudden end when Trump becomes commander in chief on January 20, 2017. That's when he will, on a daily basis, have to cope with a resentful former superpower engaged in an aggressive campaign of espionage and propaganda against the United States and its allies--one more intense and menacing than at any time since the Cold War. Trump will likely face a binary choice: continue to engage in that intensifying shadow war, as his predecessor chose to do, or end sanctions against Russia--essentially allowing Putin to expand his influence in Eastern Europe and beyond.

The pressure on Trump to come up with an answer will be considerable. In early November, Andrew Parker, head of Britain's internal security service MI5, became the first leader of the agency in 107 years to give an interview; the focus of his conversation with The Guardian newspaper was Russia's mobilization of "a whole range of state organs and powers to push its foreign policy abroad in increasingly aggressive ways: propaganda, espionage, subversion and cyberattacks." Russia's secret war involves everything from criminal sabotage to espionage to influencing news cycles, as well as supporting disruptive political movements and deep penetration of cyberinfrastructure. That's a lot for an American president who has never before held elected office to deal with on day one.

With Trump's victory, Russia might feel that its potent mixture of hacking, propaganda and sowing distrust has worked spectacularly well. The temptation to continue spreading chaos by backing right-wingers in France, the Baltics, Germany and elsewhere is stronger than ever. "Putin has interfered in our elections and succeeded. Well done," tweeted former U.S. Ambassador to Russia Michael McFaul after Trump's victory. And Russia's elite, while careful to deny involvement in the Kremlin's alleged meddling in the U.S. presidential race, is openly jubilant about Trump's win. "First was Brexit. Now Hillary," says Russian parliamentarian Vyacheslav Nikonov, a Putin ally. "A while ago, America was saying that Russia is just a gas station, a regional power. Now, apparently, we're so influential that we are determining the outcome of their presidential election. We follow the ancient Chinese policy--we sit on the riverbank and wait for our enemy's body to float past."

But Russia isn't just sitting and waiting. It is actively engaging its enemies, albeit in clandestine ways. The Kremlin's shadow war has intensified since Russia's annexation of Crimea in March 2014 and the international sanctions that followed. That was the moment it began to "define itself by opposition to the West and act accordingly," MI5's Parker told The Guardian. "Russia has been a covert threat for decades. What's different these days is that there are more and more methods available.... There is high-volume activity out of sight with the cyberthreat."

Russia has spearheaded some increasingly bold and sophisticated operations over the past year, including hacking attacks on Ukraine's power grid and the servers of the White House, the Democratic National Committee (DNC) and Germany's Bundestag that Western intelligence agencies believe came from Russia. Western governments are belatedly waking up to the scale of the threat and are readying the biggest counterespionage operation since the end of the Cold War. Spy agencies have pivoted with urgency. When the decades-long nuclear standoff with the Soviet Union and its allies came to an effective end with the demise of the Soviet empire in 1991, Western intelligence and security agencies largely turned their attention and resources elsewhere--especially to the Middle East and Afghanistan, as Islamist extremists' attacks appeared to become the greatest threat to the West. That challenge remains. But the Russian threat is back.

The Kremlin's new army of spooks is motivated by a single ideology-- to fight back against a supposed Western campaign to undermine Russian power and foment unrest and revolution in Moscow's backyard. Bizarre as this may seem to American and European observers, the majority of Russians--crucially, Putin and his inner circle--are convinced that the pro-democracy revolutions that swept Georgia, Ukraine and Kyrgyzstan in 2003 and 2004, the mass protests in Moscow against Putin in 2012 and the uprising in Kiev against pro-Moscow President Viktor Yanukovych were all part of a CIA-led conspiracy to weaken Moscow. "This is not just laughable rhetoric but an expression of a genuine belief," says Mark Galeotti, a senior research fellow at the Institute of International Relations in Prague. "When Moscow identifies all kinds of NGOs as 'foreign agents,' this is not only a convenient way to silence and marginalize critics. It also reflects a conviction that the West supports investigative journalists and anti- corruption movements in Russia not on their own merits but to undermine the regime."

Russia's spying operations, therefore, are justified as a part of a major pushback against perceived aggression. "You Americans meddled in our elections for years; now we meddle in yours. How do you like it?" wrote Ekaterinburg-based blogger Evgeny Smirnov in September. "You say we are influencing your politics with our propaganda. Yes--just as you taught us!"

Preventing further Russian meddling in American politics will become the problem of a president-elect whose true feelings about Russia, Putin and just about every other major policy area remain opaque. Sure, in the days following Trump's victory, Russia's television talk shows were full of clips of the president-elect's warm words about Putin. Trump called Putin a "stronger leader" than outgoing U.S. President Barack Obama and told ABC in July that "the people of Crimea, from what I've heard, would rather be with Russia than where they were." Asked by a reporter in July whether he would consider recognizing Crimea and lifting sanctions, Trump replied, "Yes, we would be looking at that," sparking jubilation in Moscow. Gennady Zyuganov, veteran leader of Russia's Communist Party, tells Newsweek he sees Trump as "a candidate of peace, not war, who will respect the interests of Russia and stop [the last administration's] aggressive encroachment on our borders."

But Trump has also blasted Putin. "Russia took Crimea during the so-called Obama years," Trump tweeted in September. "Who wouldn't know this, and why does Obama get a free pass?" And Russia's optimism about the end of sanctions is also misplaced; His "Yes, we would be looking at that" response is, as many reporters pointed out, just a line Trump often uses to move on to the next question. Russian hackers may have helped Trump to victory. But if and when Trump disappoints the Kremlin--perhaps by bowing quickly to congressional Republicans' strong support for Ukraine in its fight against Russian-backed separatists--the 45th president of the United States could find himself facing off against the same ruthless adversary in Moscow who made life so hard for the 44th. And the 43rd. And the 42nd.

Hybrid Warfare

If Trump is looking for a reminder of the real-world damage Putin's online special forces can cause, he might want to ask the CIA for a briefing on a cyberattack that began on December 23, 2015. A winter's early dusk was falling over the Ivano-Frankivsk region in western Ukraine when Russian hackers took control of the electricity grid. Controllers at the headquarters of the local energy utility, PrykarpattyaOblEnergo, watched helplessly as they were locked out of their computers. Cursors began operating on their own, clicking circuit breakers in the utility's central command system, shutting down electricity substations one by one. Within half an hour, 700,000 residents, as well as hospitals and schools, were without power. That marked the start of the biggest and most sustained cyberattack against any nation ever conducted. Over the following nine months, according to the Ukrainian Security Service, hackers made more than 15,000 other attempts to sabotage Ukraine's critical infrastructure, from the control systems at Kiev's Boryspil International Airport to the country's Central Election Commission. So far, nobody has died as a result of the cyberassault--but the attacks proved the hackers could shut down operating rooms and airports at will.

"A clear Rubicon was crossed," says Alexander Klimburg, senior fellow at the Atlantic Council think tank in Washington and author of the upcoming book The Dark Web, which describes how future conflicts will be fought over the internet. "Cyberweapons have officially joined the arsenal of modern warfare."

Putin has apparently tasked Russia's securocrats with doing what Soviet spies dreamed of but could never achieve--fighting a war of covert disruption in parallel to their more traditional role, straight intelligence-gathering. The strategy is laid out in the latest version of Russia's official military doctrine. A key task of modern so-called hybrid warfare is "the prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favorable response from the world community to the utilization of military force." To that end, all the state's resources--led by Russia's security services--are responsible for "developing forces and resources for information warfare."

Aric Toler, an American researcher at the activist group Bellingcat, has been on the receiving end of that information war machine. Founded by British blogger Eliot Higgins in 2014, Bellingcat has used open-source material, such as social media posts and YouTube video footage, to expose Russian troops operating illegally in eastern Ukraine and, most controversially, to precisely track the course of a Russian Army BUK rocket launcher that shot down Malaysian Airlines Flight 17 over eastern Ukraine on July 17, 2014. It was Russia's involvement in the shooting down of MH17 and its subsequent stonewalling over the investigation that became the main focus of biting EU and U.S. sanctions on the Russian economy--not, as Russia often claims, its annexation of Crimea. Moscow has continued to deny its BUK rockets were involved--blaming the crash on, variously, Ukrainian jets or Ukrainian surface-to-air missiles. But Bellingcat's evidence, from dozens of sources tracking the BUK's progress into and out of eastern Ukraine on that fateful day, is more than just the work of internet geeks. Official Dutch and Malaysian investigators are using it to draw up formal charges against the Russian soldiers and officials responsible. The British bloggers have exposed attempts to cover up the truth on MH17--and in the process helped deny the Russian economy billions of dollars in investment. No wonder the Kremlin appears to have gone after Bellingcat with such ferocity.

Over the past 18 months, Toler has regularly received phishing emails containing viruses that would allow hackers to access his computer--if any of us were dumb enough to click on the links." More threatening, over the summer pro-Russian online activist group CyberBerkut hacked into the emails of Ukrainian government officials and used the information to smear Toler by alleging he is linked to the Kiev government. Finally, Russian state-sponsored TV channels, like Russia Today and Sputnik, keep up a regular stream of invective against Bellingcat's work, while a small army of trolls on Twitter and social media are busy denouncing it on an hourly basis.

"We've been targeted by the full force of the Russian information machine," says Toler. "We can't say for sure if these are Russian government or proxy groups...but the phishing emails [we received] are the same as those which targeted the Democratic National Committee."

In June, Russian hackers gained international notoriety by breaking into the email database of the DNC and releasing emails embarrassing to Hillary Clinton. The hacker groups behind the break-in, APT 28 and APT 29 (or more snappily nicknamed Cozy Bear and Fancy Bear by U.S. cybersecurity companies) are in fact two operations linked, respectively, to Russia's Federal Security Service, or FSB, and Russian military intelligence, or GRU. James Clapper, the U.S. director of national intelligence, has launched an investigation into alleged Russian operations against the U.S. presidential election.

The incoming American president would do well to consider that while the DNC hack might have helped him during the election campaign, Fancy Bear and Cozy Bear later showed they have a broad range of targets. In September, the groups were linked to the release of sensitive data stolen from the World Anti-Doping Agency that revealed that several top Western athletes--including U.S. tennis stars Venus and Serena Williams--had been given exemptions for taking prohibited drugs during the Olympics, while a swath of Russian athletes had been banned for illegal drug use. Later that month, the groups leaked emails from General Philip Breedlove, NATO's former supreme allied commander for Europe, that suggested his dissatisfaction with some European allies and then released first lady Michelle Obama's passport and sensitive travel information from the White House. To cap off a busy U.S. election season of hacking, Fancy Bear in October leaked a series of emails from former Secretary of State Colin Powell in which he allegedly said, "I would rather not have to vote for [Hillary]" and described Clinton as having "a long track record [of] unbridled ambition, greedy, not transformational."

It's enough to make an incoming president and his aides wonder whether the Kremlin is already reading in on the transition plans.

Crooks and Spooks

If Russian hackers launch fresh attacks on the U.S. after January, the new president will likely face flat denials of involvement from the Kremlin--and he and U.S. intelligence officials will struggle to provide evidence to back up their claims of state involvement, say Western intelligence sources and computer security experts. That's because Russia's spies have formed an alliance with the country's notorious cybercriminals--and the spooks use the crooks as cover. "At least half" of the Kremlin-backed hackers' arsenal "is derived from cybercrime, perhaps much more," says internet security expert Klimburg. The partnership between Russian criminals and Russian spies goes back as far as 2007, when hackers known collectively as the Russian Business Network deployed computers they had infected with Trojan horse viruses and turned them into a network of zombified machines known as botnets to bombard and shut down internet servers in Estonia. The attack was apparent punishment for Estonia taking down a monument to a Red Army soldier. Just as with the DNC hack, the Kremlin indignantly denied responsibility. But subsequent investigations linked the attack to, variously, the pro-Kremlin youth group Nashi and a former parliamentary aide. A clear chain of command was never established-- but the pattern was: The cybercriminals had become the Kremlin's cyber hatchet men.

"It's not unprecedented for governments to use criminals to do their dirty work. Back in the day, [French President Charles] de Gaulle used the Corsican Mafia against the [ultranationalist] OAS; the CIA used the

Italian Mafia against the Cubans," says a senior U.K. security official not authorized to speak on the record. "But most of us thought that kind of thing has been left behind with the Cold War--along with poisoning defectors and the like. We've been proved quite wrong on both counts."

In October, a Russian hacker was arrested in Prague on an Interpol warrant issued after an investigation by the FBI. Identified by Czech police only as Yevgeniy N., the hacker was busted for his involvement in a massive 2012 break-in at LinkedIn, a company spokesman told Reuters, which compromised the credentials of 100 million users, prompting the company to launch a massive password reset operation. According to one cyberexpert who advises Western governments, Yevgeniy N. is of special interest to law enforcement because of suspicions that the information he gathered during his hacking career "cropped up in later hacks that we believe are clearly [Russian] state- sponsored."

Multiple spy agencies are involved in Russia's full-spectrum assault--and some of them are growing rapidly. The FSB is Russia's largest security agency--and will, according to a document leaked to the Russian Kommersant Daily in September, soon become larger, thanks to its plan to create a new super-ministry of state security. The Kremlin's Presidential Administration is the most influential agency involved in Russia's shadow war, says Galeotti, coordinating traditional spies controlled by Russia's External Intelligence Service, or SVR, alongside propaganda operations run by state-funded media outlets, such as Sputnik and the RT English-language television news channel, formerly Russia Today, which is available to 700 million people in more than 100 countries around the world. The SVR's headquarters, in the Yasenevo district of Moscow, has doubled in size since 2007, as images posted online by transparency activist Steven Aftergood of the Federation of American Scientists' Secrecy News blog clearly show.

And it's not just computer geeks who are filling the desks and offices inside. Russia's old-school spies are working to undermine the West as much as, if not more than, their Soviet predecessors. According to John Bayliss, a former official at Britain's electronic surveillance agency, the Government Communications Headquarters (GCHQ), "There are more Russian intelligence agents [in the U.K.] now than at the height of the Cold War."

The chief analyst of Sweden's SAPO intelligence service, Wilhelm Unge, warned in October that a third of all Russian diplomats stationed in Sweden are intelligence officers, far more than during the 1980s, and that Russia constitutes "the biggest intelligence threat against Sweden." In May, a Warsaw military court convicted a Polish army lieutenant-colonel for passing information about soldiers with disciplinary problems to a Russian handler (prosecutors claimed that servicemen in trouble with the authorities were easier to recruit). In October, Montenegro's long-serving, pro-Western prime minister, Milo Djukanovic, claimed he'd been the victim of an attempted coup with a "strong foreign connection." Montenegro's security forces arrested 20 Serbs and Montenegrins on October 16, and Serbian Prime Minister Aleksandar Vucic confirmed that the men arrested in Montenegro had hatched their coup plot in Serbia, assisted by Russian intelligence. An indignant Vucic said he would not allow his country to "act as the puppet of world powers."

There's no proof linking the Kremlin to the Montenegrin coup plotters--but there is plenty of evidence that there has been a major uptick in Russian efforts to meddle in the internal politics of a range of European countries. Last month, the Czech Republic's BIS intelligence agency accused Russia of not just spying but also of "creating or promoting inter-societal and inter- political tensions" in the country, including covert support for domestic extremist and populist organizations that "tend to hold consistently pro- Russian stances on domestic and international issues. They are also highly critical of NATO and the EU, and promote the view that, like Britain, the Czech Republic should seek to exit the EU." Czech intelligence's annual report caused a sensation when it was published in September, because it stated bluntly that the Kremlin's aim was to "destabilize or manipulate Czech society at any time, if Russia wishes to do so."

Moscow has also been actively reaching out to France's National Front, whose anti-immigrant, anti-EU leader, Marine Le Pen, has become a hero on Russian media. The National Front confirmed that it had borrowed 9 million euros from the Moscow-based First Czech Russian Bank in 2014, while in February of this year the party's treasurer, Wallerand de Saint-Just, made no secret of the fact that he was seeking up to 23 million euros from "any other" Russian banks that would be willing to stump up. At a private pro-Trump election party I attended in an English-themed pub in downtown Moscow, three specially commissioned portraits stood in pride of place: Trump, Putin and Le Pen. Le Pen has called for sanctions on Russia to be lifted and for a deal to build two Mistral-class warships for Moscow--blocked by French President François Hollande under strong U.S. pressure in the wake of the Crimea annexation--to go ahead.

"We are entering a new era of politics," says political scientist Sergei Mikheyev. "Europe will be free to think for itself instead of obeying Washington's Russophobia. Le Pen is a patriot who is ready to defy American diktat."

Le Pen will be a candidate for the French presidency in the spring of 2017. She is expected to do well--but, like Trump at a similar stage of the electoral cycle, nobody is expecting her to win.

Best Frenemies

The West is starting to fight back against the Putin threat--and Trump will find himself in charge of the effort to combat the man he has called "very much a leader." This month, the U.S.'s most important ally--the U.K.--announced a new £1.9 billion national cybersecurity strategy designed to develop what Finance Minister Philip Hammond called a "fully functioning cyberattack capability" to be able to "match the cyberattack abilities of foreign rogue states." Britain is opening a new cyberinnovation center and scaling up its security services by recruiting 1,900 additional staff. And intelligence agency MI6, which employs around 2,500 people, is set to receive over half of those new personnel. "The areas of expansion are obviously internet resources like social media, plus the use of facial recognition technology," for intelligence gathering, says one former Secret Intelligence Service staffer with knowledge of the expansion plans. "The emphasis has changed from just running agents like in the

past." But even with the new recruits, Russia will have more than six intelligence officers for every British spook, according to Bayliss, the former GCHQ officer.

There's also been a scramble across Western intelligence services to recruit and train Russian experts. For the first time since the Soviet Union's collapse in 1991, the U.S. has diverted resources from counterterrorism to counterespionage to push back against Russia, according to Evelyn Farkas, a top Russia official at the Pentagon until his retirement in 2015. "The Russia beat for intel folks was a more quiet one, frankly speaking, over the last couple decades," Farkas told NPR recently. "And now it's quite hot. And we have to find linguists. We have to find people who can analyze all the information that we have to find coming in, in Russian and other languages."

Trump is unlikely to ask America's intelligence agencies to give up recruiting Russian-speakers and let Putin have his way. And it's entirely possible that by the time he is inaugurated, the new president will have concluded that the affinities he shares with Putin are really only slogan-deep. Both may harbor a strong nostalgia for postwar glory days when, as Trump told an interviewer in March, "we were not pushed around. We were respected by everybody. We had just won a war." Both may espouse social conservative rhetoric, claim a distrust of educated elites and rely on the support of the American and Russian working classes. But in the Venn diagram of American and Russian interests, there's not a huge overlap.

Moscow is trying to disrupt and fragment Europe, but it's in the U.S.'s interest to keep Europe prosperous, united and at peace. In Syria, Russia would like to demonstrate that its military and diplomatic support can keep despotic client leaders like Bashar al-Assad in power--while the U.S. has always insisted that Syria must have democratic elections that include all non-jihadi opposition groups. The Kremlin would like to once again make Ukraine a client state--or, failing that, cripple the country by sponsoring an ongoing civil war to prevent it from joining the EU and becoming a post-Soviet success story. But congressional Republicans--working in parallel with the Obama White House-- have always strongly supported the struggle of what Senator John McCain calls "the captive nations" against their former Russian overlords.

And then there's the Baltics, a corner of northeastern Europe Trump may not have spent much of his career thinking about. It's in the Baltic states of Estonia, Latvia and Lithuania--all once constituent parts of the U.S.S.R. with large ethnic Russian populations--that Trump's potential chumming up with Putin could have its first tragic consequences. Trump has called NATO "obsolete and extremely expensive" and has suggested he would not honor NATO members' commitments on collective defense unless other alliance members pay their fair share. If he repeats that rhetoric, let alone implements it, Putin could order his troops or local proxy forces to attack or destabilize the Baltic states--all of them members of NATO--under the pretext of protecting fellow ethnic Russians. "I really hope that the rhetoric on defense and Russia was mostly a part of the election campaign," Saulius Skvernelis, Lithuania's incoming prime minister, said in an interview with Reuters on November 9. "I hope the election campaign is now over and it is not yet time to panic."

The coming months will likely show Skvernelis whether his hopes are justified. If he gets lucky, he'll watch the former reality-TV star rapidly figure out who America's allies are--and how important it is to protect pro-American countries like Lithuania. "It is a very imperfect world, and you can't always choose your friends," Trump said in September. "But you can never fail to recognize your enemies."

The next president has only a few more weeks to figure out whether Putin is a friend or a foe.

Associated Press
China doubles down on internet control after tough new law
Thursday, 17 November 2016
Byline: Gerry Shih

Beijing - China's leaders and official media are pushing for greater control of the internet and technology products as tensions surrounding a far-reaching Chinese cybersecurity law loom over a gathering this week of the world's leading tech firms and Chinese officials.
The Communist Party's mouthpiece People's Daily warned in an editorial on Thursday that China must break monopolies over core technologies and standards and remain untethered to other countries' technology supply chains.

The commentary, aimed apparently at Silicon Valley in unusually stark terms, comes one day after President Xi Jinping called for "more fair and equitable" governance of the internet at the opening of the state-run World Internet Conference. Since 2014, China has hosted executives from the likes of Microsoft, Apple, Facebook and Alibaba in eastern China to promote its vision of an internet that is more tightly controlled by national governments rather than running unchecked as a transnational network.

The conference this week has highlighted U.S. and China's competing and increasingly entrenched views about the internet, trade and cybersecurity, and the potential for these issues to become an enduring irritant in bilateral relations.

Xi reiterated on Wednesday the Chinese position of "internet sovereignty" over its 700 million Internet users, while other top leaders declared the country's willingness to work with the global industry for mutual benefit -- if security could be assured on China's terms.

Earlier this month, China passed a broad cybersecurity law that gives law enforcement greater powers to access private data and requires data to be stored locally on Chinese servers. Human rights groups have voiced concern about police overreach while U.S. firms have lobbied against the measure, saying it would wall off China's internet and unfairly hamper their access to the market.

Other Chinese proposals in recent years have effectively discouraged state-backed companies and agencies from buying foreign products out of cyber-spying concerns. China has also encouraged its

state-backed sector to develop -- or outright acquire -- technologies in strategically critical industries like semiconductors, which it believes to be an Achilles heel of the Chinese economy. Recent efforts to acquire U.S. chip companies have been rebuffed by U.S. regulators on national security grounds.

Foreign technology trade groups say the regulations have used security as a pretext for enacting protectionist trade policies to benefit China's tech industry, and more than 40 groups signed a letter to Communist Party cyberspace officials last week urging China to respect its World Trade Organization commitments.

"We are concerned that these commitments are undermined by public statements and other forms of high-level guidance that call for indigenous and controllable substitution plans for information technology products and services," the trade groups said, while acknowledging that China faced "legitimate security concerns."

Beijing has said the internet has been overwhelmingly dominated by the United States and it has backed a proposal to transfer control over some of the internet's core architecture to a U.N agency, the International Telecommunication Union.

Critics, however, objected to letting authoritarian regimes like Iran and China get equal votes on matters affecting speech. The U.S. government in September privatized control over the systems by transferring them to a nonprofit oversight organization.

The People's Daily made clear in its editorial on Thursday that China needed to avoid dependence on foreign firms "particularly by breaking monopolies over core technologies and standards and not allowing other countries to control vital supply chains."

Les Echos
ADP veut réduire l'attente aux contrôles de police
Thursday, 17 November 2016
Byline: Bruno Trévidic

Paris - Le groupe ADP va financer le déploiement d'une nouvelle génération de bornes de contrôle automatisé des passeports.
Devant l'allongement des files d'attente aux guichets de la police aux frontières (PAF), à Roissy, Paris Aéroports s'est finalement résolu à mettre la main à la poche, pour tenter de remédier à une situation de plus en plus cauchemardesque pour les passagers. En l'absence de moyens supplémentaires émanant du ministère de l'Intérieur, le groupe ADP va financer à 100 % l'installation d'une centaine de nouvelles bornes Parafe de contrôle automatisé des passeports, a annoncé mercredi son PDG, Augustin de Romanet, lors d'une rencontre avec la presse.

Avec le renforcement des contrôles aux frontières, suite aux attaques terroristes, la durée de l'attente est devenue le principal motif de mécontentement des passagers débarquant à Roissy. Au contrôle systématique de tous les passagers, français et étrangers, entrant dans l'espace Shengen se sont en effet ajoutés des contrôles aléatoires à l'arrivée de certains vols au sein même de l'espace Shengen. Le tout sur fond de manque chronique d'effectifs à la PAF que ne compensent pas les actuels sas Parafe, peu nombreux, trop lents, souvent en panne et réservés aux détenteurs de passeports français biométriques.

« Depuis le début de l'année, les temps d'attente de plus de trente minutes ont été multipliés par 20 » , déplore Augustin de Romanet. De quoi ruiner tous les efforts d'ADP pour améliorer l'accueil des passagers et l'image de l'aéroport de Roissy-CDG et convaincre plus d'un touriste étranger de choisir un autre point d'entrée en Europe.

Passeports biométriques

Après avoir tenté, sans succès, d'obtenir de l'Etat des moyens supplémentaires, le PDG du groupe ADP a donc jugé préférable de lancer sans plus attendre un appel d'offres, remporté par Gemalto. Ces nouveaux portillons, différents des actuels sas Parafe, peu nombreux, peu fiables et trop lents, devraient être déployés dans le courant du premier semestre, à l'issue d'une période de test qui débutera le mois prochain. Ils devraient être accessibles à tous les passagers français munis de passeports biométriques, mais peut-être aussi à tous les autres ressortissants de l'Union européenne, à l'instar de ce qui se fait déjà dans d'autres grands aéroports européens comme Londres- Heathrow.

A condition toutefois que l'administration française accepte de valider le système de reconnaissance faciale, basée sur la photo du passeport. Car, pour l'heure, la réglementation française ne reconnaît comme valide que le contrôle des empreintes digitales.

Radio-Canada Nouvelles
À l'école des cybersoldats
Tuesday, 22 November 2016
Byline: Raphaël Bouvier-Auclair

Avec les menaces de cyberattaques qui ne cessent de se multiplier et d'évoluer dans leur forme, les Forces armées canadiennes veulent augmenter considérablement leurs ressources pour bien se défendre. Nous sommes allés visiter des classes où sont formés des militaires armés de claviers. Des fils et des écrans qui débordent de codes. Nous sommes loin des images qui nous viennent habituellement en tête quand on pense à des exercices militaires.

Pourtant, dans cette classe du Collège militaire royal du Canada, à Kingston, sont formés certains des soldats de demain.

Le collège offre un programme de génie électrique et informatique au premier cycle et aux cycles supérieurs. Des programmes qui ont été affinés et qui ont gagné en popularité au cours des dernières années.

Au premier cycle par exemple, l'un des cours de cyberdéfense se termine avec un stage de deux semaines organisé par l'agence américaine National Security Agency (NSA).

Francis Langlais, élève-officier de premier cycle au Collège militaire royal, à Kingston. Photo : CBC / Radio-Canada / Raphaël Bouvier-Auclair

L'élève- officier Francis Langlais est inscrit au programme de premier cycle.

J'ai fait un diplôme en jeu vidéo avant. Ça m'intéressait beaucoup. Mais j'ai décidé de faire autre chose, aussi en informatique. S'il n'y avait pas le côté cyber dans les Forces, ça m'aurait beaucoup moins intéressé.

Francis Langlais, élève-officier au Collège militaire royal

Apprendre à attaquer

Si, au premier cycle, l'apprentissage est beaucoup plus concentré sur la création de réseau et la cyberdéfense, certains cours des cycles supérieurs vont beaucoup plus loin. Il y a, par exemple, le cours qui s'intitule menaces et techniques d'attaque cybernétiques.

Au menu : craquage de mots de passe, virus, etc. En lisant la description, on croirait consulter le guide du parfait pirate informatique.

En ce moment, les Forces armées canadiennes doivent se concentrer sur la cyberdéfense et n'ont pas pour mandat de mener des attaques.

N'empêche, pour l'instructeur au Collège Guillaume Vigeant, apprendre certaines techniques d'attaque est essentiel.

On ne peut pas dire à un soldat : "ne fais qu'encaisser les coups". Il faut savoir comment attaquer pour savoir comment bien se défendre.

Guillaume Vigeant, instructeur au Collège militaire royal de Kingston

En classe, les étudiants analysent des menaces en se basant sur des cas d'actualité. Ils se penchent, par exemple, sur l'utilisation de cyberattaques dans certains conflits, notamment en Ukraine et en Irak. Le ver informatique Stuxnet, qui a paralysé des centrales iraniennes en 2010, est aussi un cas discuté.

Loin des stéréotypes

L'instructeur Guillaume Vigeant pendant un cours de cycle supérieur. Photo : CBC / Radio-Canada / Raphaël Bouvier-Auclair

L'instructeur Guillaume Vigeant en convient, sa classe est formée de nombreux « geeks », des maniaques de l'informatique.

« C'est un style de soldats qu'on n'est pas habitué d'associer au stéréotype de soldat », explique-t-il.

Son collègue, le professeur Sylvain Leblanc, précise qu'il n'y a là rien de nouveau. Plusieurs ingénieurs font déjà partie des rangs de l'armée ainsi que de la marine et de l'aviation royales.

Je ne pense pas que ce soit quelque chose de nouveau. Historiquement, il y a beaucoup de développement que l'on utilise aujourd'hui, dans le transport, dans les télécommunications, qui ont été développés par des gens intelligents en uniforme.

Sylvain Leblanc, professeur agrégé au département de génie électrique et génie informatique au Collège militaire royal

Dans un contexte où les bombes et les armes ne suffisent plus pour défendre les frontières canadiennes, les débouchés sont intéressants pour les étudiants de génie informatique à Kingston.

D'ailleurs, les Forces armées entendent créer dès l'an prochain un nouveau métier, celui d'opérateur cybernétique, qui sera uniquement dédié à la protection des réseaux.

Radio-Canada (Le Radiojournal)
Cyberattaque contre les Forces canadiennes : un nouveau métier verra le jour
Tuesday, 22 November 2016
Byline: Isabelle Poulin

Montréal - Les forces canadiennes intensifient leurs efforts dans la cyberdéfense.
BRIG.-GÉN. FRANCIS ALLEN (FORCES CANADIENNES) :

Il y a des adversaires qui veulent exploiter des vulnérabilités. -

Bonsoir, ici Isabelle Poulin, à Montréal. L'attaque qui a visé le site Internet de recrutement des Forces canadiennes, la semaine dernière, rappelle que le Canada demeure une cible dans le cyberespace. Le gouvernement Trudeau est en train de revoir sa politique de défense et Radio-Canada a appris qu'entre-temps les forces vont créer un nouveau corps de métier qui sera uniquement consacré à la cyberdéfense. Voici Raphaël Bouvier-Auclair.

RAPHAEL BOUVIER- AUCLAIR (REPORTER) :

Le constat des Forces canadiennes est sans équivoque. Les bombes et les fusils ne suffisent plus pour défendre le Canada. La brigadière-générale Francis Allen.

BRIG.-GÉN. FRANCIS ALLEN (FORCES CANADIENNES) :

Il y a un changement dans la menace. Maintenant, il y a des adversaires, des acteurs non étatiques qui veulent exploiter des vulnérabilités.

RAPHAEL BOUVIER-AUCLAIR (REPORTER) :

Pour l'instant, les Forces disposent de 200 personnes pour assurer la protection de leur réseau. Le nombre doit plus que doubler d'ici quatre ans, et dès l'an prochain, un nouveau métier très spécialisé, opérateur cybernétique, verra le jour. D'ailleurs, au Collège militaire royal, à Kingston, on forme ces soldats de demain. Dans des salles remplies de claviers et d'écran, des étudiants presque tous en uniforme assistent à des cours de premier et de deuxième cycle en génie informatique. Francis Langlais est du nombre.

FRANCIS LANGLAIS (ÉTUDIANT, COLLÈGE MILITAIRE ROYAL DE KINGSTON) :

Défendre le territoire canadien ou tout autre territoire physiquement, c'est important, mais s'il y a de l'information qu'on veut protéger est perdu, le domaine physique est compromis aussi.

RAPHAEL BOUVIER-AUCLAIR (REPORTER) :

À Kingston, on enseigne non seulement la défense, mais aussi les cyberattaques, des opérations que les forces ne sont pas autorisées à lancer en ce moment. L'ancien directeur du Service canadien du renseignement de sécurité, Richard Fadden, croit que cela devrait être envisagé, mais avec prudence.

RICHARD FADDEN (ANCIEN DIRECTEUR DU SCRS) :

Si on n'aime pas se faire attaquer, il faut se demander quelle va être la réaction des autres quand on attaque.

RAPHAÀL BOUVIER-AUCLAIR (REPORTER) :

L'option est sur la table. Le gouvernement Trudeau est en train de revoir les stratégies canadiennes de cybersécurité et de défense. Ici Raphaël Bouvier-Auclair, Radio-Canada, Ottawa.

Radio-Canada (Nouvelles)
Un nouveau métier au sein des forces armées pour se protéger des cybermenaces
Monday, 21 November 2016
Byline: Raphaël Bouvier-Auclair

Ottawa - La menace de cyberattaques est de plus en plus présente et les Forces canadiennes veulent mieux y répondre. Radio-Canada a appris qu'à partir de l'année prochaine, un nouveau corps de métier totalement consacré à la cyberdéfense sera créé au sein de l'armée.
Le risque de cyberattaques a de nouveau été exposé au grand jour la semaine dernière. Même si l'origine du problème demeure inconnue, le site de recrutement des Forces canadiennes a été ciblé jeudi.

Lorsqu'ils tentaient d'y accéder, les internautes étaient redirigés vers une page du gouvernement chinois. Par la suite, le site de recrutement des Forces est demeuré inaccessible pendant plusieurs jours.

Pour protéger les frontières virtuelles du pays de ce genre d'incident, les Forces canadiennes sont en train de développer un nouveau métier qui verra le jour l'an prochain.

Selon nos informations, les futurs opérateurs cybernétiques devront entre autres tester la vulnérabilité des réseaux, analyser les incidents liés à la sécurité et protéger les actifs informatiques.

Pour l'instant, ce sont surtout des ingénieurs et des techniciens qui sont responsables de la cyberdéfense au sein des forces.

Actuellement, 202 personnes assurent ce service. D'ici quatre ans, ce nombre doit passer à 429, notamment grâce à l'arrivée des opérateurs cybernétiques.

Attaquer ou non?

Au Canada, l'armée a pour fonction d'assurer la défense des réseaux, mais n'est pas autorisée à mener d'attaques. Ailleurs dans le monde, certains pays comme la Chine, la Russie et les États-Unis participent à des attaques dans le cyberespace.

Puis il y a des organisations terroristes comme Daech (connue aussi sous le nom de groupe armé État islamique).

Les possibilités qu'offre Internet sont quasi infinies. Prise de contrôle de sites hostiles, contrôle de réseaux électriques... Dans ce contexte le Canada devrait-il être autorisé lui aussi à aussi mener des assauts?

L'ancien directeur du Service canadien du renseignement de sécurité (SCRS) Richard Fadden y est favorable, mais croit qu'il faut avoir une discussion nationale sur le sujet puisque, selon lui, mener des cyberattaques vient avec son lot de risques.

Pour le professeur Thomas Keenan, chercheur associé à l'Institut canadien des affaires mondiales, les Forces canadiennes auraient tout à gagner à se concentrer sur la défense. Selon lui, ce qui s'est produit sur le site de recrutement de l'armée est la preuve qu'il y a encore du travail à accomplir.

Quant à mener des cyberattaques, Thomas Kennan souligne les risques qu'il y a à se frotter à des forces plus développées que les nôtres.

Il revient au gouvernement de Justin Trudeau de décider si les Forces canadiennes doivent développer une force de frappe dans le cyberespace. Un examen de la politique de défense est en cours en ce moment.

Au Canada, il n'y a pas que la Défense nationale qui est responsable d'assurer la cybersécurité. Le ministère de la Sécurité publique et des agences comme le Centre de la sécurité des télécommunications ont aussi un rôle important à jouer.

Sputnik
Russia, China Target Canada's Classified Data - Security Intelligence Service
Monday, 21 November 2016

Washington - Russia and China have been targeting Canada's classified information and official persons, the briefing notes for Canadian Security Intelligence Service (CSIS) Director Michel Coulombe claimed on Monday.

CSIS spokeswoman Tahera Mufti explained that "a number of foreign states" have sought to obtain political, economic and military information in Canada.

"Russia and China, in particular, continue to target Canada's classified information and advanced technology, as well as government officials and systems," the briefing notes, obtained by the Canadian Press through an Access to Information Request, said. "States and other entities abroad have interests... and will pursue those interests by a variety of means," Mufti told the Canadian Press. "Some will do so through espionage and interference, targeting the Canadian economy, strategic interests and assets, societal institutions and members of the diaspora." In October, US authorities accused Russia of trying to interfere with the election process in the United States by breaching of the Democratic National Committee (DNC) email servers, but have offered no proof to back their claims. Russian officials have denied the allegations, calling them absurd and further stating Moscow does not want to interfere in or attempt to influence the US elections.

ABC (Australia)
Superannuation funds vulnerable to terrorist funding and money laundering abuses: AUSTRAC
Tuesday, 22 November 2016
Byline: Stephen Letts

Canberra - Financial intelligence agency AUSTRAC has found evidence Australia's $1.3 trillion superannuation pool may be being used to fund terrorism activities and remains vulnerable to criminal exploitation.
A two-year study of so-called "suspicious matter reports" (SMRs) by AUSTRAC found 19 reports related to potential terrorism funding, with transactions totalling almost $260,000.

However, AUSTRAC pointed out the study, conducted with the Australian Federal Police, Australian Crime Commission and Australian Taxation Office, may have significantly under-reported the problem given just five funds reported more than half of all SMRs.

The study -- conducted over 2014 and 2015 -- found terrorism financing is a small but emerging and serious threat.

"There is evidence foreign terrorist fighters have rolled over payments from APRA-regulated superannuation funds to SMSFs (self-managed superannuation funds), with the money ultimately being used for terrorism financing," the AUSTRAC report noted.

"Fighters may also be supported by family or others in their community who are accessing their superannuation savings legitimately."

Superfund accounts also appear to be a handy tool for patient criminals to launder proceeds of crime, parking their money in the legitimate financial system and securing long-term low tax capital gains.

Cyber-attacks on super funds now a daily event

However, AUSTRAC said by far the biggest threat of criminal activity in superannuation was fraud and cybercrime with most funds contacted for the study noticing regular, even daily, hacking attempts.

Around 85 per cent of all suspicious transactions reported to the study, or 249 in total, related to fraud or cybercrime.

"Hacking provides criminals with the data they need to breach the defences that superannuation providers have in place," the report said.

"One large fund noted that cyber-enabled fraud attempts often started with small-scale attempts to find weaknesses in a fund's procedures and systems.

"Once a weakness was established, the fund was subject to 'mass waves of attack' from a number of fraudsters."

The study found the superannuation system had several key vulnerabilities to breaches of money laundering and terrorist funding (ML/TF) laws.

These include:The extremely large number of member accounts and volume of transactionsLow levels of member engagement, which hampers timely detection of fraudPost-preservation accounts which have few restrictions on making transactions to and from the accountsVoluntary contributions to accumulation accounts by members, where the source of money is difficult to verifyPayments to members and outgoing rollovers that are vulnerable to fraud and illegal early releaseThe growing reliance on online delivery of products and services, resulting in less face-to-face interaction with customers and increasing online data storage

Low levels of reporting may indicate weak protection

The report urged all super funds to strengthen anti-money laundering and counter- terrorism funding controls.

"Given the size of superannuation holdings and the level of criminal activity in the sector, it is likely that all funds would be exposed to potential suspicious matters," the report said.

"Low levels of reporting compared to industry peers may be an indicator of an ineffective [Anti-Money Laundering/Counter-Terrorism Financing] program."

AUSTRAC chief executive Paul Jevtovic said the risk assessment report should encourage the superannuation sector to identify and submit increased volumes of suspicious matter reports.

"As with all regulated sectors, AUSTRAC will seek to engage funds that appear to have lower levels of compliance than their industry peers," Mr Jetovic said.

"There is considerable scope for superannuation funds to expand their suspicious matter reporting and strengthen internal controls against financial crime."

Saudi Gazette
KSA ranked 1st in MEA for ransomware attacks
Tuesday, 22 November 2016
Byline: Staff Report

Riyadh - Symantec's Internet Security Threat Report (ISTR), Volume 21, revealed an organizational shift by cybercriminals: They are adopting corporate best practices and establishing professional businesses in order to increase the efficiency of their attacks against enterprises and consumers. This new class of professional cybercriminal spans the entire ecosystem of attackers, extending the reach of enterprise and consumer threats and fueling the growth of online crime.
"Advanced criminal attack groups now echo the skill sets of nation-state attackers. They have extensive resources and highly-skilled technical staff that operate with such efficiency that they maintain normal business hours and even take the weekends and holidays off," said Eyas Hawari, Country Director, Saudi Arabia, Symantec.

The Kingdom of Saudi Arabia's (KSA) 2015 global Internet Security Threat Profile ranking improved in 2015, moving from 42nd place globally in 2014 to 47th in 2015. This shift indicates a lower global percentage of source-based security threats, including malicious code, spam, phishing hosts, web and network attacks, and bots detected emanating from the country. In the Middle East and Africa, KSA ranked 7th, one place below the UAE and improving three places from last year.

"Given the size of its population, strategic geographical local, breadth of industries, and strong consumer spending power, Saudi Arabia is home to some of the region's largest organizations. Cyberthreats are one of the most critical security challenges that organizations across the globe face.," said Hawari added. "Organizations and consumers across the country are targeted with a variety of threats, including ransomware. It is therefore imperative that they continue to adopt robust security measures and global best practises to protect themselves against such attacks."

Advanced professional attack groups are the first to leverage zero-day vulnerabilities, using them for their own advantage or selling them to lower-level criminals on the open market where they are quickly commoditized. In 2015, the number of zero-day vulnerabilities discovered on a global level more than doubled to a record- breaking 54, a 125 percent increase from the year before, reaffirming the critical role they play in lucrative targeted attacks.

Globally, there were 430 million new malware variants discovered in 2015, a 36 percent increase from the previous year, proving that professional cybercriminals are leveraging their vast resources in attempt to overwhelm defenses and enter corporate networks.

In addition, organizations in KSA were highly attacked by malware, ranking 4h within Middle East and Africa region. 1 in 98 emails contained malware, while more than half (57.3 percent) of the emails were spam. In addition, large organizations (2,501+) were the most targeted for malware where 1 in 75 malware-mails received contained malware.

In KSA, web attacks were the most prevalent threat, catipulating the country's global web attack rank to 30th place, up 9 positions from 2014 and 2nd in the MEA region. Social media scams are also highly prevalent in Saudi Arabia, where it ranked 4th in the Middle East and Africa and 25th globally. This could be attributed to a range of socio-economic factors including the high smartphone penetration and high-speed internet access rate in the country as these connections can be easily leveraged and exploited by cybercriminals.

Data breaches continue to impact the enterprise. In fact, large businesses that are targeted for attack will on average be targeted three more times within the year. Additionally, the largest data breach ever publicly reported occurred last year with 191 million records compromised in a single incident. There were also a record-setting total of nine reported mega-breaches. While 429 million identities were exposed, the number of companies that chose not to report the number of records lost jumped by 85 percent. A conservative estimate by Symantec of those unreported breaches pushes the real number of records lost to more than half a billion.

Ogranizations in the Finance, Insurance and Real Estate and Wholesale sectors sector were the most affected by targeted attacks in KSA in 2015.. These organizations may be targeted as they have a lucrative database of customers, which cybercriminals can leverage for future attacks.

Ransomware also continued to evolve in 2015, with the more damaging style of crypto-ransomware attacks growing by 35 percent. This more aggressive type of ransomware, known as crypto-ransomware attacks encrypts all of a victim's digital content and holds it hostage until a ransom is paid. This year, ransomware spread beyond PCs to smartphones, Mac and Linux systems, with attackers increasingly seeking any network-connected device that could be held hostage for profit, indicating that the enterprise is the next target. KSA was the #1 most impacted country in the Middle East and Africa region in regards to ransomware, and the 31st globally with about 41 attacks per day measured.

As people conduct more of their lives online, attackers are increasingly focused on using the intersection of the physical and digital world to their advantage. In 2015, Symantec saw a resurgence of many tried-and-true scams. Cybercriminals revisited fake technical support scams, which saw a 200 percent increase last year. The difference now is that scammers send fake warning messages to devices like

smartphones, driving users to attacker-run call centers in order to dupe them into buying useless services.

Bahrain News Agency
For a New Approach to Cyber Security
Tuesday, 22 November 2016

Manama - Last January, Brown University launched a milestone Executive Master in Cybersecurity. The 16-months program aims at training a new generation of top security executives by offering professionals with a combination of on-campus as well as online, highly collaborative and interactive education modules.
Experts from many different departments of the University were drawn into the program in order to provide students with a deep understanding of this multi-faceted issue looking at InfoSec from a global, technical, human, and policy perspective.

This ambitious program stands out thanks to this interdisciplinary approach and is a much- needed step towards the shift Corix Partners has constantly been advocating for that is, the realisation that InfoSec is not a merely technical challenge and should primarily be approached from a governance and management perspective. The programs motto says it best: Strategy is the best Security.

The three main pillars of this program Technology, Law and Policy, and more importantly Human Factors are reflective of such mindset.

Advanced technological knowledge is of course essential for any cybersecurity professional, and many universities are already doing a great job training technical experts in this field.

On the other hand, Law and Policy is perhaps that part of InfoSec that is the most salient to top executives and board members in all organizations. It is obvious that the regulatory environment surrounding cyber-protection and the sometimes disastrous legal consequences of undergoing a cyber attacks are very important as businesses dive into the digital era. However, this focus tends to lead organizations to approach InfoSec from a merely reactive, tick-in- the-box and compliance-oriented perspective that prevents them from effectively addressing the issue.

What is truly underestimated when it comes to true cybersecurity leadership is the last pillar Human Factors. Your people indeed represents the biggest threat to the digital security of your organization, and any successful InfoSec strategy must fully recognize and address this issue. Classes such as Human Factors in Computer Security and Privacy which aims at giving students a rich understanding of the complexity of human agents and draws from behavioral science, user interface and personal management should allow future top executives of organizations to build innovative, much more resilient cybersecurity strategies.

It is good to see top universities finally addressing the critical cross-silo aspects of cybersecurity

And it should help a number of executives come to terms with the true dimension of the problem, looking beyond its mere technical dimension.

However, this kind of program is still mostly designed for CISO-level executives who rarely make it to the board room. The incorporation of InfoSec considerations into top executive MBA curriculums is the next crucial step that business schools must take in order to truly drive change at the top decision-making level. This is especially true as cyber security, data protection and privacy issues are quickly entering the realms of both CSR and corporate ethics. As of now, however, none of the worlds best-ranked MBA programs has yet decided to place enough emphasis on these emerging issues.

Washington Post
Hackers get leeway to report Pentagon bugs
Tuesday, 22 November 2016
Byline: Ellen Nakashima

Washington - The Defense Department on Monday became the first U.S. government agency to launch a policy enabling researchers to report bugs or flaws they discover in its websites without fear of prosecution.
Calling it a "see something, say something" policy for the digital domain, Defense Secretary Ashton B. Carter said the program is aimed at improving the security of the Pentagon's unclassified, public-facing networks.

The Army also opened registration Monday for Hack the Army, a challenge in which researchers and hackers scour Army sites for software flaws and compete for thousands of dollars in bounty rewards.

The Army contest explicitly authorizes researchers to try to hack a limited set of Army systems to find weaknesses. Meanwhile, the new policy is aimed at creating a way for hackers or researchers who come across flaws to report them without exposing themselves to criminal liability.

"This is a historic moment for hackers and the U.S. government," said Katie Moussouris, founder of Luta Security and an adviser to the Pentagon on the new policy. "For the first time since hacking became a felony offense over 30 years ago, the Department of Defense has now opened the doors for ongoing vulnerability disclosure from helpful hackers who want to help secure these systems without fear of legal prosecution."

There are security researchers who conduct broad scanning of Internet systems to discover and map vulnerabilities. In doing so, they might come across flaws in Pentagon websites. There are also hackers who, for an intellectual challenge, probe systems to try to find flaws that might be exploited. In either

case, these researchers and hackers could be charged with violating the Computer Fraud and Abuse Act, a prospect that has chilled security research.

Assistant Attorney General Leslie Caldwell, head of the Justice Department's criminal division, called the new policy "a laudable way to help computer security researchers to use their skills in an effective, beneficial and lawful manner to reduce security vulnerabilities." Her division advised in the crafting of the policy.

Pentagon networks are under constant assault from hackers seeking to find weaknesses they can exploit. In recent years, there have been intrusions into the unclassified email systems of the secretary of defense and at the Joint Chiefs of Staff. In 2008, the department's classified network was compromised in an operation thought to have originated in Russia.

The vulnerability disclosure policy will provide a standard avenue of reporting for all department websites. Bug data that is reported will be used for defensive purposes only, the policy states, to fix vulnerabilities in the department networks or applications, or in the software of vendors.

Individuals who report flaws will not receive bounties. The policy states that they may not harm the network, withdraw any data, compromise the privacy of department personnel or disclose details of the vulnerability without permission from the Pentagon.

The policy is aimed at people who come across the bugs in the course of their jobs or through research, said Alex Rice, chief technology officer and co-founder of HackerOne, a tech firm that helps companies set up bug-bounty and vulnerability disclosure programs. It has been working with the Pentagon on the program.

"The Department of Defense is not explicitly asking them to hunt for vulnerabilities," he said, "but they want to make sure they have a clear line of disclosure when they find them."

The program grew out of Hack the Pentagon, a bug-bounty challenge earlier this year in which about 250 people found and submitted flaws found in Pentagon sites. Of those, 138 received bounties totaling $75,000. One of the lessons learned from that experience, Rice said, was the lack of a way for people to report these vulnerabilities to the department outside of the bounty program.

The new policy does not cover the use of bugs for offensive or hacking purposes. The White House has a separate policy addressing that issue as applied to government agencies that discover or purchase software flaws. Tech policy experts have called for more disclosure of the policy's details and how it has been implemented.

Wall Street Journal
NSA Chief Michael Rogers Talks Cybersecurity

Tuesday, 22 November 2016
Byline: Rebecca Blumenstein

Interview - Cyberattacks represent an expanding and perilous front line for companies and the government. What do we do about a borderless war that has impacted business across the world and even a presidential campaign?
The Wall Street Journal's Rebecca Blumenstein spoke with Adm. Michael S. Rogers, head of the National Security Agency and commander of the U.S. Cyber Command. Here are edited excerpts of the discussion.

MS. BLUMENSTEIN: How worried should CEOs be about the state of cybersecurity?

ADM. ROGERS: Do we have a challenge here that requires attention? Yes. Is there a role for CEOs to play in this? Yes. You don't want your network-security team deciding unilaterally what's important. You as the leader need to set that tone. I do that in my own organization.

MS. BLUMENSTEIN: What can go wrong? It was now two years ago when the Sony hack happened. What can we learn?

ADM. ROGERS: I thought the positives were great collaboration between a private company--they knew they were dealing with something. They felt they needed to reach out to the government.

They could have sat there and said to themselves, "We really need to minimize this. Let's not really confront this publicly." They were very up front when they approached the government.

And we're going, "Look, if you want us to provide value and insight to you, then the only way this is going to work is if we get full access to your network and your data. It's the only way we can really generate the level of insight that I think you expect from us. I realize that that may make you uncomfortable. You're opening your structure. You're opening your networks. You're opening your data. You have to be comfortable with that."

They came back to us and said, "We're comfortable with that. What we ask you to do is inform us of what you're doing while you're doing it. And you stick to that."

MS. BLUMENSTEIN: But there were things that went wrong. It took a long time for them to detect this, right?

ADM. ROGERS: It doesn't matter if it's a commercial network, if it's a government network.

Networks that I have been accountable for defending, we generally find there's a significant time lag for most organizations between discovery of activity and the actual time the adversary initially penetrated the network.

MS. BLUMENSTEIN: How concerned should we be about state actors?

ADM. ROGERS: Probably 60% to 65% of the total activity we see of concern is criminal. It's not nation-states. Criminal activity includes theft of intellectual property. You also see nation-states doing this. But you see criminal groups penetrating networks to steal information that they think they can sell to someone. At the same time, you also have nation- states who you find are engaged in actions designed to penetrate the networks within the commercial sector.

You also find individuals and groups who are brought together for specific purposes under a specific ideology or focus. They'll harness that interest to a specific outcome. "Hey, let's do the following because we're all united by the idea we don't like this particular policy." We have seen Anonymous engage in activities against nation-states, companies, individuals.

I don't want it to get to the point where it takes some significant calamity to drive us to the conclusion that we've got to do something different than what we're doing now. The ultimate solution in my mind is how do you bring this public-private partnership?

The agreement I always reach with whoever we're working with is: I will not use the data we gain for anything other than the exact purpose I communicate to you.

Traditionally as a nation, we have very much differentiated between what is the role of the government, and what is the role of the private sector.

Cyber does not recognize these arbitrary lines that we have drawn. It doesn't recognize geography. I think it is totally unrealistic to expect the private sector to withstand the onslaught of activity that is being directed against them by nation-states and other actors.

Likewise, I don't think it's realistic to say, "Well, the government's going to do this." The challenge with the government doing it is if you want me to defend something, I can't do it from the outside. It's like fighting with one hand tied behind your back. It's not realistic, and it doesn't generally lead to positive outcomes.

MS. BLUMENSTEIN: I have to ask about WikiLeaks. You told NPR in August, "These emails were clearly leaked for a reason, and they were leaked, I believe, to achieve an effect." What can you tell us?

ADM. ROGERS: There's an ongoing investigation. I'm just not getting into the specifics. I still think there shouldn't be any doubt in anybody's mind. This was not something done casually. This was not something done by chance. This was not a target that was selected purely arbitrarily. This was a conscious effort by a nation-state to attempt to achieve a specific effect.

Christian Science Monitor
Influencers: Trump won't improve cybersecurity
Tuesday, 22 November 2016
Byline: Sara Sorcher

Boston - President-elect Donald Trump has promised that protecting the country from cyberattacks will be a "major priority" for his administration, but three-quarters of Passcode's pool of digital security and privacy experts say they do not believe cybersecurity will improve with the Republican in the Oval Office.
Passcode's latest Influencers Poll, a regular survey of 160 current and former government and intelligence officials, and leaders from the private sector and advocacy community, revealed broad pessimism about country's digital security over the next four years both because of Mr. Trump's stated policies - and his own personal lack of tech knowledge.

"I voted no simply because the president elect himself has shown no interest in understanding the issue," says Michael Hayden, a retired Air Force general and the former director of the CIA and National Security Agency.

Trump's response to a question about how he would improve the country's cybersecurity at a presidential debate this fall - in which he brought up his 10-year-old son's "unbelievable" computer skills and referred to digital threats as "the cyber" - was largely panned by the security community as an indication he didn't understand the complexity of digital threats facing the country. And many security experts were mystified by his refusal to blame Russia for the high-profile hacks on political organizations that took place during the campaign, a public break with the conclusions of the US intelligence community and prominent researchers who investigated the cyberattacks.

While Mr. Hayden, now a principal at global advisory firm The Chertoff Group, says "there may be some hope, however, that the government under him will continue to move albeit slowly in the right direction," other experts are wondering if Trump's campaign trail comments make it less likely top tech talent will choose to work in his administration over (typically) higher-paying jobs in the private sector.

"Set aside the lack of understanding (10-year-old sons excluded) and turning a blind eye to Russian role in an attack on American institutions, the real damage may be on the people side," says Peter Singer, strategist and senior fellow at New America think tank. "It is hard enough for government to recruit and retain talent, especially in a field like cybersecurity. It just got bigly harder."

Several security and privacy experts voiced concerns with Trump's strong stance against encryption. During the campaign, he went so far as to call for a boycott of Apple as it pledged to fight a court's ruling to help the FBI unlock the iPhone used by the shooter in the San Bernardino terror attack. Those who believe that strong encryption is essential for protecting consumers' data from cyberattacks are alarmed at the prospects of Trump's administration trying to mandate companies build in ways for the US government to access secure communications.

"To date, Trump's stance on encryption, backdoors, and cybersecurity appears naive and contrary to our founding fathers' vision and innovation," says Nico Sell, cofounder of encrypted messaging app Wickr. "Everyone in the global information security community is now watching to see who Trump surrounds himself with. Security is a global critical challenge; my hope is that he brings his views up to date once briefed by intelligence experts. The world needs a strong role model on this very important issue that impacts us all."

Cindy Cohn, executive director of the Electronic Frontier Foundation, is also calling for Trump to listen to security experts on encryption policy. "We desperately need leadership that recognizes that empowering users and companies to provide the strongest security and creating incentives for them to do so is the best way for us to actually be more secure," she says. "That means supporting strong encryption and helping companies fix security problems rather than keeping them open and hoping no bad guys find them. While Mr. Trump could remedy his lack of knowledge with some reasonable appointments, there's no indication yet that he will."

However, 25 percent of Influencers said they believed cybersecurity would improve under Trump. "Yes, I think The Cyber will continue to enjoy more attention from both the executive and legislative branch under the new administration," said one Influencer who chose to remain anonymous. "Cyber will be a priority issue for the Trump administration, and progress will continue, as it would had the election results been different," another Influencer added. "It is a 'must do,' not a 'nice to do' issue." Passcode allows Influencers to reply on the record or anonymously to preserve the candor of their responses.

The cybersecurity plan on Trump's campaign website offers some ideas about how he might improve cybersecurity, including commissioning an "immediate review" of both the country's defenses and security weaknesses, and creating task forces to respond to digital threats. Trump has also said he will seek recommendations on how to enhance the military's Cyber Command with "a focus on both offense and defense." He's also already tapped retired Army lieutenant general Michael Flynn, a former director of the Defense Intelligence Agency, as his National Security Adviser.

"Could this be a Nixon to China moment? I hope so. Trump's more aggressive rhetoric on cybersecurity gives him an obvious opportunity to set norms of restraint on certain kinds of destabilizing behaviors," says Steve Weber, professor at the School of Information at the University of California - Berkeley. "A 'no first use' pledge around something like critical infrastructure would mean a lot coming from this new administration."

Other Influencers were optimistic even if they didn't think that the president-elect or his administration would be the ones to alleviate the cyberthreats. "If there is some major national hack, Congress will act instead," one Influencer said.

And some privacy advocates said they thought Trump himself could be the reason people fortify their digital defenses - in opposition to his embrace of surveillance and government access to encrypted

communications. "Trump's presidency," says Elana Zeide, a research fellow at New York University's Information Law Institute, "gives everyone more incentive to secure their communications."

Comments:

NO

"With change in administrations there is opportunity, but in the near term they will be learning how to govern. While cybersecurity played out as a backdrop to the election it was not focal to Trump's campaign. Immigration, trade, infrastructure, and Obamacare reform will suck all the oxygen out of the room and leave little room for the (civilian) security community to make gains." - Jeff Moss, founder of Black Hat and DEF CON

"Data security and security of IoT is a major concern for consumers. My biggest concern is the next administration mandating broad exceptional access mandates which would undermine the security of IoT." - Terrell McSweeny, Federal Trade Commissioner

"The current mix of incentives and disincentives in the US is not driving improvements and the Trump stated goals for information sharing are unlikely to improve the situation. Hopefully his focus on more efficient and effective government causes reform of acquisition and procurement, which would have a net positive effect within government." - Influencer

"The answer of course depends on who the advisors to the president are and on the final policy decisions that are made and enacted, but initial indications are not favorable overall with respect to cybersecurity policy. Based on his prior comments (essentially anti-Apple/anti-encryption), the president-elect is likely to favor less security in exchange for more government access, which would weaken our security overall. Further, with a closely divided Senate, the current glacial rate of policy developments on cybersecurity will not likely accelerate, placing us further 'behind the curve' relative to worldwide developments and needs in cyberspace over time. One outstanding issue that could improve under the Trump administration is the Wassenaar Agreement, more specifically its language on 'intrusion software' to which cybersecurity technology firms and legitimate cybersecurity are strongly opposed. As this ongoing debate will run into the next presidential term, the Trump Administration has an opportunity (and presumably an interest) in 'rebooting' the conversation, hopefully aiding in bringing it to a more acceptable conclusion. With proper industry expertise being applied to the renegotiation of this problematic contract, cybersecurity companies can confidently take a more active role in stopping cybercrime and cyberespionage without running the risk of prosecution or other negative impacts to their business or freedom." - Influencer

"My assessment is based on the initial challenges I believe the Trump administration will face in retaining and attracting the best technical talent and the most strategic policy and law thinkers. I believe we will continue to maintain a robust cybersecurity technical and tactical capacity, but I worry that episodic interference from President Trump's senior political advisors, or unconventional geopolitical

decisions by President Trump himself, may complicate a coherent approach. This challenge may, ironically, lead to more public discussion, debate, white papers, recommendations, etc. from the establishment cyber-warrior class and perhaps have more influence of time on the global cybersecurity strategy of a Trump administration over time." - Influencer

"Nothing suggests Trump - or anyone on his staff - understands even the basics of why we need to improve the nation's defenses. - Chris Finan, CEO of Manifold Security

"It is too early to tell, and not enough is known about their concrete policy objectives to speak with authority on whether they will take actions that improve or weaken cybersecurity. I am open to working to educate the administration about the Internet, and others should be as well." - Christian Dawson, executive director and cofounder of the Internet Infrastructure Coalition (i2Coalition)

"[What's on Trump's website] is extremely vague and contains no meaningful indication that Trump would improve the current state of cybersecurity. - Yan Zhu, engineer at Brave

"Trump has advocated an 'America first' foreign policy, but this type of isolationism will not work for cybersecurity. Improving cybersecurity will require US leadership and global partnerships as this is not a problem that the US can solve on its own." - Influencer

"Our most capable adversaries will exploit the gaps created by a change in leaders and capabilities. State sponsored activity is frequent, and taking fewer steps to disguise the activity." - Jenny Durkan, global chair of the Cyber Law and Privacy Group at Quinn Emanuel law firm

"One tries to be hopeful. In reality there's no way to predict." - Influencer

"Trump will not regulate the IoT makers or the software makers for fear of hurting their growth and jobs. Cybersecurity under Trump will be more of the same current reactive 'cyber smoke alarm and cyber fire station' approach which has proven in the physical world not to prevent cities from burning down. It's not until we have the fortitude to mandate the equivalent of brick firewalls between buildings and sprinkler systems will things change. Expect to see plenty of offense from our cyber glass house." - Chris Wysopal, cofounder at Veracode

"I haven't seen any urgency on this matter during his campaign, nor do I think his base is particularly concerned with matters of cybersecurity." - Jeffrey Carr, president and CEO of Taia Global, Inc.

"US cybersecurity will continue to grow in relevance and attention regardless of who the president is, and companies will have to dedicate more resources and time to making good and secure decisions about how to protect data. Now, whether US *government* cybersecurity will improve - for that we'll have to wait until a cybersecurity chief is named to begin to guess." - Influencer

"Trump and his advisors have demonstrated no understanding of cybersecurity, nor any comprehension of its importance. Moreover, the recent purge of any qualified cybersecurity experts such as Mike Rogers from his team - in favor of hacks from Breitbart and Jeff Sessions' office - makes clear that they are more interested in absolute power than any constructive accomplishments." - Influencer

"Trump lacks the discipline and vision to implement a coherent and effective approach to cybersecurity." - Tor Ekeland, managing partner of Tor Ekeland, P.C. law firm

"My biggest fear is Trump's implied support for extension of law enforcement powers to include forcing vendors to break their end-to-end security in order to accommodate search warrants. The FBI's analogy is a bank's safety deposit box; I believe data to be fundamentally different though, and without precedent. A lot of damage can be done between now and when a relevant Supreme Court decision on this is made." - Nick Selby, cofounder and chief executive officer of StreetCred Software

"It is *WAY* too soon to say cybersecurity will get better or worse under a Trump Presidency, or whether the Presidency will have any influence on the state of cybersecurity. We have zero track record on what his administration will or will not champion and what his administration will or will not mandate." - Influencer

"There are not enough 400 pound hackers." - Influencer

"US cybersecurity will improve during the Trump administration. But any improvements will have more to do with overcoming an era of cyber inertia than with anything stemming from a Trump presidency." - Influencer

"Cybersecurity defenses are always getting better and the next four years will not be an exception (in large part because most improvements in cybersecurity arise from the private sector with its own motives). Unfortunately, cybersecurity offenses are always getting better too. Finally attack surfaces are growing, as an increasing number of Internet of Things stories reminds us. So, a broad answer has to balance three very different trends. Then there's the question: improved relative to what? Will science advance in a Trump administration? Undoubtedly, because science never goes backwards and that would be true if science funding were cut to zero. But, with cybersecurity as with science, the question is one of comparison. If cybersecurity would have advanced more in a hypothetical Clinton administration than in a Trump administration is the answer to your question still 'yes'? And of course, we have no clue who Trump is going to appoint - and, otherwise, I really cannot tell what Trump's cybersecurity policies are going to be." - Martin Libicki, senior management scientist at RAND

YES

"Fresh eyes." - Mark Weatherford, principal at The Chertoff Group

"While Trump in his campaign program gave little or no indication of a concrete plan to improve cybersecurity in the US, the reality is so dire that improvements in cybersecurity will be a must." - Influencer

"Yes, contingent on him walking the talk regarding regulation accelerating the protection of the .gov morass. He needs to support the transformation at NSA and rethink the role of government." - Influencer

"I really don't see how he can make it worse so any changes at all will likely be improvements no matter how small. Obama couldn't get stuff through Congress and so had to make his changes through executive proclamation. Barring some major national hack I don't see Trump doing that. If there is some major national hack, Congress will act instead. So really I don't see much improvement under Trump other than incremental changes. Anything like CFAA reform or changes to DMCA are pretty much off the table now I am sure. We may see a new 'cyber' bill get passed but it will be about as effective as CISA, in other words sound real good and have 'cyber' in the title but not really make a whole hell of a lot of difference." - Influencer

"President-elect Trump has been more specific about the need to improve cybersecurity than about most defense issues. At a minimum, he's likely to continue initiatives from the Obama administration to strengthen cybersecurity." - Influencer

"Previous presidents have so far been unsuccessful in constructing cohesive and well informed cybersecurity policies or installing multi-disciplinary leadership. As the International cyber threats have increased in sophistication and scope, we're rapidly approaching an inflection point where if something isn't done, it will be done to us via external entities. Just as hacking, cybersecurity, and email breaches have been core to the election process, they will continue to grow and affect Trump's new government. Hence, in Trumps presidency, the US government and agencies are having their hands forced in to dealing with this invasive hacking epidemic. - Günter Ollmann is chief security officer at Vectra

"In October, the US Chamber wrote an open letter to the 45th president to recommend that the incoming administration prioritize three cybersecurity issues: First, we need to build on the momentum behind the joint industry-National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity, which business leaders and policymakers see as a key pillar for managing cyber risks at home and internationally. Closely linked, we urge the incoming Trump administration to harmonize existing regulations with the cyber framework. Cutting cyber red tape will serve the cause of bolstering security. Second, the Trump team starts in a strong position with the enactment of the Cybersecurity Information Sharing Act (CISA). By working as an ally with industry, the next administration can lead a culture shift to bring businesses off the sidelines to engage in effective threat information-sharing. Third, Washington's policies ought to encourage greater adherence to international norms of acceptable behavior and deterrence in cyberspace. The pros and cons of cyber deterrence deserve more careful scrutiny than they have received to date." - Matthew Eggers, executive

director for cybersecurity policy in the National Security and Emergency Preparedness Department at the US Chamber of Commerce

"The reason for 'Yes' is that, in cybersecurity, offense has permanent structural advantage. AI applied to offense will result in Mexican standoff, which will be called 'peace.' - Dan Geer chief information security officer for In-Q-Tel

"It is not possible at this point to predict this. Trump changes his mind all the time and the direction is most likely to be determined by top advisors who as yet remain unnamed." - Influencer

Bloomberg News
Firing NSA Chief Would Be 'Extremely Reckless,' Nunes Says
Tuesday, 22 November 2016
Byline: Chris Strohm, Nafeesa Syeed

Washington - Removing the head of the National Security Agency and U.S. Cyber Command would be "extremely reckless" and leave the U.S. vulnerable to security threats during a delicate time of presidential transition, said House Intelligence Committee Chairman Devin Nunes.
Nunes, a California Republican, commented in an interview Monday after a Nov. 19 report in the Washington Post said that Defense Secretary Ash Carter and James Clapper recommended that Admiral Michael Rogers be removed as the head of both agencies.

Carter has grown increasingly frustrated with Cyber Command and Rogers for a lack of progress in countering Islamic State's cyber operations, according to a U.S. official who asked to not be identified discussing internal deliberations.

Clapper's motivation for removing Rogers would be to split the leadership roles of the NSA and Cyber Command and to have a civilian in charge of the NSA, according to the Washington Post report. Clapper already has submitted his resignation as Director of National Intelligence in anticipation of the new administration.

The Pentagon and Office of the Director of National Intelligence declined to comment when contacted by Bloomberg, while the NSA didn't respond to requests for comment.

To date, no reason has been communicated to the intelligence committee to justify firing Rogers, and intelligence leaders haven't informed the panel that the chief of the NSA and Cyber Command was failing in his duties, Nunes, a California Republican, said in the phone interview.

'Snake Pit'

"The knives are out to get Rogers," Nunes said, describing elements of the intelligence community as a "snake pit."

Rogers took over NSA and Cyber Command in 2014 in the wake of former contractor Edward Snowden's disclosures of secret surveillance programs. The NSA was bruised earlier this year by revelations that another of its contractors was accused of stealing millions of pages of data over 20 years. That followed an incident in August in which an online group called ShadowBrokers posted two encrypted dossiers with what appeared to be highly classified NSA hacking tools to online file-sharing sites.

President Barack Obama this weekend called Rogers "a terrific patriot" and declined to say whether he would seek his resignation.

Nunes, who is serving as an adviser to President-elect Donald Trump's transition team, said he believes Rogers is doing an excellent job and would support him as the next director of national intelligence under Trump.

Rogers, 57, met last week with Trump in New York as his name surfaced as a potential replacement for Clapper. Discussions about the possibility of removing Rogers occurred before that meeting, the official said.

Decision Shelved

The intelligence committee has asked Clapper and Carter, or their aides, to confirm Monday whether a recommendation has been made to remove Rogers and, if so, why.

Clapper and Carter have formally recommended that the NSA and Cyber Command be split apart, a second U.S. official said. For now, that recommendation has been shelved during the presidential transition, but a new leader for each agency could be chosen if the plan goes forward.

Nunes said in a Nov. 19 letter to Carter and Clapper that he has been "consistently impressed" with Rogers' leadership and accomplishments.

"His professionalism, expertise, and deckplate leadership have been remarkable during an extremely challenging period for NSA," Nunes said, using a term for leaders who set the tone for their teams. "I know other members of Congress hold him in similarly high esteem."

San Francisco Chronicle
Trump's CIA pick would reinstate US collection of phone data
Tuesday, 22 November 2016
Byline: Bob Egelko

San Francisco - The federal government's long-hidden authority to sweep up records of all phone calls made in the U.S. was repealed last year in a bipartisan vote of Congress. But President-elect Donald Trump's choice to head the CIA has called for reinstatement of the data haul and said its elimination was part of "Edward Snowden's vision of America."
Snowden, a former National Security Agency contractor, revealed in 2013 that the NSA had been collecting bulk data on U.S. phone calls without a warrant for more than a decade. President George W. Bush's administration had ordered the collection unilaterally after the terrorist attacks of Sept. 11, 2001, then obtained approval from a secret intelligence court in 2006.

The records contain so-called metadata, showing the numbers called and duration of the calls, but not the content of the messages. The law that President Obama signed in June 2015, called the USA Freedom Act, leaves the records with the phone companies but allows the National Security Agency to request data on individual customers without a court order.

Rep. Mike Pompeo, R-Kan., whom Trump named Friday as his choice for CIA director, was among a minority of House Republicans who opposed the change. In a December 2015 column in the National Review magazine, he attacked Republican presidential candidates who supported the new law.

"Those who today suggest that the USA Freedom Act, which gutted the National Security Agency's metadata program, enables the intelligence community to better prevent and investigate threats against the U.S. are lying," Pompeo wrote.

"Less intelligence capacity equals less safety. To share Edward Snowden's vision of America as the problem is to come down on the side of President Obama's diminishing willingness to collect intelligence on jihadis."

In a January 2016 Wall Street Journal column co-authored by conservative commentator David Rivkin, Pompeo called for Congress to reauthorize collection of U.S. phone records, which would be combined with "publicly available financial and lifestyle information" into a government database.

"Legal and bureaucratic impediments to surveillance should be removed," Pompeo and Rivkin wrote.

Neither Trump's presidential transition office nor Pompeo's congressional office responded Monday to inquiries about the issue. But privacy advocates predicted congressional resistance to any attempt to reinstate government authority to gather Americans' phone records.

"This was an invasion of privacy for every single American, Americans who had never been accused of any crime," said Neema Singh Guliani, legislative counsel for the American Civil Liberties Union. And a review by the government's Privacy and Civil Liberties Oversight Board found that the records haul "never played a substantial role in stopping an act of terrorism or stopping a terrorist suspect," she said.

"I think a lot of Americans would be very nervous to learn Donald Trump has access to our phone records," said Elizabeth Goitein, co-director of the Liberty and National Security Program at the Brennan Center for Justice in New York. "It would make a lot of Congress nervous as well."

Although Snowden, now in Russia, has been accused of wrongdoing by both Trump and his defeated Democratic presidential opponent, Hillary Clinton, Goitein said Pompeo's attempt to discredit the former NSA contractor had misfired.

"If Edward Snowden's vision of America is an America that doesn't spy on Americans, I guess (Pompeo's) right," she said.

Because the USA Freedom Act was passed by Congress, it would take an act of Congress to repeal it. But the Trump administration could act within the law to expand data collection.

For example, said Singh Guliani, the U.S. Drug Enforcement Administration had its own program since the 1990s of collecting metadata on phone calls to and from countries associated with drug trafficking, including Canada, Mexico and most of Central and South America. The Obama administration suspended that program in September 2013 after Snowden's disclosures, but a new administration might revive it.

Snowden also disclosed records of surveillance programs that monitored the content of phone calls to and from certain countries without court approval, programs that the Trump administration could expand, Singh Guliani said.

Goitein noted that the USA Freedom Act was compromise legislation that allowed the government to obtain not only individual records from a phone company, but also records of anyone the targeted person had called. And she said one of the law's safeguards, requiring the secret court to publish a summary of any ruling it issues on a significant issue, allows the government to decide which issues are "significant" and what information should be withheld for security reasons.

Another privacy-rights advocate, Cindy Cohn, executive director of the Electronic Frontier Foundation in San Francisco, said Obama could have done more to adopt lasting protections against surveillance abuses.

"The Obama administration's approach was fixing internal rules" for its own actions, Cohn said. "That leaves it really ripe for change by the next administration." And Obama, she added, "could have taken a turn away from all this secrecy" that still envelops the programs.

Susan Freiwald, a University of San Francisco law professor who teaches courses in privacy and cyberlaw, said Pompeo and his future colleagues will have leeway to interpret the law "broadly so they may collect vast amounts of information."

"Pompeo is promoting the discredited view that it is always good for a government to collect more data on its people," she said.

The National (UAE)
BlackBerry Dtek60: Phone maker returns to the fray (Canada).
Tuesday, 22 November 2016
Byline: John Everington

Abu Dhabi - With the new Dtek60 BlackBerry has produced a pretty compelling Android smartphone at a quite reasonable price of Dh1,999, all overlaid with the brand's security features IT departments supposedly love.
It's just a shame it comes out so late in the game for the company, with its market share lower than ever.

The Dtek60 is pretty similar design wise to its predecessor the Dtek50, sporting the same solid, if slightly uninspiring, off-the-shelf form factor of the Alcatel Idol 4S.

Looks aside though, the Dtek60 is a massive upgrade on its predecessor; the display is slightly larger at 5.5 inches, and is now Amoled, offering a far higher pixel density and much more vibrant colours.

At long last, BlackBerry has fin-ally made a handset with a fingerprint scanner, located on the rear of the phone just below the camera, as per the LG G5 and others.

Camera-wise, the Dtek60 now sports a 21MP rear snapper (compared with the 13MP of the Dtek50), with the same 8MP selfie camera as its predecessor. Performance is decent if not stellar, with one or two struggles in low light compared with the iPhone 7 and the best-in-class Samsung Galaxy S7.

The Dtek60 is still a BlackBerry at heart. BlackBerry Messenger (BBM), BlackBerry Hub and BlackBerry Intelligent Keyboard are all present and correct for the faithful. There's even a little red notification light in the top right-hand corner.

Plus the brand continues to tout its security features as its trump card. Like its predecessor, the Dtek60's storage is encrypted right out of the box, while its Dtek app notifies you when the handset camera, micro-phone and location are being accessed.

Additionally, BlackBerry has been active in providing Android security patches faster than any other manufacturer other than Google (for its Nexus and Pixel ranges), something that will continue to appeal to IT managers and the more security-conscious consumers.

The Dtek60 at long last provides BlackBerry with a properly compelling smartphone after the overly expensive Priv and the uninspiring Dtek50, offering pretty high performance and solid security at a reasonable price. Such a shame then that it didn't come out 12 months ago.

Herald Sun

Call to arms on cyber attacks

Wednesday, 23 November 2016

Byline: Annika Smethurst

Section: general

Melbourne - Cyber terrorism is a growing threat, and state-sponsored -attackers are using online technology to strike Australia, the Federal Government will warn today.
Just seven months after the Coalition launched a multi-million-dollar strategy to -tackle criminal and state--sponsored cyber attacks, Prime Minister Malcolm Turnbull will reveal that tech experts are also helping in the fight against Islamic State in Iraq and Syria.

"Less well known, but of increasing importance, is that this fight against Daesh is also conducted through cyberspace," Mr Turnbull is expected to say in a national security speech to parliament.

In recent years, the Federal Government has bolstered its defence against hi-tech heists, and appointed a minister to help defend the nation's cyber networks.

In an address to the National Press Club today, Dan Tehan, the Prime Minister's Assisting Minister on Cyber-security, will emphasise the need to stay "ahead of the game" in the face of growing cyber crime from hackers.

Mr Tehan is expected to urge the government to accelerate the rollout of its Cyber Security Strategy in the face of the growing threat.

"What we do today will prepare us for tomorrow," he says in a draft speech. "If we can do this, we can be confident in facing what comes next." Mr Tehan has identified a number of areas where the government could improve its online defence capabilities, -including better co-ordination between departments -- that he says should take "greater responsibility" for internet -security.

He believes governments and businesses should also be more open with the public about cyber attacks.

"We need to continue to be transparent when attacks occur and release this information to the public as soon as the details are known, and it is safe and secure to do so," Mr Tehan will say.He will also flag new laws and a "strong cop on the beat" to deter criminals and protect online information.

Australian Associated Press

Aust hits Islamic State in cyberspace

Wednesday, 23 November 2016

Byline: Max Blenkin and Roje Adaimy

Section: general

Canberra - Australia is conducting online warfare against Islamic State but Australian businesses, government organisations and individuals remain vulnerable to cyber attacks.
In a revelation about Australia's growing cyber capability, Prime Minister Malcolm Turnbull disclosed the Australian Signals Directorate had taken the fight against Islamic State into cyber space.

It was making "a real difference", he told parliament on Wednesday.

But neither Mr Turnbull nor his cyber security minister Dan Tehan would reveal any details of how that was being done.

Delivering a statement on national security, Mr Turnbull said cyber security operations were subject to the same rules of engagement that apply to other military capabilities.

That includes the six RAAF F/A-18 Hornets which have been bombing IS targets in Iraq and Syria whose rules are intended to minimse risk of harm to civilians.

Similarly Mr Tehan declined to discuss offensive cyber capabilities - though he said publicly available literature speculated on what could be done.

IS has long been adept at using the internet for its own purposes, using slick video productions to trumpet its successes and persuasive social media pitches to potential western converts.

Cyber attack could take the form of denying IS use of its computer networks, or penetrating their systems to steal information or compromise command and control.

One academic paper terms this type of attack as above espionage but below violence.

Australia certainly isn't going it alone against IS - the US also has a Cyber Command with advanced capabilities for defensive and offensive operations.

Mr Tehan warned of the devastating "cyber storm" in which attacks compromise power, telephone, emergency and financial networks.

Such attacks could be mounted by a foreign power, criminals or kids causing trouble. Cyber terrorism is an emerging threat.

"We are naive if we think that in Australia we are immune to any of these threats," the minister told the National Press Club.

Mr Tehan said everyone needed to do more to guard against the threat.

"All of us must be on notice - it is not a case of if but when government, businesses or individuals will be hit," he said.

Mr Tehan said there were areas where more needed to be done, including working with state and territory governments and businesses to better protect critical infrastructure.

We needed to recognise that links between government departments were where attackers would find vulnerabilities to exploit.

"When the Bureau of Meteorology was compromised it was most likely because it was seen as an entry to other organisations," Mr Tehan said.

New Straits Times

MCMC: 4,800 websites blocked from 2015 to Sept this year

Wednesday, 23 November 2016

Section: general

Kuala Lumpur - From 2015 to the end of Sept this year, 4,800 websites were blocked for various offences under the law, said the Ministry of Communications and Multimedia.
In a written reply in the Dewan Rakyat today, the ministry said some of the websites were blocked upon the request of the Royal Malaysian Police under the Common Gambling Houses Act 1953.

Replying to a question from Datuk Liang Teck Meng (BN-Simpang Renggam) who asked about the measures taken to censor websites, especially pornographic ones, the ministry said police had requested that 1,931 internet pornographic and gambling sites be blocked.

"At the same time, some sites were blocked upon the request of other enforcement agencies including the Health Ministry, the Ministry of Domestic Trade, Cooperatives and Consumerism, as well as Bank Negara Malaysia. "Action was also taken against advertisements which contravened the law," the ministry said.

The Malaysian Communications and Multimedia Commission (MCMC) had also taken steps to educate and increase awareness among consumers throughout the country on the positive use of the internet and practicing self-control.

According to the ministry's statement, the steps include applications for parental control tools which could be set up with the cooperation of the internet service provider.

The Hindu

Malware cleaning centre to start in a month

Wednesday, 23 November 2016

Byline: Staff Reporter

Section: general

Hyderabad - After missing deadlines for more than a year, a unique centre that can detect a virus and clean it from the digital gadgets and devices might finally see the light of the day. The Botware Cleaning and Malware Analysis Centre will be operational within a month, said Ministry of Electronics and Information Technology Additional Secretary Ajay Kumar.
He said that the centre can be utilized by the citizens to clean up their mobiles, laptops and PCs. The facility had to come up last year as part of the digital India programme.

Speaking at the launch of the second edition of the Cyber Security Conclave on Tuesday, Mr. Kumar informed that the tendering process for setting up National Cyber Coordination Centre is in its final stages. The Centre will report on possible cyber threats in the Indian cyber space and protect it from breaches, he said adding that it will be operational from March 2017.

Listing out the initiatives taken up by the Central Government in the field of cyber security, he said that they are also working on developing strategies to safeguard biometric and financial database of various institutions of the country.

"In all 24 per cent of the Indian companies are exposed to cyber attacks as against the global average of 15 per cent," said Mr. Kumar. "We have written to the ministries and companies of major sectors like banking, petroleum, IT and others to have CISO (Chief Information Security Office) in every organisation."

He said that cyber threats are a matter of concern and that IT industry also has to join hands as the Government alone cannot tackle this menace.

Minister for IT, Telangana, K.T. Rama Rao said that the shortage of cyber security experts presented an opportunity for youngsters in terms of employment. He said that in the backdrop of demonetization and subsequent increased use of online transactions, the challenges in cyber space have increased multiple times.

NASSCOM (National Association of Software and Services Companies) Chairman C.P. Gurnani said that the cyber security market is expected to be around $35 Billion with a requirement of one million cyber security experts. The two-day conclave is being organised by Society for Cyberabad Security Council and Kenes Exhibitions.

Jerusalem Post

IAI introduces system to prevent collisions between civilian and military aircraft

Wednesday, 23 November 2016

Byline: Anna Ahronheim

Section: general

Jerusalem - The first military system to prevents mid-air collisions between civilian and military aircraft has been introduced by Israel Aerospace Industries.
The Collision Warning System (CWS), is an "innovative, lifesaving solution designed to warn combat pilots in situations when potential collision with commercial and civilian aircraft is imminent," according to an IAI statement.

The system monitors non- military aircraft by integrating two independent systems; one is known as "Interrogation Friend/Foe," and the other as "Automatic Dependent Surveillance- Broadcast."

The breakthrough technology was developed by the industry's MALAM Division to create an aerial picture that "provides a complete air situational picture, with warnings visible only to the military pilot."

And though civilian aircraft pilots do not get any collision avoidance warnings, military pilots get three: one by voice; one by graphic indicators sent via a tablet panel; and one by symbols presented on the plane's cockpit displays.

Designed for fourth and fifth generation fighter jets, training aircraft, military helicopters and remotely piloted aircraft, the CWS plots existing and projected flight paths of all aircraft flying in the area. The military pilot then receives a detailed picture that shows the proximity of any civilian aircraft and the potential risk of collision.

On July 7 2015, two people were killed when a civilian and military aircraft collided in the United States. According to the National Transportation Safety Board, the F-16 pilot had been aware of the civilian Cessna, and had even been advised by air traffic control to avoid colliding with it.

But, according to the military pilot, there was no visual confirmation on the civilian aircraft until it was 500 feet in front of his plane, and despite the attempts at avoidance, the two aircraft did ultimately collide.

"The growing congestion of the airspace and lack of integration between military and civil air spaces requires new, independent solutions to prevent collisions. Such systems will improve flight safety without compromising operational freedom," said Jacob Galifat, General Manager of the IAI/MALAM Division.

"The CWS we are introducing today combines the independence, operational freedom, ease of integration and affordability which are so important for the military operator, enabling military pilots to fly safely, without risk to civilian or military aircraft nearby in both training and operational flights." The system is currently being tested by several leading air forces.

Gulf News

Cybercrime cost UAE Dh5.14b this year

Wednesday, 23 November 2016

Byline: Naushad K. Cherrayil

Section: general

Dubai - The financial cost of cybercrime to the UAE has reached $1.4 (Dh5.14) billion to date this year, an increase of 4.9 per cent as hackers take advantage of consumer complacency, said an industry expert. Globally, the financial cost decreased by 16 per cent to $125.9 billion this year.
Tamim Taufiq, head of Norton Middle East, told Gulf News that the rise in the financial cost in the UAE is due to multiple reasons. The country has become the ideal target for hackers due to the high penetration rates of smartphones (over 83 per cent), adoption of new technologies, and the high profile this country has internationally.

He said that 2.53 million consumers were affected by cybercrime in the UAE this year compared to two million last year, an average of 31.5 hours per victim dealing with the consequences compared to 30 hours last year.

Globally, 689.4 million consumers were affected and an average of 19.7 hours per victim to deal with the consequences.

Consumers around the world lost an average of 21 hours (for perspective that's the entire next season of Arrested Development) over the past year dealing with the fallout from online crime, and nearly $358 on average per person, enough for a year of home security monitoring

Taufiq said that the UAE consumers are the most likely to continue engaging in risky online behaviour, leaving themselves vulnerable to further attacks.

According to Norton Cyber Security Insights Report, nearly seven out of 10 people know they must actively protect their information online, yet are still willing to click on links or open malicious attachments from senders they don't know.

"Consumer complacency and risky online behaviours are helping hackers reap rewards from their efforts as they continue to hone their craft and adapt scams. Millennials are the most commonly affected by the crime, with 53 per cent having experienced it within the past year," he said.

"Our findings show that people are growing increasingly aware of the need to protect their personal information online, but aren't motivated to take adequate precautions to stay safe," he said.

While consumers remain complacent, he said that hackers are refining their skills and adapting their scams to further take advantage of people, making the need for consumers to take some action increasingly important.

The report said that 49 per cent indicate that it is now harder to stay safe and secure in the online world than in the real, physical world while 59 per cent said they believe entering financial information online when connected to public WiFi is riskier than reading their credit or debit card number aloud in a public place.

Experiencing cybercrime is a potential consequence of living in a connected world, but he said that consumers still remain complacent and demonstrate risky online habits when it comes to protecting their personal information online.

"UAE consumers are still willing to click on links from senders they don't know or open malicious attachments. Three in ten (30 per cent) cannot detect a phishing attack, and another nine per cent have to guess between a real message and a phishing email, meaning nearly four in 10 are vulnerable," he said.

When asked to identify a real and fake banking email, he said that a third (39 per cent) of the UAE consumers was vulnerable to falling for the phishing e-mail. Moreover, those who have been phished, a majority (87 per cent) experienced a negative outcome such as an account or data compromise.

Khaleej Times

Cybercrimes are on the rise in UAE

Wednesday, 23 November 2016

Byline: Bernd Debusmann Jr.

Section: general

Dubai - More than 2.5 million consumers in the UAE have been the victims of cybercrime in the last year, according to newly released data from cyber security giant Norton by Symantec.
The Norton Cyber Security Insights Report - with 21,000 consumers globally and 883 in the UAE - estimates that 2.53 million consumers have fallen victim, each of whom have had to spend an average of 31.5 hours dealing with the consequences.

"It's definitely an increase from the last time we did the survey, which initially found that about 2.1 million people had fallen victim," said Tamim Taufiq, Head of Norton Middle East.

"There's not one particular reason we can pinpoint, but there are a few key factors," he added. "The UAE has one of the highest smartphone penetration rates globally, and there's also a perception among cybercriminals that people in the UAE are wealthy, so it's good to target them."

In the UAE, millennials were found to be the most affected, with 53 per cent saying they'd experienced it in the last 12 months.

"Millennials are more connected in general than Generation-X and the 'Golden Oldies'," explained Taufiq. "They're also more risk averse. They exhibit very slack security habits. They share their passwords easily, for example."

Men (52 per cent) and frequent travellers (50 per cent) were also likely to fall victim.

Regarding travellers, Taufiq noted that the need to be constantly connected in different locations makes them an attractive target to cyber criminals on the prowl.

"They access public Wi-Fi networks which aren't necessarily secure," he said. "It's all about having access to information and being connected wherever they are.

"People with smartphones and tablets don't necessarily have them protected," he added. "They access social media accounts, share personal information, and sometimes even make transactions online on unsecure networks."

Alarmingly, despite growing public awareness of the risks, many continue to be complacent about taking security measures necessary to safeguard their personal information. A majority of people - 68 per cent - noted that while they understand the need to protect their privacy, they are still willing to click on links from senders they don't know.

"We know that cyber crime is inevitable and is part of living in a connected world," Taufiq noted. "But human nature comes into play. Even victims of cyber crimes fall back into old habits."

Taufiq added that the only way to prevent falling victim to cyber criminals is to take common-sense security measures on "any and all" connected devices.

The report also found that 55 per cent of local consumers believe that safety should be self-taught, which - given the general ignorance of security practices - Taufiq says presents a danger.

"It's about creating good habits. Reject complacency. Make sure every device you use is protected," he said. "People need to be educated about safety tips. If you don't know the source of the e-mail, don't click on it. Avoid sharing or using the same passwords."

Associated Press

Interpol: Use biometric data to find extremist fighters

Tuesday, 22 November 2016

Byline: Staff report

Section: general

The United Nations - Interpol urged all countries on Tuesday to obtain biometric data from fighters for the Islamic State and other extremist groups to help law enforcement track them down, especially when they return home.
Interpol Secretary General Jurgen Stock said in an interview with The Associated Press that the international police organization only has biometric data -- fingerprints, DNA, iris scans and the like -- for about 10 percent of the 9,000 "foreign terrorist fighters" in its database.

Stock said Interpol is helping countries to develop biometric technology not only to identify fighters from extremist groups but criminals as well.

He cited the case of "a terrorist" who attacked a police station in France last year who had traveled across Europe using 20 different identities -- something that could have been thwarted with biometric data.

Stock said there are an estimated 20,000 to 30,000 "foreign terrorist fighters" from almost all over the world -- and about 15,000 from over 100 countries remain mainly in Syria and Iraq.

With 9,000 names in the Interpol database, this means that about 6,000 of the extremist fighters are not on an international register where they could be tracked, which Stock said is a "serious gap."

But he said the database has grown rapidly when it started in 2013 with just 12 files, and will hopefully continue to add names and biometric data.

The Interpol chief came to the United Nations from the organization's headquarters in Lyon, France to speak to the General Assembly which adopted a resolution expanding the organizations cooperation with the U.N.

Stock called the Internet "a virtual university of terrorism," where extremist groups attract and radicalize would-be fighters, and where information on building or buying bombs and explosives is readily available.

"The threat level with regard to international terrorism is unprecedented," he said, with international "terrorists" moving to short- term actions using simpler methods such as knives, axes and in the deadly attack in Nice, France on July 15 a truck.

"We are fighting a terrorist network or an organized crime network with a law enforcement network," he said.

But Stock said it's "not easy" because of legal issues which differ in various countries, including on sharing information, and the difficulties in ensuring that relevant data gets to police, border guards and other officials who need it.

He said the increasing use of encrypted websites by extremist groups is also posing "a huge challenge to law enforcement" authorities trying to conduct surveillance or track fighters and potential "terrorists."

The "dark net" has also become a major trading place for weapons and explosives used by "terrorists," Stock said.

"Investigations into the dark net are not impossible, of course," he said. "We are developing our tools, but it creates a challenge."

Stock also said Interpol is cooperating with industry on new tools "to make sure that there's no safe haven for terrorists or criminals."

Fox News Latino

Sources: Utah man held in Venezuela likely to be released by Dec. 6 as part of deal

Tuesday, 22 November 2016

Byline: Alex Vasquez S.

Section: general

Caracas - Joshua Holt, the Utah man imprisoned in Venezuela on weapon charges for almost five months now, is included on a list of 21 political prisoners the government has agreed to release in the following weeks, according to a source familiar with the ongoing negotiation with the opposition.
"He's on the list. The government is also expected to release two congressmen, journalists, Twitter users, students and protesters," the source, who asked to remain anonymous, told Fox News Latino.

He said the release should happen on or before Dec. 6, the date set for Holt's court hearing - the fourth one, after the first three were suspended - and also the date set for a third round of negotiations between the two sides of the deeply divided Venezuela.

Jeannette Prieto, lawyer of the Utah man, said she visited the 24-year-old, a member of the Church of Jesus Christ of Latter-day Saints, on Monday and found him in good condition. "He's fine. A doctor had seen him [the previous] Thursday and they will run some medical tests, but he's OK," she told FNL.

According to the unidentified source, the complaint of "cruel and inhumane treatment" brought by Prieto last month has been decisive in bettering Holt's living conditions.

Edder Jimenez, president of the Church of Jesus Christ of Latter-day Saints in Caracas, has been monitoring the case of Holt and his wife, Thamara Caleño Candelo, also a Mormon, since the beginning of their ordeal.

He said that the postponement of hearings has affected his mood, but he remains hopeful. "He has strengthened spiritually. He has his Bible and we pray for this process to end well," Jimenez said.

Holt and his Venezuelan wife face weapons charges after authorities during a raid allegedly found a small arsenal they say was intended to assist the U.S.'s efforts to undermine President Nicolás Maduro's socialist rule. Holt and his wife have insisted that the weapons were planted.

The mediation of Under Secretary of State for Political Affairs Thomas Shannon is deemed crucial in the dialogue process. He visited the South American country in late October and allegedly held a meeting with Venezuelan President Nicolás Maduro on Oct. 31.

Six political prisoners have been released since Oct. 30, when the government and the opposition started a dialogue. One of them was longtime prisoner Rosmit Mantilla, a congressman from the opposition detained on May 2, 2014 during a protest against President Nicolas Maduro. He was released on Nov. 17.

According to the NGO Foro Penal Venezolano, 108 political prisoners remain behind bars in Venezuela.

The opposition says the government uses intimidation tactics to keep them quiet.

The government is known for its use of blackmail, FNL's source said. "They release a political prisoner and then they demand that we silence ourselves, that we don't criticize them. If we do, they won't release any other prisoners."

The Intercept

U.K. Parliament Approves Unprecedented New Hacking and Surveillance Powers

Tuesday, 22 November 2016

Byline: Ryan Gallagher

Section: general

Washington - A few years ago, it would have been unthinkable for the British government to admit that it was hacking into people's computers and collecting private data on a massive scale. But now, these controversial tactics are about to be explicitly sanctioned in an unprecedented new surveillance law. Last week, the U.K.'s Parliament approved the Investigatory Powers Bill, dubbed the "Snoopers' Charter" by critics. The law, which is expected to come into force before the end of the year, was introduced in November 2015 after the fallout from revelations by National Security Agency whistleblower Edward Snowden about extensive British mass surveillance. The Investigatory Powers Bill essentially retroactively legalizes the electronic spying programs exposed in the Snowden documents -- and also expands some of the government's surveillance powers.

Perhaps the most controversial aspect of the new law is that it will give the British government the authority to serve internet service providers with a "data retention notice," forcing them to record and store for up to 12 months logs showing websites visited by all of their customers. Law enforcement agencies will then be able to obtain access to this data without any court order or warrant. In addition, the new powers will hand police and tax investigators the ability to, with the approval of a government minister, hack into targeted phones and computers. The law will also permit intelligence agencies to sift through "bulk personal datasets" that contain millions of records about people's phone calls, travel habits, internet activity, and financial transactions; and it will make it legal for British spies to carry out "foreign-focused" large-scale hacks of computers or phones in order to identify potential "targets of interest."

"Every citizen will have their internet activity -- the apps they use, the communications they send, and to who -- logged for 12 months," says Eric King, a privacy expert and former director of Don't Spy On Us, a coalition of leading British human rights groups that campaigns against mass surveillance. "There is no other democracy in the world, possibly no other country in the world, doing this."

King argues that the new law will cause a chilling effect, resulting in fewer people feeling comfortable communicating freely with one another. He cites a Pew survey published in March 2015 that found that 30 percent of American adults had altered their phone or internet habits due to concerns about government surveillance. "It's going to change how people communicate and express their thoughts," King says. "For a society that's supposed to be progressive, that encourages open debate and dialogue, it's awful."

Other civil liberties advocates are concerned that the new law will be viewed by governments across the world as a green light to launch similar sweeping surveillance regimes. "The passing of the IP Bill will have an impact that goes beyond the U.K.'s shores," says Jim Killock, executive director of the London-

based Open Rights Group. "It is likely that other countries, including authoritarian regimes with poor human rights records, will use this law to justify their own intrusive surveillance powers."

Despite the broad scope of the Investigatory Powers Bill, it generated little public debate in the U.K., and did not receive a great deal of coverage in the mainstream press. One reason for this was undoubtedly the U.K.'s shock vote in June to leave European Union -- known as Brexit -- which has dominated news and discussion in recent months. But there was another major factor for the swift passage of the law in the face of little backlash. The Labour Party, the U.K.'s leading opposition political party, had pledged to fight back against "unwarranted snooping," but ended up supporting the government and voting in favor of the new surveillance law. "Blame has to be fixed on the Labour Party," says Killock. "They asked for far too little and weren't prepared to strongly challenge many of the central tenets of the bill."

In an effort to placate some of its critics, the government has agreed to strengthen oversight of the surveillance. The Investigatory Powers Bill introduces for the first time a "judicial commissioner" -- likely a former senior judge -- who will have the authority to review spying warrants authorized by a government minister. It also bolsters provisions relating to how police and spy agencies can target journalists in a bid to identify their confidential sources. New safeguards will mean the authorities will have to seek approval from the judicial commissioner before obtaining a journalist's phone or email records; previously they could obtain this data without any independent scrutiny.

The U.K.'s National Union of Journalists, however, believes that the law does not go far enough in protecting press freedom. The union is particularly alarmed that any potential surveillance of media organizations will be kept completely secret, meaning they will not be afforded the chance to challenge or appeal any decisions relating to them or their sources. "The bill is an attack on democracy and on the public's right to know and it enables unjustified, secret, state interference in the press," the union blasted in a statement last week, adding that "the lack of protection for sources has an impact on journalists working in war zones or those investigating organized crime or state misconduct."

Other issues relating to how the law will be applied remain unclear. It contains a provision, for instance, allowing the government to serve a company with a "technical capability notice," which can include "obligations relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data." Earlier this year, technology giants Apple, Facebook, Google, Microsoft, Twitter, and Yahoo criticized this power, expressing concerns that it could be used by the government to force companies to weaken or circumvent encryption technology used to protect the privacy of communications and data.

In practice, if the law is used to undermine encryption, it may never come to light. The government included a section in the law that criminalizes "unauthorized disclosures" of any information related to its surveillance orders, which could potentially deter any whistleblowers or leakers from coming forward. The punishment for breaches is a prison sentence of up to 12 months, a fine, or both.

Though the Investigatory Powers Bill will soon to come into force, it is likely to face several lawsuits. There are at least three ongoing cases that could result in changes to some of its provisions. One of these cases is a major challenge in the European Court of Human Rights, which could potentially rule the government's mass collection and retention of data to be illegal. (Judgments from the European Court of Human Rights remain binding in the U.K., despite its vote to leave the European Union.)

Either way, some are not willing to leave it up to the courts to determine how much of their data the government can vacuum up. One recently established British nonprofit company, calling itself Brass Horn Communications, says it is planning to build a new internet provider that is based on Tor -- a tool used to browse the internet anonymously -- in an effort to help people protect themselves from the spying. "We should be able to research an embarrassing medical condition, or ask questions on Google, without having to worry about it being stored on a permanent internet record somewhere," says a spokesperson for the company. "The government has decided that everyone is a suspect, but you can't treat an entire society as criminal."

Tribune de Genève

Un informaticien indiscret du SRC devant la justice

Wednesday, 23 November 2016

Byline: Lucie Monnat

Section: general

Berne - Le procès de l'homme qui a volé des données du Service de renseignement s'ouvre aujourd'hui.
On avait frôlé la catastrophe
Cette affaire avait fait l'effet d'un séisme au sein du Service de renseignement de la Confédération (SRC). En mai 2012, Carlo B. , alors informaticien spécialisé dans les banques de données au sein du SRC, est arrêté pour avoir dérobé 507. 1 GByte de données dans le but de les revendre. L'équivalent, environ, d'un document de deux millions de pages. Son procès s'ouvre ce matin au Tribunal pénal fédéral (TPF) de Bellinzone. Accusé de service de renseignements politiques aggravé et tentative de violation du secret de fonction, il risque 3 ans de prison maximum.

L'affaire est hors norme, et les faits relatés dans l'acte d'accusation sont à la limite du rocambolesque. En mai 2012, Carlo B. , alors en congé maladie, se rend plusieurs fois dans les bureaux du SRC à Berne. Il y télécharge et copie illégalement 159 fichiers du système de sécurité du SRC contenants des données sensibles, « non seulement confidentielles mais également classifiées » . Dans les fichiers, on trouve des informations détaillées sur des coopérations effectuées avec des services étrangers, des opérations de

renseignement, des données sur les marchés ou encore la totalité des échanges de mails du personnel du SRC, membres de la direction compris.

Carlo B. est peut-être fourbe, mais il ne fait pas partie des plus malins. Quelques jours après le vol, il se rend dans une filiale bernoise d'UBS pour se renseigner sur les modalités d'ouverture d'un compte à numéros. Il confie même à l'employé de banque qu'il attend le versement d'une somme variant entre 100 000 et 1 million de francs, fruits d'une vente de données. L'employé de banque a la puce à l'oreille. Il sent que son client, en tant qu'informaticien du SRC, a accès à des données mais qu'il ne marchande pas celles-ci à la demande de ses employeurs. Il le signale à la police, qui perquisitionne le domicile de Carlo B. Les policiers y trouvent, entre autres, une lettre d'offre en anglais proposant son magot pour un montant de 100 000 francs, « probablement à des partis ou des organisations étrangères » , présume le Ministère public. Carlo B. est arrêté avant d'avoir pu transmettre quoi que ce soit.

Bien que la catastrophe ait pu être évitée, la facilité avec laquelle cet employé a pu agir choque la Suisse entière. Quelques mois plus tard, un rapport de la Délégation des commissions de gestion du parlement émet de sévères critiques envers le directeur du SRC, Markus Seiler, et le ministre de la Défense d'alors, Ueli Maurer. Ni l'un ni l'autre n'auraient rempli leur devoir de surveillance. Depuis, 40 mesures ont été prises.

D'origine italienne, Carlo B. , 48 ans aujourd'hui, vit désormais à Salerne (I). Reste à savoir s'il se présentera à son procès. Il bénéficie toutefois d'un sauf-conduit, ce qui signifie qu'il ne peut être arrêté pendant son séjour.

Le Temps (Suisse)

Vers un Google du renseignement suisse

Wednesday, 23 November 2016

Byline: Mehdi Atmani

Section: general

Berne - Surveillance Achat de logiciels d'interception, embauche de personnel, écoutes renforcées: après le plébiscite dans les urnes le 25 septembre dernier, l'heure est à la mise en oeuvre de la loi sur le renseignement. Quels sont les plans de la Confédération?
Le 25 septembre, deux tiers des Suisses ont décidé de muscler les moyens d'action du Service de renseignement de la Confédération (SRC). Les espions helvétiques pourront désormais mener des opérations de surveillance préventive dans des espaces privés: écoutes téléphoniques, intrusion dans

des réseaux informatiques, surveillance des réseaux câblés, c'est-à-dire le réseau filaire par lequel transitent les communications électroniques (courriels, téléphonie, Internet). Mais tout cela est encore très théorique. En pratique, le SRC va d'abord devoir repenser son organisation en profondeur et renouveler sa boîte à outils. Après le plébiscite dans les urnes, l'heure est à la mise en oeuvre.

Le SRC a publié une feuille de route précise pour la mise en oeuvre de la loi sur le renseignement. Elle entrera en principe en vigueur le 1er septembre 2017. Dès la mi-octobre 2016, les offices cantonaux ont démarré la consultation des trois ordonnances d'application, qui portent sur le service de renseignement, les systèmes d'information et de stockage électronique du SRC, ainsi que sur l'autorité de surveillance indépendante.

Ces ordonnances seront élaborées avec les Commissions de la politique de sécurité du parlement et la Délégation des Commissions de gestion (DélCdG), qui conservera un droit de regard sur les activités du SRC. De janvier à avril 2017, ces ordonnances seront mises en consultation publique. Une deuxième consultation des offices est prévue en juin 2017, pour déboucher, en principe en août, sur l'arrêté du Conseil fédéral.

Un effectif renforcé

L'effectif du SRC sera renforcé pour assumer ses nouvelles missions. La nouvelle loi prévoit l'embauche de 20 nouveaux collaborateurs entre 2017 et 2019. A terme, les trois quarts (16) de ce personnel seront affectés au service de renseignement pour « la mise en oeuvre des mesures de recherches spéciales soumises à autorisation », explique Isabelle Graber, porte-parole du SRC. Parmi eux, des techniciens opérationnels pour le suivi des moyens de recherche soumis à autorisation du Tribunal administratif fédéral et du chef du Département de la défense.

Concrètement, ce sont ces nouveaux employés qui pourront mener les intrusions dans les réseaux câblés ou demander la mise sur écoute d'un individu. Ils devront préalablement justifier la nécessité de cette mission et obtenir une autorisation valable six mois. La loi prévoit aussi l'embauche d'analystes pour l'évaluation des informations obtenues, et de juristes pour la préparation des demandes d'autorisation. Le solde restant sera réparti entre le Tribunal administratif fédéral (un poste), la base d'aide au commandement (deux) et les Archives fédérales (un). Les premiers postes seront mis au concours en janvier 2017 pour une entrée en fonction au mois de juillet.

Nouveauté: la loi prévoit la création d'une autorité de surveillance du service de renseignement. Aujourd'hui, la surveillance du SRC est rattachée au secrétariat du Département fédéral de la défense. C'est donc l'armée qui jette un oeil sur les activités des espions. Selon le calendrier prévu, le Conseil fédéral nommera en février prochain le chef de l'autorité de surveillance en tenant compte de la proposition de Guy Parmelin. Cette autorité disposera de son propre budget et engagera son propre personnel. Aucun chiffre n'est pour l'heure articulé.

Dans la future boîte à outils du SRC, l'exploration du réseau câblé par lequel transitent les communications électroniques (courriels, téléphonie, Internet) est la mesure de surveillance qui a cristallisé toutes les critiques durant la campagne. La nouvelle LRens autorisera en effet le SRC à intercepter en continu toutes les communications internationales qui transitent par la Suisse via le réseau câblé. Avec l'aval du Tribunal administratif fédéral et de la Délégation pour la sécurité du Conseil fédéral, le SRC pourra filtrer les courriers électroniques, procéder à des écoutes téléphoniques par Internet, et rechercher des informations dans le réseau câblé par catégorie de mots- clés.

En Suisse, la surveillance se fera sur les noeuds où convergent et transitent les données. Le SRC ne pourra rechercher que des informations sur des « événements importants en matière de politique de sécurité se produisant à l'étranger » . Les données qui ne correspondraient pas à ce critère devront être détruites. L'habilitation du SRC est également valable dans le cas d'une « menace pour la sécurité intérieure » ainsi que pour « préserver les intérêts nationaux d'une grande importance » .

Seules les données transitant par le réseau câblé suisse vers des fournisseurs étrangers seront surveillées. L'utilisation des données collectées entre expéditeur et destinataire situés en Suisse sera interdite. Pour autant que leurs adresses e-mails soient enregistrées auprès d'un fournisseur d'accès à Internet (FAI) en Suisse.

Prenons l'exemple d'un courrier électronique envoyé de Lausanne à Saint-Gall. Si le destinataire utilise une adresse Gmail ou appartenant au service de messagerie allemand GMX, le courriel transitera par les serveurs de Google à l'étranger ou par l'Allemagne, traversera momentanément les frontières helvétiques et pourra donc être intercepté. Le projet de loi précise que « les exploitants suisses de réseaux câblés ainsi que les fournisseurs suisses de prestations de télécommunications » fournissent « des renseignements sur les itinéraires des flux de données et, sur ordre, en détournant les flux de données en question » .

« Garantir un contrôle fiable »

Toutes les agences internationales de renseignement n'utilisent plus seulement des motsclés, mais surtout des algorithmes. Ces méthodes de calcul permettent l'exécution optimisée de procédés répétitifs précis. Ceux-ci viennent enrichir des bases de données dans lesquelles l'information interceptée est structurée, puis mise en relation et enrichie avec d'autres informations, dites secondaires: adresse postale, abonnement de téléphone mobile, profil LinkedIn, c'est-à- dire les données personnelles d'un citoyen.

Cette technique du Deep Learning Management permet aux agences d'affiner au maximum l'information et d'en tirer le plus de sens possible. Elle fonctionne comme un Google du renseignement. Si les services suisses ont l'objectif de se mettre au niveau des techniques de collecte et d'analyse des agences internationales, ils devront employer les mêmes méthodes. Ce sont du moins les craintes des opposants à la LRens.

Pour explorer le réseau câblé, le SRC va s'appuyer sur des partenaires extérieurs. Dans le cadre de la LRens, c'est l'Autorité de contrôle indépendante (ACI) pour l'exploration radio qui sera désormais responsable de cette tâche. Selon Martin Wyss, président de l'Autorité, tout est encore très théorique. « Nous avons rédigé notre futur cahier des charges. Nous examinons actuellement comment l'assumer. Il n'est pas exclu que nous devions modifier nos méthodes de travail et notre fonctionnement. Et ce, pour garantir un contrôle fiable. »

Les nouvelles ambitions du SRC coûteront cher: 720 000 francs par an pour le nouveau personnel, 6 millions pour l'acquisition de matériel espion, 800 000 francs pour sa maintenance sans compter les frais de licence. A cela s'ajoutent les frais occasionnés par la surveillance des communications ellemême. « Elle coûte extrêmement cher, souligne François Charlet, juriste spécialisé en droit des technologies. En matière pénale, une telle surveillance se chiffre à plusieurs milliers de francs à la charge des autorités de poursuite. »

Puis viennent les coûts d'acquisition et d'investissements des nouveaux systèmes de surveillance. Selon le rapport du Conseil fédéral, ils se chiffrent entre « 5 et 7 millions de francs par an, auxquels il faut ajouter des frais ré cur rent s de que lque 800 000 francs pour la maintenance, l'adaptation et le coût des licences » .

En règle générale, poursuit le Conseil fédéral, « ces systèmes sont acquis et financés dans le cadre du programme d'armement » . Pour les mesures de recherche d'informations soumises à autorisation en Suisse, par exemple la localisation, la surveillance de données d'utilisation et de communication de raccordements de téléphonie fixe et mobile ou la surveillance d'accès à Internet, le SRC fera appel au service Surveillance de la correspondance par poste et télécommunication du Département fédéral de justice et police. Les frais de traduction des communications enregistrées se montent à 800 000 francs.

Quant aux coûts pour l'exploration des réseaux câblés, le Conseil fédéral les estime à « 500 000 francs. Certaines technologies, par exemple pour l'introduction dans des systèmes informatiques hautement sécurisés, ne sont encore que peu développées. Comme le marché pour ces systèmes est relativement limité et volatil et que les développements techniques dans ce domaine sont rapides, leurs coûts ne peuvent pour l'instant que faire l'objet d'estimations. »

Qui fournira les logiciels?

Pour garnir sa nouvelle boîte à outils, la Confédération va devoir acheter ce matériel. Mais auprès de quels fournisseurs? Isabelle Graber ne commente pas ce point. Mais le service de renseignement peut-il passer outre l'exigence d'un appel d'offres sur le marché public? Selon le juriste François Charlet, « il n'y a pas d'exceptions dans la LRens » .

Les nouveaux moyens du SRC permettront-ils d'assurer la crédibilité du renseignement suisse, et donc une collaboration plus soutenue avec les Etats étrangers? Une autre source au sein du renseignement

souligne « qu'il est clair que si la Suisse a davantage de moyens techniques, elle acquiert plus de crédibilité vis-àvis de ses partenaires étrangers et restreint sa dépendance » .

Quelques semaines après le vote, l'opposant à la nouvelle loi Balthasar Glättli accuse le coup, mais veille au grain. « Il y a toujours des termes et des définitions qui ne sont pas clairs dans le nouveau texte de loi, estime le président des Verts suisses. Nous allons veiller à ce que cela soit traduit de manière précise. Nous allons également veiller à ce que les nouvelles compétences du SRC ne soient pas utilisées de manière abusive. » Dans les faits, Balthasar Glättli mise beaucoup sur la procédure de consultation des ordonnances du Conseil fédéral. « J'espère qu'il tiendra compte de nos critiques. »

Chaque courriel transitera par les serveurs de Google à l'étranger ou en Allemagne et pourra être intercepté en Suisse

« Nous allons veiller à ce que les nouvelles compétences du SRC ne soient pas utilisées de manière abusive »

BALTHASAR GLÄTTLI, PRÉSIDENT DES VERTS SUISSES

Agence Belga

Nucléaire: les services belges n'ont rien trouvé dans le "darknet"

Tuesday, 22 November 2016

Byline: Journaliste maison

Section: general

Bruxelles - Ni les services de sécurité, ni une société privée n'ont trouvé sur le "darknet" des documents relatifs aux installations nucléaires belges qui auraient mis en péril la sécurité de celles-ci, a indiqué mardi le directeur du Centre de cybersécurité, Miguel De Bruycker, devant la sous- commission "sécurité nucléaire" de la Chambre.
Les journaux de SudPresse ont relaté le mois passé la façon dont ils avaient trouvé sur le "darknet" (des réseaux de partage anonymes utilisés en général par des criminels) des plans des centrales nucléaires de Tihange. Le Centre de cybersécurité en a immédiatement référé à la Sûreté de l'Etat et aux renseignements militaires (SGRS) afin de savoir si des documents mettant en jeu la sécurité des installations nucléaires se trouvaient dans le "darknet". Une société privée a également été consultée et un "pirate éthique" a proposé ses services.

"Aucune de nos sources d'information n'a trouvé les plans des installations nucléaires de Tihange ou des documents d'installations nucléaires qui comportaient un risque sérieux de sécurité", a expliqué M. De Bruycker.

Les seules indications retrouvées visaient un document disponible sur le serveur d'un sous-traitant à l'étranger. L'information n'était toutefois pas suffisamment concrète.

Certains députés se sont demandés s'il fallait en conclure qu'il n'y avait pas eu de document sur le net. Le directeur n'a pu fournir une réponse définitive. "Les documents n'y sont peut-être pas, ou peut-être y a-t-il autre chose. C'est chercher une aiguille dans une botte de foin", a-t-il souligné.

Le Devoir
Protection des sources - Une loi nécessaire
Thursday, 24 November 2016
Byline: Manon Cornellier

Editorial - Perquisitions, saisies de notes, collecte de relevés d'appels téléphoniques... Les corps policiers ne ménagent pas leurs efforts pour identifier les sources de journalistes qui dérangent. Les tristes révélations des dernières semaines au Québec ont tout de même eu un effet positif. Elles ont ravivé l'intérêt pour une loi sur la protection des sources journalistiques et ont poussé au moins un parlementaire fédéral à l'action, le sénateur conservateur Claude Carignan.Secoué par les révélations sur la surveillance policière d'une dizaine de journalistes québécois, le gouvernement Couillard a rapidement réagi en créant entre autres une Commission d'enquête sur la protection de la confidentialité des sources journalistiques. Cette dernière doit faire rapport d'ici le 1er mars 2018 et pourra aller jusqu'à recommander l'adoption d'une loi sur la protection des sources journalistiques. C'est loin, 2018, et une loi sur la protection des sources ne peut avoir de dents sans mettre le fédéral dans le coup. Le Code criminel et les dispositions autorisant la délivrance de mandats relèvent de lui.

Pour l'instant, le fédéral n'affiche aucune volonté d'agir et tente d'apaiser tout le monde. Le premier ministre Justin Trudeau et le ministre de la Sécurité publique, Ralph Goodale, disent avoir obtenu l'assurance de la GRC et du Service canadien de renseignement de sécurité (SCRS) qu'aucun journaliste n'était " actuellement " sous surveillance. Mais qu'en est-il des années passées ? M. Goodale ne le sait pas et ne l'a pas demandé parce que ce qui compte, c'est le présent, dit- il.

Rien de rassurant quand on se souvient de la perquisition de la GRC, effectuée en 2004, chez la journaliste Juliet O'Neill ou de la filature, en 2007, de deux journalistes de La Presse. Actuellement, la GRC exige les messages numériques échangés entre le journaliste de Vice Ben Makuch et un Canadien s'étant joint au groupe État islamique. L'affaire est en appel et si M. Makuch perdait et refusait toujours de remettre ses messages, il pourrait se retrouver en prison.

La protection des sources est un principe fondamental en journalisme. Le travail journalistique, surtout d'enquête, est impossible sans une relation de confiance entre un reporter et la personne qui accepte, souvent à grands risques, de lever le voile sur des malversations ou des problèmes au sein d'un gouvernement, d'une entreprise ou d'une organisation. Si les journalistes deviennent malgré eux des outils policiers, on se méfiera d'eux, les empêchant d'alerter le public de ce qui se passe dans l'ombre. Alors pas de commission Charbonneau, pas de mise en lumière des problèmes dans le système de santé, pas de projecteurs sur les dérives de certaines institutions... C'est la liberté de presse qui écope.

Une loi, comme il en existe ailleurs et comme le demandent les journalistes québécois depuis quelques décennies, est nécessaire pour protéger la confidentialité de ces sources et les mettre à l'abri de représailles.

Le sénateur Carignan en est lui aussi convaincu. Devant ce qu'il appelle les tergiversations d'Ottawa, il a décidé de présenter un projet de loi mardi qui répond largement aux inquiétudes soulevées par les membres de la Fédération professionnelle des journalistes du Québec lors de leur congrès de la fin de semaine dernière.

En vertu de ce projet de loi, seul un juge d'une cour supérieure pourrait accorder un mandat de perquisition, d'écoute ou de surveillance contre un journaliste. Pour guider sa décision, le projet de loi établit une série de critères où figurent la liberté de presse et les conséquences de la divulgation sur la source et le journaliste. Le fardeau de démontrer le respect des conditions énoncées dans la loi reviendrait au demandeur du mandat. Si ce dernier était accordé, tout matériel recueilli devrait être mis sous scellés avant d'être consulté, copié, analysé ou utilisé. Le policier ou l'agent de renseignements voulant y avoir accès devrait en aviser le journaliste et son média, et ceux-ci auraient 10 jours pour contester la demande ou exclure des informations.

" Il s'agit d'un bon pas dans la bonne direction ", a réagi mercredi un des spécialistes du droit des médias présents au congrès, Me Mark Bantey. Selon lui, ce projet ouvre la porte à un débat sérieux sur des mesures concrètes.

Un autre de ses grands mérites est de mettre le gouvernement fédéral au pied du mur. Soit il attrape la balle au bond, soit il se défile et révèle ainsi ses vraies intentions.

Consultez tous nos textes sur le dossier des journalistes sous surveillance

L'Actualité
Le gouvernement vous écoute (encore plus que vous ne le pensez)
Wednesday, 23 November 2016
Byline: Naël Shiab

Ottawa - Sans qu'on s'en soit rendu compte, le Canada s'est doté d'une machine de surveillance digne de Big Brother.
Oublions un instant l'espionnage policier subi par les journalistes Patrick Lagacé, Alain Gravel, Isabelle Richer, Marie-Maude Denis et Vincent Larouche. Parlons de vous. Parlons de votre droit à la vie privée, qui s'est effrité petit à petit au fil des années.

Vos grands-parents pouvaient décider de partir au chalet pour la fin de semaine et personne ne le savait. Vous, c'est différent. Votre cellulaire indique constamment votre position à votre service téléphonique. L'application GPS que vous utilisez pour connaître le bon chemin vous suit également à la trace. Le petit café où vous vous arrêtez en cours de route offre le Wi-Fi gratuitement. Pendant que vous grignotez une pâtisserie, l'identifiant unique de votre téléphone et les sites Web que vous consultez sont gardés en mémoire. À la petite épicerie du village où vos grands-parents auraient payé comptant, vous avez sorti votre carte de crédit: l'opération a été enregistrée et sera conservée. Sur Facebook et

Instagram, vous publiez ces photos de magnifiques paysages enneigés, ajoutant une pièce de plus à votre autobiographie numérique.

Si quelqu'un obtient ces empreintes électroniques que vous disséminez lors de vos pérégrinations, il peut alors reconstituer votre existence. Vos déplacements, vos achats, vos loisirs, vos interactions sociales. Non seulement votre passé peut être fouillé, mais votre avenir proche peut être prédit.

«Et alors?» pensez-vous sans doute à ce moment. «Qu'est-ce que ça change si on sait que je suis allé au chalet? Je n'ai rien à cacher.»

C'est vrai, le chalet est anodin. Mais une clinique d'avortement? Le bureau d'un psychiatre? Une rencontre pour alcooliques anonymes? Une célébration religieuse? Et je ne parle même pas de vos achats. Un jouet sexuel? Une revue politique d'extrême droite ou d'extrême gauche?

«Bah! Qui s'intéresse à ma vie? Je ne suis personne...»

Peut-être bien. Pour l'instant. Mais beaucoup de choses ont changé ces dernières années. Auparavant, pour surveiller un suspect, il fallait une équipe de plusieurs personnes. Aujourd'hui, une seule derrière un écran peut en surveiller des milliers, voire des millions. Les autorités recueillent de gigantesques quantités de données, et les trient ensuite à la recherche de quelque chose de louche. Si vous êtes au mauvais endroit au mauvais moment, vos données peuvent faire partie du lot, être un jour ou l'autre utilisées, que vous soyez un suspect ou non, que vous le vouliez ou pas, et être conservées pendant une période indéterminée.

De nombreux indices glanés par les médias, recueillis par des fonctionnaires, déposés en preuve devant les tribunaux ou rendus publics par des lanceurs d'alerte portent à croire qu'une entité ayant de tels pouvoirs existe: notre gouvernement. Son objectif, louable, est de surveiller de potentielles menaces à notre sécurité et de nous en préserver. Mais peut-être avons-nous laissé s'emballer cette machine censée nous protéger.

Notre droit à la vie privée s'est dissous dans un océan de données ces dernières années et certains événements semblent tirés d'un film d'espionnage. Pourtant, tout est vrai. Toutes mes sources sont en hyperliens. Pour faciliter la compréhension, je vous présente tous les faits en ordre chronologique.

Comme le disait l'ancien chef du Centre de la sécurité des télécommunications du Canada, John Adams, lors d'une entrevue exclusive accordée à la CBC en octobre 2013: «Si vous êtes sur Internet, c'est littéralement comme si vous étiez sur la première page du Globe and Mail.» L'ancien militaire était aux commandes de cette agence de renseignements, aux activités secrètes, de 2005 à 2011. En mai 2014, devant le caucus des sénateurs libéraux, il y est allé d'une autre déclaration, cette fois à propos des internautes canadiens: «La moitié [d'entre eux] est stupide et l'autre moitié est stupide [aussi]. [.] Nous mettons davantage de choses sur Facebook que n'importe quel autre pays dans le monde. Nous ne

sommes pas très intelligents, nous avons beaucoup de chemin à faire.» Plutôt tranchant, pour celui qui était à la tête de l'une des plus importantes machines de surveillance du pays.

***

Au Canada, il existe deux agences fédérales spécialisées dans le renseignement: le Service canadien du renseignement de sécurité (SCRS) et le Centre de sécurité des télécommunications (CST). Le SCRS recueille et analyse des informations au Canada et à l'étranger pour déceler de potentielles menaces à la sécurité nationale. De son côté, le CST se spécialise dans la surveillance des télécommunications à l'étranger et dans la protection de l'infrastructure électronique de l'État. À elles deux, ces agences emploient 5 500 personnes et disposent d'un budget cumulé de 1,2 milliard de dollars pour 2016-2017.

Leur histoire remonte à la Deuxième Guerre mondiale. Les Forces canadiennes interceptaient des signaux électroniques cryptés en provenance d'armées étrangères. Des civils enrôlés au sein de la Sous-section de l'examen avaient pour mission de les déchiffrer. Après la guerre, en août 1946, la Direction des télécommunications du Conseil national de recherches est mise sur pied, et les 179 personnes qui tentaient de décoder les messages ennemis y sont intégrées. La création de ce nouveau service se fait grâce à un décret adopté en secret. Dès leurs débuts, les organismes de surveillance du Canada baignent dans une aura de mystère. L'organisme d'État travaillera dans l'ombre pendant trois décennies, avant d'être révélé au public par un documentaire de la CBC, en 1974. L'année d'après, il changera de nom pour devenir le Centre de sécurité des télécommunications.

La Sous- section de l'examen était une équipe civile qui avait pour mission de déchiffrer les signaux électroniques ennemis pendant la Deuxième guerre mondiale. (Photo: Centre de la sécurité des télécommunications)

En parallèle, pendant la guerre froide, la Gendarmerie royale du Canada est responsable de la collecte de renseignements liés à la sécurité nationale. Lors de la crise d'Octobre, en 1970, le gouvernement fédéral demande à la GRC d'accumuler des informations sur les militants souverainistes. Les policiers mettent en oeuvre «une vaste campagne de collecte de renseignements, d'infiltration, de harcèlement et de perturbation visant la quasi-totalité des manifestations du sentiment nationaliste au Québec». Une multitude d'actes illégaux sont commis par les agents, dont notamment l'entrée par effraction dans les locaux du Parti québécois et le vol de la liste de ses membres.

Plusieurs reportages révéleront au public les agissements des policiers. En 1977, la pression est trop forte: le gouvernement de Pierre Elliott Trudeau institue une commission d'enquête sur les activités de la Gendarmerie royale du Canada. On y apprend que les policiers mènent depuis des années des activités de surveillance qui n'ont jamais été autorisées par la loi, comme l'ouverture du courrier, par exemple. On recommande de retirer à la GRC la responsabilité du renseignement de sécurité. Selon la commission, l'équilibre entre la collecte de renseignements de sécurité et le respect des droits et libertés sera problématique tant que ce mandat restera entre les mains de policiers. En 1984, le

Parlement décide finalement de voter une loi pour créer une agence civile spécialisée: le Service canadien du renseignement de sécurité (SCRS).

À la fin des années 1980, le Service canadien du renseignement de sécurité et le Centre de sécurité des télécommunications sont donc en place. Mais deux événements changent radicalement la nature et l'ampleur des moyens à la disposition des agences: l'essor d'Internet et les attentats du 11 septembre 2001.

La loi antiterroriste de 2001 donne de nouveaux pouvoirs aux agences d'espionnage canadiennes, qui continuent de fonctionner dans le plus grand secret.

Dans les années 1990, les communications numériques envahissent rapidement la vie quotidienne. Pour les agences de surveillance, c'est à la fois une manne extraordinaire et un défi de tous les instants. D'une part, la technologie évolue sans arrêt et devient de plus en plus complexe, et d'autre part, les lois régissant les pouvoirs d'enquête ont été écrites avant ces bouleversements technologiques, laissant les agences dans des impasses ou des flous juridiques.

Puis, survient l'écrasement de deux avions contre les tours du World Trade Center, à New York, le 11 septembre 2001. La Loi antiterroriste est rapidement déposée à la Chambre des communes et entre en vigueur dès le 18 décembre de la même année. Les élus, craignant d'autres attaques, dotent les agences de nouveaux pouvoirs et de nouveaux moyens. Le budget du SCRS a plus que triplé depuis les années 2000. Les effectifs du Centre de sécurité des télécommunications ont quant à eux doublé depuis la mise en place de la Loi.

Auparavant, le CST était uniquement autorisé à saisir des échanges électroniques à l'extérieur du pays. La Loi antiterroriste lui permet désormais de surveiller les communications en partance ou à destination du Canada. Le Centre n'a pas le droit de surveiller des citoyens canadiens, mais le changement législatif rend cette option possible si des échanges ont lieu avec une entité étrangère. Le CST n'avait pas le droit non plus d'intercepter des communications privées. La nouvelle loi lui accorde aussi ce pouvoir, à condition d'obtenir l'autorisation spéciale du ministre de la Défense. Tous ces changements sont majeurs. D'ordinaire, les autorités doivent obtenir un mandat d'un juge, qui s'assure de façon indépendante que les enjeux de sécurité justifient un tel empiètement sur la vie privée des personnes. Mais le CST, lui, n'a pas à se conformer à ce protocole. La décision revient au ministre, qui peut déclencher l'interception de milliers de communications en une seule autorisation. Selon un reportage diffusé par Radio-Canada en 2013, le ministre en avait signé 48 depuis la nouvelle loi.

En décembre 2005, le New York Times révèle que l'ancien président George W. Bush a secrètement autorisé l'espionnage de centaines, voire de milliers de citoyens aux États-Unis, et ce, sans aucun mandat, après les attentats du 11 septembre 2001. La même chose s'est-elle produite avec son équivalent canadien, le Centre de sécurité des télécommunications? Le commissaire du CST, l'ancien juge en chef de la Cour suprême du Canada Antonio Lamer, veut en avoir le coeur net. Son rôle est de s'assurer que l'agence d'espionnage respecte les lois, notamment la Charte canadienne des droits et

libertés. Dans des documents obtenus par La Presse Canadienne en 2006, on apprend qu'une enquête interne de deux mois a été menée. Mais les documents sont hautement confidentiels et de nombreuses parties ont été censurées. Les conclusions du commissaire devaient être déposées devant le Parlement, dans son rapport annuel. Finalement, le document en question apporte bien peu de réponses. Aucune conduite illicite de la part du Centre n'a eu lieu, conclut le rapport, sans donner de détails.

Antonio Lamer (à gauche) et Charles D. Gonthier (à droite), deux anciens juges de la Cour suprême qui ont été commissaires du Centre de la sécurité des télécommunications. (Photo: Cour suprême du Canada)

L'année suivante, un nouveau commissaire entre en fonction, Charles D. Gonthier, lui aussi ancien juge à la retraite. Son rapport donne un aperçu beaucoup plus clair des opérations de surveillance du CST. En vertu de la loi, il est strictement illégal pour le Centre d'espionner expressément des citoyens canadiens, mais «lorsqu'il recueille des renseignements étrangers, le CST peut incidemment acquérir des renseignements personnels sur des Canadiens». Le Centre peut conserver ces renseignements s'il «les juge indispensables à la compréhension des renseignements étrangers». De plus, il peut divulguer ces informations, par exemple à la GRC, si un mandat est obtenu. Le CST peut aussi aider d'autres agences fédérales à collecter des renseignements, y compris sur des Canadiens, si un mandat a été obtenu.

À la fin des années 2000, la capacité de surveillance de masse du CST et du SCRS sont encore peu connus. Le rôle du CST, par exemple, est d'«acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information». Mais qu'est-ce que cela signifie concrètement? Les citoyens et les élus n'ont pas la moindre idée de l'ampleur des opérations qui sont menées. En vertu de la loi, ces agences ne rendent des comptes qu'au ministre de la Défense, qui est lui-même tenu au secret.

Survient alors le 9 juin 2013: le lanceur d'alerte Edward Snowden entre en scène et lève le voile sur les opérations les plus secrètes du gouvernement.

Pour la première fois, grâce au lanceur d'alerte Edward Snowden, les Canadiens découvrent l'ampleur des opérations de leurs agences d'espionnage.

Le 9 juin 2013, Edward Snowden sort de l'ombre. L'Américain de 29 ans a travaillé pendant quatre ans pour la National Security Agency (NSA), l'agence d'espionnage des États-Unis. Le lanceur d'alerte donne aux journalistes des milliers de documents ultrasecrets qui mettent au jour un système de surveillance de masse. Comme la NSA collabore très souvent avec les agences canadiennes, certains documents émanent directement de ces dernières. Pendant des mois, des journalistes s'affaireront à trier et à tenter de confirmer l'authenticité de tous les documents donnés par Snowden. Les Canadiens ne le savent pas encore, mais des révélations explosives feront bientôt les manchettes...

Entre-temps, les remises en question des services de renseignements s'enchaînent. En juin 2013, le commissaire sortant du Centre de sécurité des télécommunications, Robert Décary, présente son dernier rapport sur les activités de l'agence d'espionnage. L'ancien membre de la Cour fédérale d'appel souligne que certaines données sur les opérations passées du CST, qui permettent normalement de s'assurer que les cibles du Centre sont «bel et bien étrangères et situées à l'extérieur du Canada», sont manquantes. «L'absence d'information a limité ma capacité à évaluer la légalité des activités du Centre à cet égard», écrit le commissaire. Plus loin dans son rapport, un autre passage montre les limites de sa capacité d'examiner les actions de l'agence d'espionnage: «Un petit nombre de dossiers suggéraient la possibilité que des Canadiens aient été visés par certaines activités, ce qui est contraire à la loi. Certains dossiers du Centre relatifs à ces activités n'étaient pas clairs ou étaient incomplets. Après un examen minutieux et approfondi, je n'ai pas pu parvenir à une conclusion définitive sur la conformité ou non à la loi.»

Les mois qui suivent ne sont pas de tout repos pour les agences de renseignements, qui continuent de se retrouver à la une des journaux. En octobre 2013, c'est l'ancien chef du CST lui-même, John Adams, qui soutient lors d'une entrevue à la CBC qu'il faut une plus grande supervision des activités de l'agence d'espionnage.

Un mois plus tard, en novembre 2013, le juge de la Cour fédérale Richard Mosley rend une décision dans laquelle il conclut que le SCRS et le CST ont délibérément caché des informations à la Cour. L'affaire remonte à 2009. Les agences d'espionnage demandent un mandat spécial pour surveiller deux citoyens canadiens à l'extérieur du pays. Les autorisations sont données par le juge Mosley, à condition que les opérations soient menées par des fonctionnaires canadiens, à partir du Canada. Cinq ans plus tard, alors que le juge fait un suivi de l'affaire, il se rend compte que les agences ont en fait demandé à des autorités étrangères de surveiller les citoyens canadiens à leur place. «Compte tenu que, au cours des 10 dernières années, le partage de renseignements avec des agences étrangères a souvent mal tourné [...], il ne fait aucun doute que les agences canadiennes sont conscientes de ces dangers», indique le juge Mosley dans sa décision, faisant écho à l'affaire Maher Arar. Cet ingénieur canadien a été expulsé vers la Syrie en 2002, alors qu'il revenait de vacances en Tunisie en passant par New York, à cause de fausses informations provenant de la GRC, qui le soupçonnait d'être un activiste terroriste. Emprisonné et torturé dans son pays d'origine, il a finalement été blanchi quatre ans plus tard, après une enquête publique qui a coûté 15 millions de dollars.

Puis, le 28 janvier 2014, c'est au tour de la Commissaire à la protection de la vie privée du Canada de demander davantage de transparence au Centre de sécurité des télécommunications, dans un rapport spécial au Parlement. «La manière dont [les activités de renseignements] sont menées peut ouvrir la voie à une collecte à grande échelle, écrit Chantal Bernier. L'information [...] comme celle que l'on retrouve sur les sites de réseautage social, est balayée électroniquement et a le potentiel de devenir la principale source de renseignement. [...] Le potentiel d'atteinte à la vie privée dans ce nouveau contexte est tel qu'il exige une protection de la vie privée proportionnelle.»

Ironie du sort, deux jours seulement après l'appel de la Commissaire à davantage de transparence, les journalistes de la CBC sont prêts à rendre publiques les révélations d'Edward Snowden. Dans un des documents donnés par le lanceur d'alerte et daté du 10 mai 2012, une révélation explosive: le Centre de sécurité des télécommunications a recueilli des métadonnées sur toutes les personnes qui s'étaient connectées au réseau Wi-Fi d'un aéroport canadien, pendant deux semaines. Dans le même document, on apprend aussi que le Centre a balayé une «ville de taille modeste». Ses employés se sont attardés à deux réseaux sans fil en particulier, auxquels 300 000 appareils différents se sont connectés sur une période de deux semaines. Il n'est pas indiqué dans le document si cette autre opération s'est déroulée au Canada, mais selon la CBC, ce serait le cas. Le CST s'intéressait aussi à d'autres aéroports, en plus d'hôtels, de cafés et de bibliothèques publiques.

Après ces révélations, le chef du CST doit s'expliquer devant le Comité sénatorial permanent de la Sécurité nationale et de la défense, le 3 février 2014. On y apprend que les métadonnées avaient été recueillies à l'aéroport international Pearson, à Toronto, le plus fréquenté du pays. «L'opération faisait partie de notre collecte de données habituelle à l'échelle mondiale», indique John Forster, avant d'ajouter que «les terroristes ou les auteurs de prises d'otages accèdent souvent à Internet dans les lieux publics, comme un aéroport ou un café, parce qu'ils essaient de se cacher au milieu de la foule». Ses équipes essayaient de mettre au point un logiciel pour identifier une cible dans la nuée des millions d'échanges et de connexions qui ont lieu en même temps sur Internet. «Je sais que ce modèle a été utilisé au moins deux fois au cours des 12 derniers mois pour trouver des cibles étrangères légitimes», ajoute John Forster pour défendre son service.

Lors de cette audience sénatoriale, on découvre aussi que deux directives ministérielles ont été signées, l'une en 2005, par le libéral Bill Graham, et l'autre en 2011, par le conservateur Peter MacKay. Ces deux directives autorisaient le CST à conserver des métadonnées, comme celles de l'aéroport Pearson, pendant une durée déterminée. «S'agit-il d'une directive secrète?» a demandé le sénateur Hugh Segal. «Oui», a répondu John Foster. Impossible donc de savoir si les données de l'aéroport Pearson ont été détruites ou si elles sont toujours entre les mains de l'agence.

Les enjeux de sécurité percutent de plein fouet le droit à la vie privée des personnes. Deux événements jettent de l'huile sur le feu: l'attentat de Saint-Jean-sur- Richelieu et la fusillade au parlement, en octobre 2014. Encore une fois, la question se pose: où se trouve la limite entre le respect de la vie privée et la surveillance de l'État au nom de la sécurité nationale?

Malgré les révélations des années précédentes, le gouvernement décide de donner encore plus de pouvoirs aux agences d'espionnage, avec le projet de loi C-51.

Le 27 janvier 2015, les journalistes qui ont étudié les documents donnés par Edward Snowden publient une nouvelle bombe: une opération nommée Levitation permet au Centre de sécurité des télécommunications de surveiller des centaines de millions de téléchargements sur des sites d'échanges gratuits, tout autour de la planète. Selon le document, datant de 2012, le CST épie de 10 à 15 millions de téléchargements par jour. Une dizaine d'entre eux sont dits «intéressants» au quotidien. Le filet du CST

est tellement large qu'une des pages du document est intitulée «Filtrer les épisodes de Glee», série télévisée populaire très téléchargée. Selon la CBC, ce serait une note d'humour de la part des employés du CST.

Lorsque l'agence détecte un téléchargement suspect, par exemple un manuel pour fabriquer des explosifs, elle est capable de reconnaître l'adresse IP de l'ordinateur utilisé. À partir de cet identifiant, elle peut alors repérer toutes les activités faites sur cet appareil cinq heures avant et après le téléchargement. Si la personne s'est connectée à son profil Facebook pendant cette période, le Centre est ainsi capable de l'identifier. Deux adresses IP canadiennes, localisées à Montréal, se trouvaient dans le document non censuré, d'après la CBC. Selon la fiche descriptive du système Levitation, le logiciel a permis de découvrir la vidéo d'un otage allemand ainsi que des documents stratégiques d'al-Qaïda au Maghreb islamique. On ne sait pas si ce sont là ses seuls succès.

Dès le lendemain de la diffusion du reportage sur le sujet par la CBC, les réactions fusent de toutes parts. D'un côté, le ministre associé à la Défense nationale, le conservateur Julian Fantino, pour justifier les opérations, déclare que «notre gouvernement ne restera pas immobile pendant que les terroristes utilisent des sites Web pour attirer, radicaliser et entraîner des individus qui menacent nos valeurs et notre liberté». Le chef du Parti libéral et futur premier ministre, Justin Trudeau, rétorque qu'il est «temps de parler d'une supervision adéquate pour s'assurer que le gouvernement agit de façon responsable».

La députée néo- démocrate de Portneuf-Jacques-Cartier, Élaine Michaud, renchérit lors de la période des questions: «Le gouvernement veille-t-il à ce que les activités personnelles des Canadiens ne soient pas surveillées, pour ne pas dire espionnées? Comment s'assure-t-il de protéger la sécurité des Canadiens, tout en préservant leur vie privée?» Julian Fantino se contente de répondre que le commissaire du Centre de sécurité des télécommunications «a confirmé qu'elles étaient conformes à la loi».

Pour rappel, le commissaire du CST doit s'assurer que le Centre agit en toute légalité. C'est généralement un juge à la retraite qui occupe ce poste à temps partiel. Il dispose d'une équipe de 11 personnes pour surveiller les activités des 2 200 employés du CST. Depuis sa création, en 1996, le Bureau du commissaire du CST n'a jamais constaté la moindre activité illégale, sauf une fois, en 2016, et c'était parce que... le CST l'avait prévenu.

Les révélations des journalistes et l'indignation des partis politiques d'opposition n'empêcheront pas le gouvernement conservateur de Stephen Harper de déposer le projet de loi C-51 deux jours après les révélations, le 30 janvier 2015, pour... donner encore plus de pouvoirs aux agences. Pour l'opposition, ce texte de loi va trop loin. «Comment peut-on empêcher que ce projet de loi soit utilisé pour espionner les ennemis politiques du gouvernement?» s'inquiète le chef du NPD, Thomas Mulcair.

Le Commissaire à la protection de la vie privée du Canada, Daniel Therrien, décide alors de prendre position. Dans une lettre ouverte publiée dans des quotidiens du pays, il soutient que la nouvelle loi fera

en sorte que «tous les citoyens seront pris dans cette toile, pas seulement ceux soupçonnés de terrorisme». En vertu de la loi, 17 nouveaux organismes pourront échanger et recevoir des informations du SCRS. Or, 14 d'entre eux ne font l'objet d'aucune surveillance indépendante. «Le terrorisme représente une menace croissante. Des mesures s'imposent en matière de sécurité nationale. Mais à quel prix? [...] Ces nouveaux pouvoirs sont démesurés et les mesures de protection de la vie privée proposées sont nettement insuffisantes.»

Le 25 mars 2015, la nouvelle chef du CST, Greta Bossenmaier, témoigne devant le Comité permanent de la défense nationale. La députée du NPD, Élaine Michaud, lui rappelle les opérations secrètes d'aspiration de données de l'aéroport Pearson et de surveillance des téléchargements, avant de lui poser sa question: «Pouvez-vous confirmer cela ou nous donner plus de précisions sur cette nouvelle vocation plus offensive que semble prendre le CST?» Réponse de la patronne du CST: «J'espère que vous comprenez qu'il m'est impossible de me prononcer sur la divulgation non autorisée d'informations classifiées.» La députée tentera à plusieurs reprises de pousser Greta Bossenmaier à répondre à ses questions. Sans succès. Elle baissera finalement les bras tout en concluant: «Il est essentiel de disposer d'un comité parlementaire de surveillance qui soit habilité en matière de sécurité de façon à pouvoir analyser ce qui se passe. À l'heure actuelle, la reddition de comptes est strictement impossible à l'endroit des parlementaires. Ils ne peuvent pas non plus obtenir de réponses à des questions pourtant légitimes.»

Alors que le projet de loi C- 51 poursuit son chemin à la Chambre des communes, Michael Doucet, directeur général du Comité de surveillance des activités de renseignement de sécurité (CSARS), s'inquiète lui aussi des possibles conséquences. Son comité a pour mandat de s'assurer que le Service canadien du renseignement respecte les droits et libertés des citoyens. «Le projet de loi C-51 aura un impact considérable, non seulement sur l'efficacité même du CSARS, mais sur la reddition de comptes en matière d'activités de renseignement de sécurité au Canada», dit-il dans son discours d'ouverture au comité sénatorial permanent de la sécurité nationale et de la défense, le 23 avril 2015. «L'adoption du projet de loi C-51 placerait le CSARS dans une position délicate où sa capacité de s'acquitter efficacement de ses fonctions de surveillance pourrait être compromise.»

Mais tous les avertissements venant des élus et des fonctionnaires ne changeront rien: le projet de loi C-51 est adopté sans amendement à la Chambre des communes le 6 mai 2015, grâce à la majorité conservatrice et à l'appui libéral, dont notamment celui de Justin Trudeau, futur premier ministre.

Le SCRS est alors doté de nouveaux pouvoirs, dont celui d'«atténuation de la menace». C'est un tournant historique. Le Service se contentait jusqu'à présent de recueillir de l'information, de l'analyser et de guider le gouvernement dans ses décisions. Désormais, l'agence d'espionnage peut perturber des transactions financières, des voyages ou des communications au pays ou à l'étranger, s'il existe «des motifs raisonnables de croire qu'une activité donnée constitue une menace envers la sécurité du Canada». De plus, la Loi sur la communication d'information ayant trait à la sécurité du Canada ayant aussi été créée, le SCRS n'a plus besoin du mandat d'un juge pour obtenir, par exemple, des informations provenant de l'Agence du revenu du Canada.

En juillet 2015, le National Post publie un document apparemment secret du Conseil du Trésor, divulgué par le groupe Anonymous. Alors que le gouvernement n'avait admis l'existence que de trois stations d'opération étrangères du Service canadien du renseignement de sécurité (à Washington, Londres et Paris), le document stipule qu'il y en aurait 25, «dont la plupart se trouvent dans des pays en voie de développement et/ou dans des environnements instables». Quelque 70 employés seraient chargés d'y traiter environ 22 500 messages par an. Il semblerait de plus qu'elles soient en fonction depuis au moins 30 ans, puisqu'il est précisé dans le document que ces stations n'ont pas été rénovées «depuis que les activités de collecte étrangères du Service ont commencé, au milieu des années 1980». Le gouvernement n'a pas confirmé l'authenticité de ce document.

Le 19 octobre 2015, Justin Trudeau et les libéraux prennent les commandes de la Chambre des communes. Une de leurs promesses: reprendre le pouvoir sur les agences d'espionnage. Mais le début de leur règne commence avec de nouveaux déboires...

Le nouveau gouvernement libéral de Justin Trudeau respectera-t- il sa promesse de remettre la haute main sur les agences d'espionnage du pays?

En 2016, les révélations continuent d'accaparer les agences d'espionnage. En janvier, pour la première fois de son histoire, le commissaire du Centre de sécurité des télécommunications écrit au ministre de la Défense et au procureur général du Canada «pour les informer qu'il avait découvert que le CST ne se conformait pas à la Loi sur la défense nationale et à la Loi sur la protection des renseignements personnels». Le CST échange régulièrement des informations avec des partenaires étrangers. Lorsque ces données concernent des Canadiens, le Centre doit les anonymiser, ce qui n'avait pas été fait correctement, indique Jean-Pierre Plouffe, selon qui «le CST n'avait toutefois pas agi avec une diligence raisonnable».

La polémique se poursuit en février, lorsque le commissaire Jean-Pierre Plouffe témoigne devant le Comité sénatorial permanent de la Sécurité nationale et de la défense. On y apprend que le manquement a duré pendant des années. Il a été découvert en novembre 2013, et la procédure a été arrêtée en 2014, bien que le public n'en ait été prévenu qu'en 2016. «Parle-t-on de centaines de milliers [de Canadiens touchés]?», demande le sénateur Claude Carignan. «Il est impossible de déterminer quoi que ce soit», lui répond le commissaire.

En juin, c'est le Globe and Mail qui en apprend davantage, grâce à des documents confidentiels déposés devant les tribunaux. Le partage d'informations non anonymisées sur des Canadiens remonterait jusqu'en 2005 et comporterait des listes d'appels téléphoniques et d'échanges par Internet. Selon le document, pour les courriels, les adresses étaient anonymisées, mais pas les adresses IP. Et le CST lui-même ne sait pas quelle est l'ampleur de cette erreur qui a duré probablement pendant près d'une décennie. Le contenu des messages, a priori, n'aurait pas été collecté.

Puis, en novembre 2016, c'est de nouveau au tour du SCRS de se faire taper sur les doigts. Le juge de la Cour fédérale Simon Noël rend une décision sans équivoque: «Le SCRS a manqué, une fois encore, à son obligation de franchise envers la Cour.» Depuis 2006, le SCRS conservait des métadonnées, obtenues auprès de fournisseurs de service, «même si le contenu auquel elles sont associées n'était pas considéré comme lié à une menace». De nombreuses parties du jugement étant confidentielles, il est difficile de savoir de quoi il s'agit exactement. Toutefois, ces données étaient traitées par un puissant logiciel nommé Operational Data Analysis Centre, qui permettait de donner «un portrait précis et intime de la vie et de l'environnement des personnes sur lesquelles le SCRS enquête. Le programme permet d'établir des liens entre diverses sources et d'énormes quantités de données, ce qu'aucun humain n'arriverait à faire.» Sauf que la Cour n'a jamais autorisé le Service à conserver les données en question, et donc, que le programme était illégal dès ses débuts, il y a 10 ans. «Il est peut-être temps que les Canadiens relancent le débat sur le mandat et les fonctions de son service de renseignement national», ajoute le juge Noël dans sa décision.

Justement, les libéraux, bien qu'ils aient voté pour le projet de loi C-51, ont aussi promis lors de la dernière campagne électorale qu'ils «ramèneront l'équilibre entre notre sécurité collective et nos droits et libertés». Une consultation est d'ailleurs en cours sur le sujet depuis le 8 septembre. Les Canadiens ont jusqu'au 15 décembre pour y participer.

Mais le débat semble aujourd'hui dépasser les agences de surveillance fédérales. Les services policiers, eux aussi, utilisent de plus en plus des techniques qui menacent la vie privée de milliers de personnes qui ne sont suspectées d'aucun crime.

En avril dernier, on apprenait que la Gendarmerie royale du Canada utilisait secrètement depuis 2005 un appareil pour surveiller tous les échanges téléphoniques ayant lieu dans une zone donnée, lors de certaines de ses enquêtes. Appelé Stingray ou IMSI Catchers, ce dispositif de la taille d'une mallette relève toutes les communications, sans discrimination, par exemple dans un quadrilatère d'appartements. Que vous soyez le suspect ou non, si vous êtes au mauvais endroit au mauvais moment, vos communications peuvent donc être épiées, et vous ne le saurez jamais. Par ailleurs, au Canada, tous les appareils utilisant les ondes radio doivent être approuvés par une agence fédérale, et ces appareils ne l'ont jamais été.

Mais ce n'est pas tout. Dans des documents déposés devant les tribunaux, la GRC a aussi été forcée de révéler cette année qu'elle disposait de la clé globale de cryptage des téléphones BlackBerry. Sur ces appareils, les messages sont tous cryptés lorsqu'ils transitent entre deux interlocuteurs. Si quelqu'un intercepte ces messages, il est en théorie impossible pour lui d'en connaître le contenu. Sauf qu'il existe une clé universelle pour les déchiffrer et que les policiers fédéraux la possédaient depuis au moins 2010. Lors d'une enquête menée à Montréal à pareille date, la GRC a intercepté et déchiffré près d'un million de messages grâce à cette technique. Dans les documents déposés devant le juge, la Gendarmerie a indiqué que cette technologie équivalait à «avoir les clés pour déverrouiller les portes des maisons de tous les utilisateurs, sans qu'ils le sachent».

Les services de police municipaux semblent aussi avoir de plus en plus d'appétit pour de vastes quantités de données concernant les citoyens. En avril 2014, la police régionale de Peel, en banlieue de Toronto, enquête sur une série de braquages de bijouteries. Pour identifier les voleurs, les policiers réclament à Rogers et à Telus le relevé de «tous les téléphones activés, ayant transmis et reçu des données» de toutes les tours de réception cellulaire «à proximité de 21 adresses civiques», pendant la période des cambriolages. La quantité de données est énorme. En une seule requête, les policiers recevraient les informations téléphoniques, nominatives et bancaires de près de 43 000 personnes. La Cour supérieure de l'Ontario a jugé la demande excessive et l'a rejetée. Toutefois, dans la décision du juge John Sproat, on apprend que de telles demandes sont loin d'être exceptionnelles et que les policiers s'en servent régulièrement.

***

Selon le plus récent rapport du Commissaire à la protection de la vie privée du Canada, Daniel Therrien, «90 % des Canadiens ont l'impression de perdre le contrôle qu'ils exercent sur leurs renseignements personnels et s'attendent à être mieux protégés». Le Commissaire souligne que la Loi sur la protection des renseignements personnels a été promulguée en 1983 et la Loi sur la protection des renseignements personnels et les documents électroniques est entrée en vigueur en... 2001. Mark Zuckerberg avait alors 17 ans et Facebook n'existait pas.

La menace, il est vrai, est réelle. Le 7 mars 2016, devant le Comité sénatorial permanent de la sécurité nationale et de la défense, le directeur du Service canadien du renseignement de sécurité rappelait que 180 personnes ayant des liens avec le Canada mènent des activités terroristes à l'étranger. Selon Michel Coulombe, une centaine d'entre eux se trouveraient en Irak et en Syrie. «Comme la participation des Canadiens à ces conflits nuit aux pays où ils se trouvent et les déstabilise, le Canada a l'obligation internationale d'empêcher les voyages à des fins terroristes.» Il y a aussi toute la question de ceux qui reviennent au pays -- une soixantaine, selon le directeur -- et qu'il faut surveiller. Sans compter les attaques informatiques, de plus en plus nombreuses et perfectionnées.

Mais comment surveiller ceux qui sont suspectés d'avoir commis des crimes sans enfreindre la vie privée des gens qui ne sont suspectés de rien? Comment garder un oeil sur ceux qui pourraient poser une menace à la sécurité sans fouiller dans la vie de tout le monde? Quels sont les critères qui déterminent ce qu'est une menace? L'histoire regorge de trop nombreux exemples dramatiques où un gouvernement en savait tout d'un coup beaucoup trop sur les orientations politiques, l'origine ethnique ou la religion de ses citoyens.

Dans une démocratie, c'est aux citoyens de décider à quel point ils sont prêts à laisser l'État fouiller dans les aspects les plus intimes de leur vie. Mais les preuves des dernières années montrent combien les Canadiens ne connaissent pas les capacités des autorités publiques. Et c'est pourtant crucial, car le droit à la vie privée, c'est le droit d'être soi-même, en toute liberté.

Globe and Mail
Not warranted
Thursday, 24 November 2016

Editorial: The discovery that the Montreal Police obtained a warrant to monitor the phone of La Presse journalist Patrick Lagacé, for several months, has rightly galvanized efforts to give substantially stronger protection to journalists and their sources.
It wasn't that the police were investigating Mr. Lagacé on the contrary, they were piggybacking on the columnist's work, and that of his sources, to investigate one of their own. They also obtained a warrant to tap the communications of another La Presse journalist, Vincent Larouche. As a result, Montreal Chief Philippe Pichet has been unrepentant, saying, "There were criminal allegations against a police officer, and we have a job to do."

This isn't only about cops and robbers and reporters. Much of our legal system, and our way of life, is based on the idea that a person's home and personal effects are his or her castle. They cannot be violated without a warrant. A judge or justice of the peace has to assess whether a violation of privacy is legally justified. Police turning reporters into unwitting police sources stretches the limits very far.

The newly arrived independent Senator André Pratte, formerly also of La Presse, had already expressed hope that the Liberal government would act to give better protection to reporters and their sources. And Senator Claude Carignan, a Conservative, this week introduced a private member's bill, the Journalistic Sources Protection Act. Bill S-231 would amend both the Criminal Code and the Canada Evidence Act.

Of course, private members' bills, especially those that begin in the Senate, don't often become law. They tend to get lost in the shuffle, unless the government smiles upon them. This is an issue, and a bill, that the Trudeau government should make part of its agenda.

What happened in Montreal raises question about when warrants are granted to police, under what circumstances and by what judicial authority. Warrants are a fundamental guarantee that the privacy rights of all citizens will only be infringed in exceptional circumstances, and after a careful and legal test that balances public safety against privacy. Yet it was clearly too easy for the Montreal police to obtain their warrants in this case. Fixing that should be top of mind for the government.

Times of India
Security body plans malware research centre in city
Thursday, 24 November 2016
Byline: Staff Report

Hyderabad - Cyber security is now a national concern and the next world war would be fought in cyberspace without shedding a drop of blood, said IT minister K T Rama Rao, speaking at the second edition of the cyber security conclave that began on Tuesday.
The conclave is meant to bring the think tank of cyber security under one roof and chart out a road map for taking the state's cyber security policy to the implementation phase.

An Israeli delegation led by Ram Levi, CEO of Konfidas meanwhile engaged in a panel discussion with cyber security experts, academicians, cops and government officials from the information technology department for the purpose.

During the conclave, the Society for Cyberabad Security Council (SCSC) announced its plans to come up with a `malware research centre' in the city, for helping companies and organizations facing cyber attacks.

The centre is also planning to set up a `BOTNET and malware analysis centre' as one of the biggest threats in the current scenario is mal ware being embedded into hardware systems.

KTR said though no blood would be shed in cyber war, "Still businesses will be hurt and people will be hurt. While digital space comes with its inherent threats, it is an opportunity for India to provide solutions not just for itself but also for others," he said.

Al Arabiya
Hezbollah chief's guard seen in Aleppo
Thursday, 24 November 2016
Byline: Ahd Fadhel

Beirut - Social media accounts since last week have circulated pictures of Lebanese Hezbollah chief Hassan Nasrallah's bodyguard, donning a military attire, in Syria.
Lebanon's Shiite movement Hezbollah is an Iranian proxy and has long supported Syrian President Bashar Al-Assad's government following the regionalization of the Syrian conflict, which began in early 2011.

On a Facebook account belonging to 'Sham Zainab' on Nov. 16, a picture of Nasrallah's body guard, who is known by his alias 'Abu Ali', was published. The caption said: "Abu Ali, Sayed Hassan Nasrallah's guard, in one of the battle fields in Syria."

On another Facebook account under the name of 'Faris Al-Quds', a picture of 'Abu Ali' was published, showing him wearing a military uniform. The caption said that the picture belonged to Nasrallah's bodyguard.

One Facebook account under the name 'Mihwar Al-Mukawa" reported on Nov. 16 that Israel's Channel 10 said that 'Abu Ali' is in Qusayr - a city in the western Syrian governorate of Homs - where a military parade was taking place.

Meanwhile, other Twitter accounts under the names of 'Ali Nazal' and 'Abu Al-Huda Al-Humsi' on Nov. 18 said "Iranian websites close to Iran's Republican Guards said Hezbollah has sent Hassan Nasrallah's guard to Aleppo, and he is called Ali Abu Jawad in search for Jerusalem's path."

'Jerusalem's path' is a term used by Hezbollah to justify its involvement in the Syrian conflict as it considers liberation of Jerusalem from Israel as its final battle that should be won for Muslims.

Lebanese media has also reported about the pictures. The independent Lebanese newspaper Annahar published on Tuesday that social media users have circulated a new picture for 'Abu Al', said to be taken at the "frontier battles between the Syrian army and militants in Aleppo."

Times of Israel
Israeli researchers: Snoops can hack your headphones to record conversations
Thursday, 24 November 2016
Byline: Sue Surkes

Jerusalem - First we learned that hackers could watch us undress through our webcams, then we discovered that they could listen to us answering security questions and giving passwords through our microphones.
Now, an Israeli team has found, mischief-makers can theoretically convert our headphones into microphones to record our conversations, Wired magazine reported Tuesday.

Researchers at Ben Gurion University of the Negev have developed a prototype, known in the trade as a proof of concept, to show that headphones can be re-purposed into microphones to enable a snooper on one side of a room to record a conversation being conducted on the other by someone using a headset.

Headphone speakers convert electromagnetic signals into sound waves through a membrane's vibrations. The malware developed by the Ben Gurion team programs the membranes to work in reverse - - picking up sound vibrations and converting them back into electromagnetic signals.

"Even if you remove your computer's microphone, if you use headphones you can be recorded," said Mordechai Guri, who led the research in the laboratories of the university's Cyber Security Research Center.

The team's malware -- malicious software -- exploits a little-known feature of RealTek, software that controls sound. Because RealTek is so widely used, the malware works on almost any desktop computer, as well as most laptops.

So far, there is no simple remedy for this kind of audio peephole, Guri said, adding that RealTek's chip will probably need to be redesigned for future computers.

Khaleej Times
Mobile data traffic to rise 13-fold by 2022 in Mena
Thursday, 24 November 2016
Byline: Staff Report

Dubai - Mobile data traffic will increase 13-fold by 2022 in the Middle East and North East Africa and help boost 5G subscriptions to 20 million, a report says.
The latest Ericsson Mobility Report for the Middle East and North East Africa forecasts that smartphones will account for 56 per cent of total subscriptions by 2022 across the region.

Mobile subscriptions are growing steadily across the region and expected to reach 690 million by the end of 2016, making up eight per cent of the global market, and reaching 850 million mobile subscriptions by 2022.

The report further said the total number of GSM subscriptions will account for 60 per cent of total mobile subscriptions by the end of 2016. It is expected that mobile broadband subscriptions will surpass GSM-only subscriptions by 2018. WCDMA/HSPA subscriptions will increase from around 30 per cent of total subscriptions in 2016 to 42 per cent in 2022.

"Our latest mobility report reflects how digital technology is fast becoming part of everyday life in the region," said Rafiah Ibrahim, head of Ericsson Middle East and East Africa.

She said the report highlights the rapid uptake of LTE deployment across the region, paving the way for 5G where the company is expecting 20 million subscriptions by 2022.

"LTE subscriptions are rapidly increasing to account for seven per cent of total mobile subscriptions by the end of 2016 and reaching up to 38 per cent by 2022," she said. "Today, we are working together with our partners to pave the way for 5G across the region and we are already seeing a great interest among operators launching 5G plug-ins on existing 4G networks," she added.

By 2022, the report anticipates that mobile data traffic will multiply 13-fold while average active smartphone data consumption per month will increase from 1.8GB in 2016 to 13GB in 2022. These figures are driven by an increase in video consumption, social networking and app usage.

For example, over 70 per cent of smartphone users in Saudi Arabia, Turkey and the UAE watch video clips on social networking websites at least once a week.

Gulf News
Philippine armed forces build up capability to fight in cyberspace
Thursday, 24 November 2016
Byline: Gilbert P. Felongco

Manila - The Philippine military said it is building up capability to fight in cyberspace -- a frontier where terrorists have steadily strengthened their competency.
"It is high time for the Armed Forces of the Philippines (AFP) to build up its cyberspace capability as we are in the midst of rapidly evolving technologies," AFP public affairs chief Marine Col. Edgard Arevalo said.

The new technologies spawned by the internet had created challenges for the Philippine military, a relatively budget- constricted fighting force.

In recent years, tech-savvy terror groups such as the Abu Sayyaf, the Bangsamoro Islamic Freedom Fighters (BIFF) and the Lanao-based Maute group had made effective use of cyberspace in carrying out propaganda and to some-extent, recruitment of fighters. They were able to do this mainly by uploading video clips on internet-sharing sites such as YouTube and other websites.

The terror groups have effectively maximised the new realm of cyberspace for their purposes and their operations have gone on without opposition.

Only a small fraction of the country's gross national product goes to military expenditures compared to the militaries of nearby countries such as China and Malaysia.

According to Arevalo, the move to beef up the AFP's presence in the virtual world was highlighted during the November 12 to 23 celebration of the 81st AFP Signal Corps Anniversary.

The AFP Signal Corps maintains the main communication backbone of the AFP. The Corps has been providing the AFP's command and control with voice and data services for the past 60 years.

The Corps also plays a key role in delivering crucial information services during natural disasters as well as in national events such as the recent Asean Summit.

Major Gen Jose P Tanjuan Jr, AFP Deputy Chief of Staff for Communications, Electronics and Information Systems, said the Signal Corps also envisions the establishment of a cyber-capable armed force by developing policies and establishing a responsive organisational structure manned by a pool of Cyber-capable workforce.

The Signal Corps was officially formed as one of the technical services of the Philippine Army in 1936 through the National Defence Act. The term "signal" became known to refer to a highly distinct military occupation dealing with methods of communications.

The Courier-Mail
Cyber war hits jihadis hard, says PM
Thursday, 24 November 2016
Byline: Staff reporter

Melbourne - Australia has taken its fight against ISIS online - and it's working, Prime Minister Malcolm Turnbull has -declared.
Mr Turnbull told Parliament the country's top-secret offensive cyber capabilities were becoming more important in countering terrorism.

"While I won't for obvious reasons go into the details of those operations, I can say that they are being used and that they are making a real difference in the military conflict," he said in an address on -national security.

Australian combat aircraft have participated in coalition air operations in Iraq and Syria since 2014, while Australian and New Zealand troops have been training Iraqi soldiers for the fight against ISIS.

ISIS has long maintained an extensive capability to use the internet for its own purposes, using slick video productions to trumpet its successes and persuasive pitches to potential Western converts.

Last week ISIS released a propaganda video that prominently featured Melbourne landmarks.

"(ISIS) will continue doing this in an attempt to intimidate us but they will not succeed," Mr Turnbull said yesterday.He said terror threats -remained at "probable".

China Daily
Enterprises prepare for insider threats to data
Thursday, 24 November 2016
Byline: Wu Yiyao

Shanghai - Insiders have become one of the largest threats to enterprises' critical digital and physical assets, according to research commissioned by EY, a consultancy services provider.
The study polled more than 665 senior executives in 17 countries and regions, including 40 professionals from China. More than 25 percent of respondents said they believe insider threats and illicit behaviors taking advantage of internet technologies are the fastest growing risk.

"About 70 percent of our services delivered to clients are focusing on illicit behavior taking advantage of internet technologies such as using loopholes in network systems and online payment schemes, particularly in fintech and online payment sectors," said Chen Zhi, an EY partner and expert in fraud investigation and dispute services.

More exposure amid increased connectivity is making it difficult to detect threats to critical assets, such as intellectual property, formulas, payment information, and clients' personal information, said Chen.

"It is not just an IT issue - it takes an enterprisewide approach including many human elements - to plan for, prevent, detect, respond to and recover from insider threats," said EY's research note on managing insider threats.

China's enterprises said they have increasingly invested in improving their organization's internet safety and internet security, including deploying more resources to build up their cybersecurity teams and use more third-party services, such as data monitoring, data recovery and user behavior pattern analysis.

On Nov 7, China's cybersecurity law was approved by the Standing Committee of the National People's Congress, China's top legislature. The law will come into effect on June 1, 2017.

"Having worked extensively with clients in APAC and China, we know the challenges they face managing data in legal proceedings and ensuring that privacy and state secrecy laws are respected. E-discovery solutions that allow clients to process data in the country and on-site at a company's premises in China are therefore essential," said Kate Chan, regional managing director in Kroll Ontrack's Asia Pacific practice, an end- to-end provider of electronic evidence services.

Even small-sized enterprises, such as startups, should bear in mind that computer forensics, e-discovery, and document review are important for protecting rights. They should start working with professionals, such as lawyers, at a very early stage of operations to ensure long-term growth and safety, said Chan.

Global Times
Xinjiang tightens passport policy to maintain social order: official
Thursday, 24 November 2016
Byline: Zhao Yusha

Beijing - Northwest China's Xinjiang Uyghur Autonomous Region has tightened passport regulations, requiring all residents to hand in their passports to local police stations for examination and management.
An anonymous police officer in Aksu prefecture confirmed with the Global Times on Wednesday that all citizens in Aksu are required to hand their passports, be it a private passport or passport for public affairs, to the police stations. The passports will be managed by the police.

"Anyone who needs the passport must apply to the police station," said the source, adding that the passport management policy is implemented throughout Xinjiang.

The Public Security Bureau in Shihezi city gave the same directive on its official Weibo account on October 19, saying that it was for "annual examination" purposes.

"Those who refuse to hand in their passports should bear the responsibility themselves if they are forbidden from going abroad," read the post.

Meanwhile, the post was deleted later.

A resident from Kashar city who didn't want to be named told the Global Times that she received a call asking her to hand her passport to the police.

She said that her husband's application for passport was denied by the local police station a few days ago. "The passport application center claimed they didn't know when citizens could apply for passports again, as they were waiting for further instructions from higher authorities," she said.

A local official in Xinjiang told the Global Times on Wednesday that the Xinjiang government had loosened control over residents' passports in 2015. The current policy tightening aims mainly to maintain social order, he noted.

Getting a passport is often complicated and takes more time in Xinjiang than in other provinces, given the rising threat of terrorism in the region and the government's ongoing anti-terrorism campaign, said the official.

The new policy will not affect ordinary people's travel plans since they can easily get their passports back, but those who have criminal or any other suspicious records would be restricted from going abroad, according to the official.

The policy in 2015 stipulated that residents in some areas in Xinjiang who obtain a passport under tourism category can still keep the passport in their personal possession.

In the past, passports under tourism category were required to be handed to the local tourism bureaus upon return, while those obtained for business or family visit purposes needed to be kept with the local police, Turgunjan Tursun, a research fellow at the Xinjiang Academy of Social Sciences, said.

Xinjiang authorities announced in 2015 that they would simplify the paperwork and speed up procedures for those who apply for a passport under the category of visiting [a family member or friend overseas], business, tourism and education.

Sky News
Enigma Codebreaker site to house cyber security college
Thursday, 24 November 2016
Byline: Staff report

London - Bletchley Park, the home of the Enigma codebreakers, is to become the home of UK's first National College of Cyber Security.
During the Second World War, Alan Turing and his team of computer scientists broke the system used by the Nazis in what many believed to be the single biggest contribution to Allied victory.

And now, some of the brightest teenagers in the country will be given the chance to follow in their footsteps.

The college - which is being created by a new cyber security body called Qufaro, will open in 2018 once a £5m restoration of buildings on the Bletchley Park site is complete.

Alastair MacWilson, chair of Qufaro and the Institute of Information Security Professionals, said: "Our cyber education and innovation landscape is complex, disconnected and incomplete putting us at risk of losing a whole generation of critical talent.

"For those interested in forging a career in cyber, the current pathway is filled with excellent but disparate initiatives - each playing a vital role without offering a truly unified ecosystem of learning and support.

"By connecting what already exists and filling the gaps, Qufaro will make it easier for budding professionals to grow their cyber security skills at every stage of their journey, and contribute more to the sector as a result."

The college will "select only the most talented and skilled students" and will combine its syllabus with modules in complementary subjects including maths, computer science and physics.

In order to tempt those who are interested in a career change, a new range of online courses are also planned.

The Daily Beast
Sorry, Hillary Clinton Fans. There's 'Zero Evidence' of Election Hacking.
Wednesday, 23 November 2016
Byline: Shane Harris

Washington - Does Hillary Clinton still have a path to the White House?

That's the provocative question posed by some computer security experts, who think voting results in key states could have been manipulated by hackers.

The emphasis here is on "could." There's no clear evidence that voting machines were rigged or that ballots were altered, but as reported Tuesday night in New York magazine, a group of computer scientists and election lawyers has urged Clinton to call for a recount in Wisconsin, Michigan, and Pennsylvania, three swing states that Donald Trump won--to the surprise of just about every pollster, pundit, and journalist in America.

Clinton would have to win those states back in order to change the outcome of the election. And while it's tempting to blame hackers, and not the failure of the political professional class, for Trump's upset, experts warn not to get your hopes up for a shocking turnaround. For hackers to have changed the votes in three states would have been even more surprising than Trump's victory.

"There is zero evidence of tampering right now. Zero," David Becker, the executive director of the Center for Election Innovation and Research, told The Daily Beast. The simpler explanation for why the vote deviated from expectations and historical trends was that Barack Obama wasn't at the top of the ticket. The results for Clinton "only look off when you compare them to the Obama elections" in 2008 and 2012, Becker said.

The hackers would have had to begin their work in advance of the election. And in those states or counties that don't use electronic voting machines exclusively, they'd probably have to be on the ground, infiltrating elections offices, and working up to Election Day if not on the day itself. Throwing the votes in these three states on the same day would have required teams of people working in coordination with a high risk that they'd get caught, Becker said.

"I don't know how you'd plan for something like this even if you had George Clooney and Brad Pitt," he said, referring to the Oceans movie franchise in which talented thieves pull of absurdly implausible heists.

Even one of the computer scientists reportedly urging Clinton to call for a recount seemed to downplay the notion that hackers stole the election for Trump.

"Were this year's deviations from pre- election polls the results of a cyberattack? Probably not," J. Alex Halderman, a professor of computer science at the University of Michigan, wrote in a post on Medium. "I believe the most likely explanation is that the polls were systematically wrong, rather than that the election was hacked. But I don't believe that either one of these seemingly unlikely explanations is overwhelmingly more likely than the other."

"The only way to know whether a cyberattack changed the result," Halderman continued, "is to closely examine the available physical evidence?--?paper ballots and voting equipment in critical states like

Wisconsin, Michigan, and Pennsylvania. Unfortunately, nobody is ever going to examine that evidence unless candidates in those states act now, in the next several days, to petition for recounts."

But that's not entirely true, because in some states, officials routinely go back and look at vote counts in order to determine to determine that laws were followed and voting machines worked properly.

Wisconsin, a state that Halderman flagged, is one of them. There, the law requires a random audit of each type of voting equipment used in the state, of which there are about half a dozen from different vendors and manufacturers, Michael Haas, the administrator of the Wisconsin Elections Commission, told The Daily Beast.

"People go through and hand count the ballots and make sure that the equipment counted them as you'd expect based on how the ballots were marked," he said. The elections commission will compile a final report by December 15 and provide it to an oversight body. Any petition to hold a recount is due by this Friday at 5pm. "We haven't received any inquires from the Clinton campaign about a petition" to hold a recount, Haas said.

Becker said he was confident that the Wisconsin audit would detect any irregularities that could indicate vote tampering. "If there is a problem, we'll know about it."

But the auditing procedures in other states may give skeptics less comfort. In Michigan, there is no audit aimed at re-tabulating or counting ballots. Rather, officials conduct a review to ensure that local officials properly followed laws and procedures. Experts say it's better than nothing, but isn't a robust means for verifying that there were no shenanigans or errors on Election Day.

Michigan only uses optical scanning systems--voters make their choices on paper ballots that are tabulated by a machine. The state doesn't use electronic voting machines, like those with touch screens that may rely on software downloaded from the internet, which could be vulnerable to tampering.

This doesn't mean the election results couldn't have been altered. But Fred Woodhams, a spokesperson for the Michigan Secretary of State, told The Daily Beast that the state has used the optical machines for more than a decade and that "time and again they have demonstrated their extreme accuracy and integrity."

Official assurances count for something. But in the last state flagged by the researchers, Pennsylvania, it's not clear that an audit would detect tampering in some parts of the state.

Pennsylvania is one of those states that gives election security experts heartburn, because the electronic voting machines it uses don't print out a paper record of the voter's selections. In effect, there is no way to verify that the machine accurately recorded the votes, experts say.

Experts have long pointed out that these paperless electronic machines would make a prime target for hackers. Pennsylvania does use paper ballots in some parts of the state, and it does conduct some post-election audits. But it could be difficult to detect tampering with the voting machines unless they're directly examined.

A spokesperson for the Pennsylvania Department of State said in a statement that officials are "aware of the report" in New York magazine. "The Pennsylvania Election Code includes a provision allowing an election to be contested in the courts. Such action must be taken within 20 days after the election. We will not speculate or comment on any potential litigation."

The statement made no mention of an audit.

The bottom line is that there's no evidence yet of election hacking, but there's also no universal policy to audit results after an election. And that's unfortunate, because regular audits would help build confidence that elections went off smoothly and weren't targeted by hackers, said Pamela Smith, the president of Verified Voting, a nonprofit group that advocates transparency and security in U.S. elections.

"My feeling is audits should be done as a matter of course," Smith told The Daily Beast, adding that states that don't conduct them now could launch "a pilot audit" as a sign that they take the issue seriously.

"A state could say, we know this was a contentious election, we have that unusual situation where the popular vote winner didn't win the most electoral college votes, what the heck, let's do an audit. I think that's a perfectly legitimate thing to do."

Le Temps
Un esprit troublé à l'origine du vol des données secrètes
Thursday, 24 November 2016
Byline: Céline Zünd

Bellinzone, Suisse - Fuite L'informaticien du Service de renseignement de la Confédération, qui avait volé des données ultrasensibles à son employeur, écope de 20 mois avec sursis
C. B., 48 ans, jeans et pull à capuche, s'est excusé devant la cour, avant de demander de pouvoir repartir d'où il venait, Salerne, en Italie, pour tenter d'y retrouver « une vie normale » . L'ancien informaticien qui avait plongé le Service de renseignement de la Confédération (SRC) dans l'une des plus graves crises de son histoire, répondait mercredi devant le Tribunal pénal fédéral de Bellinzone des chefs d'accusation d'espionnage politique aggravé et de tentative de violation du secret de fonction.

Son acte, le vol d'informations au coeur du serveur sécurisé des renseignements helvétiques, avait eu l'effet d'une bombe en 2012. La cour s'est réunie en janvier dernier à huis clos pour pouvoir examiner ce matériel sans risquer de divulguer des secrets d'Etat.

L'accusation a insisté sur ce point: ces données contenaient des informations ultrasensibles sur des opérations secrètes du SRC, ses collaborations avec des renseignements étrangers. Si elles s'étaient retrouvées dans le domaine public, non seulement la réputation des services secrets helvétiques et leur travail à l'étranger auraient été gravement compromis, mais, en plus, les vies de sources du SRC auraient été mises en danger. Sans compter les risques pour la sûreté de la Suisse.

Aux yeux du procureur Carlo Bulletti, l'accusé avait parfaitement conscience de la sensibilité du matériel copié du serveur sécurisé du SRC, puisqu'il avait été nommé administrateur de ce système, conçu précisément dans un but de protection des données. « Il était préparé, structuré, il a planifié son acte », a-t-il argumenté devant la cour. L'accusation en est convaincue: C. B. avait bien l'intention de vendre ce matériel à des tiers. Mais, même si ce n'était pas le cas, le fait de l'avoir copié avec ces données et de les avoir sortis du bâtiment du SRC suffit à le condamner. Le procureur a requis 5 ans de prison « si la capacité de discernement de l'accusé est intacte », une question qu'il a laissé le soin aux juges de trancher.

« Motivé par un sentiment d'injustice »

L'état psychiatrique de C. B., 48 ans, s'est trouvé au coeur des débats. Une première analyse, dans les mois qui ont suivi les faits, relevait l'état dépressif de C. B. Rien qui ne permette d'attester d'une responsabilité diminuée, lorsque l'informaticien a décidé de se rendre au bureau à six reprises, entre le 4 et le 18 mai 2012, pour copier 507 gigabytes de données sur deux serveurs, avant de les emmener à son domicile, dans la banlieue de Berne.

Une seconde expertise commandée par la défense aboutissait quant à elle à la conclusion inverse. Le Ministère public avait alors convoqué l'avis d'un troisième expert, Carlo Calanchini, qui s'est présenté hier devant la cour pour faire part de son analyse. Selon le psychiatre tessinois, C. B. souffre d'un trouble délirant, une psychopathologie lourde. Il a certes planifié son acte, mais « il était motivé par un sentiment d'injustice et la menace qu'il percevait de la part de ses collègues », affirme le psychiatre.

La pathologie de C. B. expliquerait aussi son étrange comportement dans l'épisode de la banque, qui s'apparente selon l'expert à une « dissociation de la personnalité » et a fini par conduire à la chute de l'informaticien. Le 15 mai, l'homme se rend dans une filiale bernoise d'UBS pour se renseigner sur les modalités d'ouverture d'un compte à numéros. Il laisse entendre qu'il attend une grosse somme pour la vente de données de la Confédération. Suspicieux, l'employé de banque alerte les autorités.

Devant la cour, l'accusé a invoqué une mémoire défaillante. Il ne se souvient pas avoir rédigé une offre en anglais pour la vente des données volées, ni avoir déclaré, à la banque, attendre le versement d'une

grosse somme. L'avocat, qui a plaidé l'acquittement, a livré sa version des faits: C. B. a copié le contenu du serveur du SRC pour prouver le harcèlement dont il aurait fait l'objet sur sa place de travail.

Au début, il entretenait de bonnes relations avec ses collègues. R. M., son premier supérieur, est venu en témoigner hier devant la cour: C. B. était un informaticien doué et loyal. C'est après le départ de ce chef, en 2011, que la situation se corse. L'informaticien se sent « mobbé », s'absente du travail de plus en plus souvent. Jusqu'à l'issue que l'on connaît.

« C'est sa maladie mentale qui a fait agir mon client. Un vrai criminel ne se serait jamais lancé dans une opération aussi risquée », affirme l'avocat. Ce n'était pas la première fois que l'informaticien rencontrait des difficultés relationnelles sur son lieu de travail. Dans toutes les entreprises où il est passé, il a fini par quitter son poste pour des pressions, des « machinations », des « animosités » de la part de collègues.

La cour aurait suivi l'avis de l'accusation et condamné l'ancien informaticien à une peine privative de liberté de 5 ans, si elle n'avait pas estimé la responsabilité pénale de l'accusé limitée en raison de ses troubles mentaux sévères. Aussi, à l'issue de ce procès d'une journée, les juges ont décidé de réduire la peine de deux tiers et condamné l'ancien informaticien à 20 mois de prison avec sursis. Quant au motif de l'accusé, « il reste inconnu », ont déclaré les juges.

Indo-Asian News Service
Indian Android smartphone users too at data theft risk: Experts
Thursday, 24 November 2016

New Delhi - News that security firm Kryptowire identified a "backdoor" spyware in Android smartphones in the US which collected sensitive personal data and transmitted it to servers in China has shaken cybersecurity experts in India -- a country where one in five smartphones are of Chinese make. Jump-started by the US Defense Advanced Research Projects Agency (DARPA) and the Department of Homeland Security (DHS), Kryptowire last week revealed that these Android devices were available through major US-based online retailers like Amazon and BestBuy and included popular smartphones such as BLU R1 HD devices.

The devices actively transmitted user and device information including text messages, contact lists, call history with full telephone numbers, and unique device identifiers to third-party servers in China without user-consent, Kryptowire claimed.

Shanghai Adups Technology Co Ltd, the Chinese company behind the spyware -- or firmware -- later admitted that it planted them in some Android phones "by mistake" but the "text messages, contacts or phone logs" were not shared with anyone else.

The revelation has raised security and privacy concerns in India. There are nearly 250 million unique smartphone users in the country and by the end of the year, there will be 280 million Indians with these devices.

"Nearly 94 per cent of these people are using Android devices and Chinese smartphone users are at roughly 60 million, which means one out of five smartphone users in India is using a 'Made in China' device. Thus, security becomes a paramount concern here," Tarun Pathak, Senior Analyst, Mobile Devices and Ecosystems at New Delhi-based Counterpoint Research, told IANS.

With digital consumption on the rise, the security risk is growing multifold. "Indian smartphone users are at the same risk as users in the US when it comes to sensitive personal data and information being copied from phones and transmitted to undisclosed locations without their consent or knowledge. This is owing to the security vulnerabilities that exist in the Android system," explained Pavan Duggal, one of the nation's top cyber law experts.

Android is a very fertile platform with a large number of contaminants and infections. Hundreds of thousands of infections have been discovered on the Android platform in the last few years.

According to Rahul Tyagi, Vice President (Training) at IT risk assessment and digital security services provider Lucideus, Indian users share the same threat as China continues to be a major exporter of smartphones.

"Given the current market, there are a lot of new phone companies/models being launched every day with advanced features at a low price, most of them being manufactured in China -- which may put user-privacy at great risk," Tyagi told IANS.

Owing to the competition, companies are trying to give the best hardware experience to consumers but what is lacking is proper security auditing in their custom-operating systems and firmware.

"Bugs at the operating system's application layer can be tackled by using updated anti-virus and other third-party security applications, but bugs at the firmware level is beyond users' reach as they will never have direct access to the firmware," Tyagi pointed out.

The threat gets bigger with more and more people embracing mobile digital payments in the wake of demonetisation.

"Mobile continues to be an area of exposure. As we get more and more used to transactions with mobile banking or e-commerce, mobile becomes more of a financial gateway and the implications are huge," added Anand Ramamoorthy, Managing Director, South Asia, Intel Security.

What if such a data theft case is identified in India? "If the government comes to know that Chinese smartphones are stealing users' data from their customers, then it is very apparent that our cyberlaw is not at all adequate to deal with such challenges," Duggal told IANS.

Though under the 2008 amendments to the Information Technology Act, 2000, all mobile phones, including smartphones, have been covered within the ambit of the Indian cyberlaw, the law still does not comprehensively deal with relevant issues in the mobile ecosystem.

The absence of India as a signatory to any international treaty on cybercrime further complicates the intrinsic ability of the immense law and legal frameworks to provide effective remedies against any such contravention.

"One of the biggest challenges in this regard would deal with the issue of attribution. How would the Indian agencies be able to attribute to the fact that the said misuse has been done from the indicated/suspected source. The issues pertaining to attribution need far more clarity," Duggal noted.

According to Rakshit Tandon, consultant at the Internet and Mobile Association of India (IAMAI) and a cyber security expert, the threat is very real for Indian users and the country lacks a sufficient law framework to tackle the situation.

"Thus, it is challenging for the Centre/state governments to ward off data stealing from smartphones by third-party software. We need stronger laws to apply enforcement on data stealing via such devices," he told IANS.

Keeping new-age security needs in mind, steps must be taken to make Indian cyberlaw more effective and redressal mechanisms must be built in for the users who are part of the digital and mobile ecosystem, Duggal added.

CBC News
The Canadian government doesn't want hackers' help
Monday, 28 November 2016
Byline: Matthew Braga

The U.S. Department of Defence has turned to well-intentioned hackers and independent security researchers to help the government agency find software bugs and vulnerabilities in its computer systems.
But in Canada, the government appears to still have no formal policy or public guidelines, which makes it difficult for those who do find flaws to know what to do, or how the government might respond.

"There's no formal process," says Imran Ahmad, a partner at the law firm Miller Thomson who works with clients on cybersecurity related issues. In the absence of such a process, he says, those who find flaws "just don't know how the government's going to react, and they just want to protect themselves."

"My advice to anyone who finds a flaw in a government website at this time would be to forget they ever saw it," wrote web developer and security researcher Kevin McArthur in an email.

In the past, companies and governments often threatened security researchers and coders who found and published details about vulnerabilities in software with litigation, prompting the adoption of an informal process called "responsible disclosure."

In practice, it means researchers will typically notify a company in private about a bug and give that company time to fix the flaw before disclosing its existence in part or full to the wider public.

In recent years, U.S. technology companies such as Facebook, Google and Microsoft have offered financial incentives and bragging rights for the responsible disclosure of bugs through the creation of programs called bug bounties ? welcoming, rather than warring against the efforts of outside researchers who manage to penetrate their systems with the goal of making them safer.

The companies typically have guidelines for how far researchers are able to go in their search for flaws, outlining specifically what is allowed and providing assurance that a researcher won't be labelled a criminal for finding a serious flaw.

Last Monday, the U.S. DoD announced a vulnerability disclosure policy, following a pilot project called "Hack the Pentagon" it organized earlier this year.

"For the first time, anyone who identifies a security issue on a DoD website will have clear guidance on how to disclose that vulnerability in a safe, secure and legal way," Secretary of Defence Ash Carter wrote.

CBC News asked seven Canadian federal government agencies - the departments of Finance; National Defence; Justice; Innovation, Science and Economic Development; Public Safety; Shared Services; and Canada Revenue Agency - questions about their policies, but did not receive a response.

"There are a lot of good people who are better at coding, who are better at hacking, who are better at a lot of things than government resources allow them to be," said Ahmad of the U.S., where the DoD's attitude has changed. "So, where in the past, you may want to jail someone for something like this, I think they're now moving towards ? bringing them into the fold, and even bringing them onto the team, instead of coming down hard on them."

Chilling effects

In 2014, a serious bug was discovered in the security software that underpinned hundreds of thousands of trusted websites. It was called Heartbleed, and researchers wasted little time determining which sites and services were vulnerable so that the hole could be patched.

Justin Bull ? a software engineer with the financial tech startup Wealthsimple and a security enthusiast in his spare time ? noticed that software used by the Canada Revenue Agency was also vulnerable. He says he spent about two hours attempting to contact various federal government agencies, finally leaving both an encrypted e-mail and voice mail with the Canadian Cyber Incident Response Centre, or CCIRC.

The CCIRC operates within Public Safety Canada, and is the government's primary point of contact for tips on cyberattacks and other computer-related incidents, but the Centre's website does not specifically address the discovery and disclosure of software flaws.

"I never ever ever got a response," Bull said. "So when I was hearing that the RCMP was investigating ? I'm like 'Holy shit, is my door going to get kicked down?' Because I'm trying to tell them here, and I don't know what's going to happen."

"You don't want to anger the beast," he added. "I understand that chilling effect. The messenger always gets shot."

Similarly, McArthur cited the fallout from the RCMP's case against Stephen Solis-Reyes, as one of the reasons he no longer discloses bugs to the Canadian government.

Like Bull, Solis-Reyes discovered that the CRA's website was vulnerable to Heartbleed, but he accessed 900 SIN numbers in the process. Solis-Reyes ? who was 19 and a student at Western University ? was investigated by the RCMP for the breach, accused of being a terrorist by his interrogators, and pleaded guilty in May to four charges.

Solis-Reyes told the court that he had no malicious intent, and only intended to test the bug's severity. His lawyer argued that he did the country a service by exposing the flaw.

"If you don't provide proof of actual vulnerability exploitation, then the problem is simply ignored and downplayed as theoretical," McArthur wrote of his own experiences bringing bugs to the government's attention, which has discouraged him from disclosing more.

"On the other hand, if you provide the government the required proof, like Solis-Reyes did by demonstrating the Heartbleed vulnerability at CRA, then they classify you as an evil hacker and you're heading for the police cells."

- Hackers wreak havoc on the 'internet of things'

Canadian Press
Parents of young kids say federal no-fly inquiries office is little or no help
Saturday, 26 November 2016
Byline: Jim Bronskill

Ottawa - Families of young children who repeatedly run into no-fly list snags at the airport say a federal inquiries office intended to help them has been of little or no use.
The problems seem likely to persist because a more permanent solution promised by the Liberals -- a full redress system to deal with mistaken identities -- is still at least 16 months away.

The parents of dozens of youngsters have experienced nerve-fraying airport delays because their children's names match those on a confidential security list.

In June, the Liberal government announced the Passenger Protect Inquiries Office to help people who are delayed during the check-in process and asked to provide identification, have to wait at the counter due to a ticketing agent placing a phone call to other officials, or are denied boarding for whatever reason.

Families with young children who have explained their cases to the office continue to experience airport hassles, said Khadija Cajee, a spokeswoman for the group known as the No Fly List Kids.

Cajee, who lives in Markham, Ont., said at least four families -- including her own -- received only an explanatory letter from the inquiries office one month after submitting details of their children's cases.

"So far it hasn't really resulted in any positive steps forward for any of us," said Cajee, whose seven-year-old son Adam was most recently delayed at the airport two weeks ago when travelling with his father.

A July 27 letter to Cajee's husband from the inquiries office, a unit of Public Safety Canada, says officials were beginning to work with Canadian air carriers and other government agencies to improve the application of search filters used in screening air traveller manifests. "These measures, such as refining search functions, could help to improve the accuracy of the screening process."

That hasn't helped Heather Harder, whose two-year-old son Sebastian has triggered red flags on two trips to Saskatoon from their home in London, Ont., since receiving a similar response from the inquiries office.

"There wasn't a lot of substance to the letter," Harder said in an interview. "It definitely didn't resolve anything for us."

The family usually faces delays of 20 to 30 minutes, and Sebastian is allowed to board the plane when it becomes obvious he is a toddler. But Harder worries what might happen when he's older and begins to travel on his own.

"It's worrisome for the future."

Four federal employees -- one manager and three analysts -- are responsible, among other duties, for responding to inquiries received by the office, said Jean-Philippe Levert, a Public Safety spokesman.

"While there is no set timeline for the resolution of each inquiry, as cases greatly vary in their level of complexity, the (office) sets out to resolve all requests in a timely manner, with the goal of being as expeditious as possible," said Levert.

"A small sample of cases may not be representative of all outcomes."

The Liberals have promised a redress system that would eventually allow travellers whose names closely match those on the Canadian no-fly list to apply for a unique identification number. They could use this number at the time of ticket purchase to clear their name in advance and prevent delays.

Public Safety Minister Ralph Goodale has said Canada needs "an entirely new database and information system" to fully solve the problem of people -- including children -- being delayed at airports.

Unlike the standalone U.S. system, Canada's no-fly list database was designed to piggyback on to airline computers, meaning it's more difficult to clear up misunderstandings.

"To put this new system in place, important regulatory and data system changes are required," Levert said. "While those changes are underway, we are aiming for implementation by spring of 2018."

Cajee, Harder and other families with youngsters who are grappling with security-list mismatches plan to attend a public meeting in Markham on Sunday with Goodale and two other Liberal cabinet ministers -- part of the federal consultation on national security policy.

Meantime, Harder and her family are planning another plane trip, and wondering what will happen at the check-in counter.

"We fly again on Wednesday, so we'll see," she said. "Each time, we're not sure. It's frustrating."

Journal De Montreal
Espionnage à l'ère du numérique
Saturday, 26 November 2016
Byline: Annabelle Blais

Montreal - Facile d'espionner en 2016? Oui, répond un enquêteur privé. Nos cellulaires et nos activités sur internet laissent beaucoup de traces et on s'intéresse peu aux enjeux de cybersécurité.
Le SPVM et la SQ ont pu espionner aisément et sans trop d'effort plusieurs journalistes québécois. Il leur a suffi d'obtenir leurs relevés téléphoniques ou d'intercepter en temps réel des numéros de téléphone, et d'activer la localisation par GPS en ce qui concerne le chroniqueur à La Presse Patrick Lagacé.

Pour comprendre la filature 2.0, Le Journal s'est entretenu avec le détective privé Claude Sarrazin, président de l'Association professionnelle des enquêteurs privés du Québec et président de l'Agence d'enquête Sirco. Il a d'ailleurs récemment présenté au Sénat-- canadien un état de la menace en matière de cybersécurité.

Est-ce que les Québécois protègent suffisamment leurs renseignements personnels ?

Non. Ce n'est pas tant une question d'équipement. Les gens disent oui à tout sur internet et font aveuglément confiance à des sites web et des fournisseurs de services. Le premier responsable de la sécurité est la personne elle-même. Et elles se font hameçonner ou se font installer un logiciel malveillant sur leur système informatique. Ce logiciel peut récupérer des images sur ton ordinateur, tes mots de passe, tes numéros de carte de crédit et même prendre le contrôle de ton appareil à distance. C'est en plein essor et plus on avance, plus on va avoir de la difficulté à contrôler.

Faut-il se protéger en utilisant certaines applications pour échanger des messages cryptés ?

Ça dépend... Vous savez, on peut tout extraire d'un cellulaire. La navigation web, les textos, appels sortants et entrants. Il faut être prudent. Je me suis fait approcher par une compagnie qui n'est pas canadienne, qui m'a dit: "Je peux rentrer dans n'importe quel cellulaire". Mais moi, je n'ai pas le droit de faire ça, alors je ne vais pas aller chercher une preuve qui n'est pas utilisable. Mais par curiosité, je leur ai demandé de pirater mon téléphone--. Et effectivement, ils m'ont piraté à distance, sans jamais avoir

accès à mon cellulaire qui est pourtant d'une marque réputée inviolable. Il avait accès à mes contacts, mes courriels, mes appels entrants, sortants, mes textos. Tout. Ça fait peur.

À titre de détective privé, pouvez-vous aller chercher nos informations sur nos téléphones intelligents ou sur nos ordinateurs ?

Les enquêteurs privés ont accès à la même information que le public, sauf qu'on a des outils d'analyse pour travailler ces données. On ne peut pas commettre d'actes illégaux. Mais on peut faire certaines choses, car on a un permis d'agent qui nous autorise à faire notre travail. Par exemple, si un patron décidait de suivre son employé pour savoir s'il est vraiment malade, ça peut être du harcèlement criminel, mais pas si c'est un détective qui le fait, parce qu'il a un mandat d'enquête. À la base, il faut aussi un motif raisonnable pour effectuer une enquête.

Et depuis cinq ans, il y a aussi un Bureau de la sécurité privée qui encadre vos pratiques.

Oui. Il y a un code d'éthique et l'Association professionnelle des enquêteurs privés a son code de conduite. La jurisprudence des tribunaux détermine aussi ce qui est acceptable.

Qui sont les clients des enquêteurs membres de votre association ?

Certains enquêteurs se spécialisent dans les infidélités conjugales. Mais ce sont surtout des entreprises, des institutions gouvernementales. On touche beaucoup aux relations employés-employeurs, par exemple, un employé qui abuse de la CSST, des problèmes de vols dans une entreprise. Il y a des centaines de milliers d'enquêtes qui se font tous les jours dans toutes sortes d'organisations, outre les organisations policières. Il y a des enquêteurs à l'interne au sein de plusieurs organisations. Toutes les grandes sociétés publiques ont un département des enquêtes: Hydro-Québec, Postes Canada, etc.

Pouvez-vous obtenir des mandats pour mettre des téléphones sur écoute ou faire des perquisitions ?

Pas pour faire une écoute. On va travailler avec des avocats pour obtenir des ordonnances pour avoir des informations que possède une banque ou une compagnie de téléphone, par exemple. Ça peut être une ordonnance qui oblige un individu à se laisser saisir d'un élément de preuve. C'est un juge qui devra autoriser ces ordonnances--, et c'est donné au compte---gouttes.

Normalement, ce n'est pas conservé longtemps sur les serveurs des compagnies de téléphonie. Mais théoriquement, ce serait possible de le faire. Personnellement, à date, je n'ai jamais-- fait de demande pour obtenir-- ce genre d'information.

Quelles informations les policiers peuvent-ils demander et obtenir de plus que les enquêteurs privés ?

Ils peuvent avoir un mandat de géolocalisation. Il y a certains cas où des enquêteurs privés ont participé à l'obtention-- d'une telle ordonnance, mais c'est excessivement rare. Il y a différents niveaux de mandat

et le plus élevé est l'enregistrement des conversations. Et ça peut être capté à distance. Les enquêteurs privés ne l'ont jamais fait. Ils n'en ont jamais fait la demande, car ils n'ont pas eu besoin de se rendre jusque-là.

Pouvez-vous installer un GPS sur la voiture d'un individu sur lequel vous enquêtez ?

Théoriquement, selon la jurispru-dence, tu peux le mettre à partir du moment où le véhicule est la propriété de l'employeur. Mais ça peut dépendre des opinions juridiques... dans certains cas, ça dépend ce qui est fait avec la preuve, si ça a été fait de bonne foi dès le départ. C'est le tribunal-- qui décide si ça doit être accepté--.

Utilisez-vous beaucoup les réseaux sociaux ?

Oui, il y a un intérêt à aller voir sur Facebook, parce qu'il y a des gens qui mettent tout ce qui se passe dans leur vie. L'année dernière, on a réglé notre premier cas de fraude à la CSST uniquement grâce aux preuves recueillies-- sur Facebook. L'individu était sur la CSST et mettait en ligne des vidéos de lui en train de construire son chalet. C'était public. Alors oui, on va continuer à utiliser Facebook pour un bon bout de temps. Mais il y a eu des cas où l'information recueillie sur Facebook a été jugée irrecevable en cour parce que c'était jugé abusif.

Est-ce que la bêtise des gens vous surprend encore après toutes ces années de métier ?

Les gens sont faciles à détourner. Leur attention n'est pas super aiguisée. On dirait que les gens ne portent pas attention aux détails. Les gens se questionnent peu et ne se méfient pas assez.

Est-ce que le travail d'enquêteur se fait maintenant surtout derrière un ordinateur ?

Il y a encore des agences qui se spécialisent uniquement en filature. Mais dans l'ensemble des dossiers maintenant, il y a une portion informatique.

Est-ce que la technologie a faci-lité le travail ?

Oui et non. Ça a complexifié le travail, c'est certain. Il y a 25 ans, il n'y avait pas d'ingénieur informatique dans les agences d'enquête. Aujourd'hui, ça en prend. La quantité de documents à analyser est parfois phénoménale. Dans un dossier, on a eu 23 millions de documents à analyser. Tu ne fais pas ça à la mitaine.

Quel conseil pouvez- vous donner pour mieux protéger l'information sur nos cellulaires ?

Si tu veux vraiment avoir des conversations confidentielles, fais-le en personne sans ton téléphone. C'est à ce point-là. Il y a des logiciels qui rendent ton cellulaire hyper sécuritaire, mais tôt ou tard, ça peut être craqué.

Plus de 25 ans de métier

Claude Sarrazin a fondé son agence d'enquête il y a 25 ans. Son premier mandat, à 20 ans, a été d'infiltrer une entreprise, qu'il ne peut identifier, afin de découvrir si du trafic de drogue avait cours sur le lieu du travail.

En se faisant passer pour un employé, il a découvert que certains vendaient de la drogue à leurs collègues et utilisaient même les camions de l'entreprise pour distribuer de grandes quantités de stupéfiants.

«Il s'agissait de personnes associées aux motards qui se servaient de l'entreprise comme cover pour distribuer de la marchandise aux quatre coins du Québec et en Ontario, sans même avoir à payer le gaz!» dit-il. Le travail d'infiltration avait duré un an.

Canberra Times
Security Headquarters plagued with clearance problems Cyber spooks quit ASIO
Sunday, 27 November 2016
Byline: Stephen Jeffery

Canberra - Australia's premier cyber security agency has released plans to leave ASIO's headquarters for larger, lower security premises, two years since it first moved into the custom-designed building. The hurdles to gaining clearance to work in or visit the Australian Cyber Security Centre (ACSC) in the classified Ben Chifley Building in Parkes hindered the organisation's recruitment and collaborative goals, a Department of Defence submission to the parliamentary committee evaluating the proposal said. The department proposed a $38.8 million relocation and fitout of the ACSC to Defence-leased buildings at Brindabella Business Park near Canberra Airport.
If approved, the centre's new headquarters would incorporate multiple security clearance levels, a mix of classified, unclassified and public meeting rooms, and space for a major expansion of its workforce to about 650, flagged in this year's Cyber Security Strategy. The centre, currently made up of about 260 cyber security specialists from the Australian Signals Directorate, the Attorney- General's Department, ASIO, the Australian Federal Police and the Australian Crime Commission, began operating on November 27, 2014, and was the first tenant to move into the Ben Chifley Building. But the Defence submission said

the classified nature of the building had impeded the centre's ability to collaborate with businesses and researchers, a core element of the Cyber Security Strategy. The need to be approved for high security clearance, which can take more than two years, was dissuading skilled workers from joining the ACSC, the submission said. The strategy, released in April, stipulates that "organisations need easy and consistent interfaces with government agencies on cyber security" and mandated that the centre move to a new location. "The need for private industry partners to obtain security clearances - and even the

overheads associated with organising visitor entry for short-term visits - currently make achievement of the government's intent considerably more difficult," the submission said. "Cyber security skills are in short supply and high demand ... very few people with the requisite skills will be prepared to wait for a role with ASD, particularly when private industry is able to offer very attractive remuneration." The building has had a chequered history, including delayed construction, reported security breaches and a $200 million budget blowout. Most of ASIO's estimated 1800 staff had moved into the $700 million building by 2015, two years behind schedule. Smashed glass panels and malfunctioning alarms made unwanted headlines last

year. Most of the work of the Australian Signals Directorate with the ACSC could be handled in a lower security environment, the Defence submission said, with its classified status seen as more of a "legacy". It pointed to Britain's National Cyber Security Centre, which is being built in London as a mostly unclassified facility, as a comparison. Depending on when it is approved, the ACSC's new headquarters could be completed by the end of 2017, with initial workers moving into the building from June. The Parliamentary Standing Committee will accept submissions on the proposal until January 13, with public hearings expected to take place later in the new year.

The International Business Times
FBI targets Islamic State social media chiefs
Sunday, 27 November 2016

Washington - The FBI has assassinated more than a dozen of Islamic State's (IS) most influential social media experts who incited followers to commit terrorist atrocities in the Western world, it has been claimed.
An American and allied forces campaign, aimed at tackling online extremism, targeted a cell known as "the Legion" in a coordinated and secretive mission to undermine IS's (Daesh) ability to incite attacks by its followers across the globe.

While American military, intelligence and law enforcement officials acknowledge the group's potent social media influence, they believe their efforts against "the Legion" have significantly reduced IS's capabilities to order and inspire attacks in Europe and the US.

Junaid Hussain, from Birmingham, led the group as one of its most influential hackers and online recruiters, according to the New York Times.

The 21- year-old was targeted in 2015 by armed drones in eastern Syria, killing him as he exited an internet cafe in Raqqa.

Initially, the threat of "the Legion" was considered to be at a law enforcement level. However, last year, the FBI stepped up its monitoring of the cell, according to officials.

While allied forces in Syria took aim at the group in a series of drone strikes, the FBI analysed their social media reach, pinpointing who had been inspired to take action and making nearly 100 subsequent arrests.

Many of the arrests were of people who had been in direct contact with "the Legion" on social media. Others had connections with Hussain and Reyaad Khan, another British leader of the group, Andrew McCabe, deputy director of the FBI told the New York Times.

In March 2015, Hussain and Khan's group was responsible for posting the names and addresses of military officials with the message: "Kill them in their own lands, behead them in their own homes, stab them to death as they walk their streets thinking they are safe."

Court records show Hussain was in touch with at least four men in four different states, urging them to commit attacks and fuel violence.

Hussain encouraged Usaamah Abdullah Rahim, who was killed by the FBI in 2015, to behead Pamela Geller, a conservative blog author. A mission he did not fulfil.

Other members of "the Legion" were also inciting violence online. Another Briton, Raphael Hostey, urged 19-year-old Mohammed Hamzah Khan from Illinois to travel to Syria, however he was stopped with his two younger siblings by the FBI.

According to a senior American law enforcement official, the spring and summer of 2015 was a "nightmare" for the FBI after a string of attacks left the bureau overstretched and under strain.

FBI director, James B Comey, told the New York Times the bureau was struggling to keep up with the fast-moving pace of the evolving threat, forcing it to move criminal officers to surveillance squads.

Months of drone strikes by American and British forces followed, killing Hostey in May and Khan some months later.

An Australian, Neil Prakash, was targeted in a strike around the same time. However, he survived the attack. According to a military official, he was arrested recently by an undisclosed Middle Eastern Government.

IS has been slow to replace "the Legion" and American officials have expressed surprise at its failure to replace hackers such as Hussain.,

However, the Bureau says it's still working hard to fight the group's work, even after "the Legion" has been neutralised.

"We are still dealing with the repercussions of that development and that recruitment of that network to this day," the FBI's Mr McCabe told the the New York Times.

Press Trust of India
Cyber attacks can cause more damage than conventional forces
Monday, 28 November 2016

New Delhi - In April 2015, the website of the office of Principal Controller of Defence Accounts (Officers) - PCDA(O) - located in Pune, was hacked. The website contains information about salaries and allowances of all serving officers of the Indian Army, across ranks. Though officials claimed that no data was lost, the act prompted the office to launch a new website with updated security features. Nearly a year later, the same office warned Army officers against clicking on links sent to them via fake messages, saying PCDA(O) had developed a phone-based app and was seeking the officers' personal information. The messages were considered to be another attempted cyber attack.

This example from Pune in the recent past is yet another proof of the increasing threat of cyber terrorism, pointed out defence officials.

With almost all sectors - railway networks, communication and stock markets among others - heavily dependent on data communication and storage, experts fear that a cyber attack on any of these is capable of causing more damage than conventional forces.

A senior Army official, who has been working in the field of cyber security, said, "This is an ongoing war and it is on as we speak. The threat to our cyber security is not just from countries like China and Pakistan, but also from non-state actors like terror groups. And these attacks can come in any form, such as hacking of websites, computer viruses and Trojan attack. It can also be a more specialised form of attack, like denial of service, a cyber attack when even authorised persons lose access to their systems, or a cryptological attack, when the attacker encrypts all the data and it takes time and effort to decrypt it. In this non-contact type of warfare, the adversaries will try to cripple each others' systems, rather than actually carry out an attack on the ground."

National security expert Lieutenant General (Retired) D B Shekatkar, who has served in the intelligence arm of the Army, said, "Cyber terrorism is currently one of the biggest challenges to national security. We are heavily dependent on web-based technology for the operation of railway networks, air transport network and communications networks. These systems can be brought to a grinding halt by cyber attacks... for example, attacking the railway or air traffic network would prove way more damaging than bombing a bridge or an airport. These attackers can even target our nuclear armoury or satellite systems."

Another Army official spoke about the "psychological aspect" of a cyber attack. "Here, the adversaries indoctrinate people, especially the young generation. They then train and use them to carry out attacks

on others. We have several examples of the youth being targeted through Internet by organisations like the Islamic State."

He added, "But the Indian Army is keeping no stone unturned in preparing itself to face any kind of cyber attack. We are in constant communication with the National Informatics Centre, the Indian Computer Emergency Response Team, the National Information Security Assurance Programme of the central government. Regular cyber audits are carried out at the unit level and above. The Army strictly uses its own network for internal communication... storage devices are completely prohibited and any kind of violations is strictly dealt with".

Bangkok Post
Fingerprint ID set to be mandatory
Monday, 28 November 2016
Byline: Komsan Tortermvasana

Bangkok - All mobile operators will have to introduce an online fingerprint ID system for new prepaid and postpaid mobile SIM card registration, with a tentative deadline set for next February.
The National Broadcasting and Telecommunications Commission (NBTC), however, compelled all existing mobile users to put their fingerprints in the system on a voluntary basis for their own security benefit.

"We urge all mobile users to participate in the system to ensure greater security of the mobile banking channel and prevent the risk of fraud, which is likely to increase in a cashless society," said NBTC secretary-general Takorn Tantasith.

Thailand has 103 million mobile subscribers, 14 million of whom use mobile banking services, he said.

Through a fingerprint enrolment process, mobile operators will scan each person's fingerprints and store the records on the NBTC's secure database server, said Mr Takorn. Mobile operators will develop an application that verifies customers' fingerprints.

Mobile banking is a service provided by banks or other financial institutions as well as mobile operators that allows customers to conduct some financial transactions remotely using any mobile device, with no bank account required.

The popularity of mobile banking activities marks a significant trend taking place in banking. But fraud and other criminal acts targeting telecommunication networks are also becoming increasingly sophisticated.

The NBTC's telecom committee approved the plan to use a fingerprint registration system in September. Mr Takorn said the NBTC adopted the fingerprint system which was developed by the Engineering

Faculty of Kasetsart University. The school won an auction held by the NBTC this month offering to supply the system for 15 million baht.

He said the fingerprint system would not create a financial burden on mobile operators because the investment can be deducted as a business expense from the universal service obligation (USO) fee operators pay annually to the NBTC.

Telecom operators have to share 5% of their total revenue with the NBTC. Of the total, 3.5% is paid for the USO fee and the remaining 1.25% goes to the licensing fee.

Mr Takorn insisted that the fingerprint system will complement the existing registration system. The regulator will not force all mobile users to register with the new system.

Banks and mobile operators have increasingly been urged to boost the standards for customer authentication systems in a bid to prevent fraud through mobile banking activities -- currently one of the most popular mobile services. The concern follows several cases of fraud committed through mobile banking apps over the past several months.

Le Monde
La surveillance de masse tend à se generaliser
Saturday, 26 November 2016
Byline: Morgane Tual

Paris - Après la France et l'Allemagne, le Royaume-Uni vient d'adopter une loi musclée sur le renseignement
De son côté, l'Allemagne a élargi, en octobre, le champ de la surveillance du BND, le service fédéral de renseignement, dans le cadre d'une réforme qui vise à mieux l'encadrer. Le BND est désormais autorisé à collaborer avec la NSA et, dans certains cas, à espionner les institutions européennes et les Etats membres.

Plus tôt dans l'année, le gouvernement avait donné son accord à l'utilisation d'un logiciel espion qui permet de dérober des informations sur une machine. Des signaux loin d'être anodins, dans un pays où la question de la surveillance reste épineuse, en raison d'une histoire marquée jusqu'à la chute du Mur par la Stasi, la police secrète est-allemande.

Du côté des Etats-Unis, la victoire de Donald Trump à l'élection présidentielle, le 8 novembre, a suscité des inquiétudes. " Voilà pourquoi il ne faut pas construire des outils de surveillance secrets et tout-puissants, critiquait, par exemple, sur Twitter, un ingénieur en sécurité informatique au lendemain de l'élection. Vous ne savez jamais quel gars finira par avoir les clés. " La proposition de Donald Trump d'installer Mike Pompeo à la tête de la Central Intelligence Agency n'a pas rassuré les opposants à la surveillance de masse : celui-ci veut encore étendre ses pouvoirs, s'est plaint de les avoir vus s'affaiblir

après les révélations de Snowden, et a fait savoir qu'il souhaiterait voir le lanceur d'alerte condamné à la peine de mort.

" Empêcher la dérive fasciste "Déjà, des voix s'élèvent pour implorer Barack Obama de restreindre le champ d'action de la NSA avant la prise de pouvoir de son successeur. L'actuel président américain " a encore quelques semaines pour faire une chose qui pourrait empêcher les Etats-Unis de dériver vers le fascisme : déclassifier et démanteler autant que possible " les outils de surveillance de la NSA, écrit, le 9 novembre, dans une tribune publiée dans le Time, Evan Greer, directeur de campagne de l'organisation Fight for the Future, consacrée aux libertés numériques.

Edward Snowden a tenu sur Twitter des propos dans ce sens, peu après le résultat de l'élection : " Les pouvoirs d'un gouvernement sont transmis au suivant. Les réformer maintenant est l'une des plus grandes responsabilités de ce président, ce qui aurait dû être fait il y a longtemps. "

Mais, jusqu'ici, Barack Obama semble rester sourd à ces appels, tout comme à ceux qui l'implorent d'accorder son pardon à Edward Snowden avant de quitter le bureau Ovale. " En pardonnant à Snowden, le président Obama contribuerait à pérenniser son héritage, tout en envoyant un puissant message - que s'élever contre les abus d'un gouvernement est une tradition que nous devons chérir et emporter avec nous ces quatre prochaines années ", soulignait, le 18 novembre, Noa Yachot, responsable de la campagne Pardon Snowden. Le même jour, dans les colonnes du quotidien allemand Der Spiegel, Barack Obama répondait par la négative : " Je ne peux pas pardonner à une personne qui ne s'est pas présentée devant un tribunal ", a-t-il déclaré.

De son côté, le lanceur d'alerte ne semble pas s'inquiéter outre mesure des conséquences de l'arrivée de Donald Trump. Lors de plusieurs visioconférences données depuis la Russie, où il a obtenu l'asile, Edward Snowden a répété que M. Trump " n'est que président ". Pour lui, la victoire de ce candidat représente " un moment sombre dans l'histoire, mais ce n'en est pas la fin "." Il faut que nous commencions à réfléchir non pas à la façon de se protèger de Trump, mais à la façon de protéger le droit de tout le monde, partout. (...) Et si on protégeait nos communications, dans le monde entier ? Soudain, on ne ferait pas que protéger les droits des gens, on pourrait les garantir. La technologie rend cela possible. "

Ces propos lui ont valu des critiques acerbes, notamment de la part du site Gizmodo, qui a qualifié l'Américain de " putain d'idiot ", qui " croit que la technologie est plus importante que la politique pour protéger les libertés ".

Et pourtant, c'est surtout sur ce plan qu'Edward Snowden a réussi son pari : celui des technologies. Ses révélations ont certes entraîné, dans la foulée, quelques timides réformes aux Etats-Unis, ainsi que des enquêtes parlementaires en Allemagne et au Brésil. Mais son action a surtout permis de faire découvrir au grand public l'ampleur de la surveillance et des capacités techniques de la NSA, ainsi que les moyens de s'en prémunir. Là où l'utilisation d'outils de communication chiffrés était, jusque-là, réservée à un petit groupe d'initiés, leur usage s'est démocratisé ces dernières années. L'application Signal, qui permet

de communiquer de façon sécurisée, plébiscitée par M. Snowden, assure avoir vu ses téléchargements multipliés par quatre depuis la victoire de Donald Trump.

Qui plus est, l'épisode Snowden a profondément modifié la façon dont les géants du Web conçoivent leurs produits. Certains de ses documents faisaient mention d'un accès direct de la NSA aux serveurs d'entreprises comme Google et Facebook - ce qu'elles ont toujours démenti.

Pour reconquérir la confiance de leurs utilisateurs, la plupart de ces entreprises ont renforcé la sécurité de leurs services, et les messageries chiffrées tendent désormais à devenir la norme. Ironie de l'histoire : ce sont désormais ces grandes multinationales qui se posent en rempart contre la surveillance de masse, alors même que leur modèle repose sur l'exploitation des données personnelles des internautes.

LePoint.fr
L'homme le mieux renseigné du monde
Saturday, 26 November 2016

Washington- Oubliez la Maison-Blanche. L'endroit le plus stratégique des Etats-Unis, le coeur du réacteur de la première puissance du monde n'est pas au 1600 Pennsylvania Avenue, à Washington. Il se situe derrière un grand mur de minuscules briques rouges percé de vitres teintées. C'est le siège de Palantir. Une société américaine qui tire son pouvoir de l'exploitation industrielle, mais minutieuse, de milliards de données géographiques, économiques, climatiques, militaires, politiques, démographiques... Une entreprise secrète, qui travaille aussi bien pour l'armée que pour de grands groupes privés et n'a ni l'habitude ni l'envie de recevoir des journalistes. Avant de pénétrer dans la forteresse Palantir, le visiteur peut néanmoins aller prendre des forces chez Lyft, un bar qui sert du jus de concombre à la menthe ou des smoothies au chou kale, fréquenté par des étudiants de Stanford. Quel silence ! Seul le ronflement du Caltrain, ce vieux tramway mécanique qui rallie, en quarante-cinq minutes, la petite ville tranquille de Palo Alto à San Francisco, rivalise avec la caresse du vent sur les érables. Au 100 Hamilton Avenue, on vérifie bien que l'on ne s'est pas trompé d'adresse : ici, il n'y a pas d'écriteau flashy géant devant lequel les touristes se prennent en photo comme on en trouve devant les QG de Facebook, Google ou Yahoo! La même discrétion est de mise sur la vingtaine de bâtiments loués par Palantir, un espace qui occupe environ 10 % des bureaux de la capitale de la Silicon Valley.
A l'accueil, c'est à un iPad que l'on doit montrer patte blanche. Quelques questions rapides pour gagner le droit de s'asseoir dans une salle d'attente décorée de peintures néocubistes, à côté d'un garage à vélos et juste au-dessous d'un immense mur de tee-shirts. Toutes les tailles sont disponibles, mais le teeshirt est toujours le même. Gris anthracite, il est estampillé de la devise maison : « Save the shire ». Clin d'oeil de la société au roman fantastique de J. R. Tolkien, « Le seigneur des anneaux » : The Shire, c'est la Comté, le pays paisible et verdoyant des Hobbits. Il faut sauver la Comté. Ce qui revient à vouloir sauver le monde pour les 1 500 employés de l'entreprise. Le nom de Palantir, désigne, lui, la « Pierre de vision », une sorte de globe de cristal inventé par les elfes, qui permet d'observer des lieux distants dans l'espace et surtout de voir dans le futur. Avant de monter dans les étages, le visiteur passe à travers un sas surplombé de deux drapeaux : un américain et un britannique.

Palantir, créé en 2004 et valorisé 20 milliards de dollars, c'est un peu les oreilles et les yeux de l'Amérique. Grâce à sa puissance de calcul, il a aidé la CIA à localiser et neutraliser Oussama ben Laden, ou encore à tracer les hackers qui s'en sont pris à la messagerie électronique du dalaï-lama. Et dire que ce projet, qu'on croirait tiré du film de science-fiction « Minority Report », est né dans la tête d'un docteur en théorie sociale. Inclassable Alex Karp... Un fan du philosophe allemand Jürgen Habermas, dont il fut l'un des élèves en Allemagne. Et un dingue de robotique. Durant son temps libre, Karp dirige Robotex, entreprise qui met au point des robots de surveillance. Né à Philadelphie il y a quarante-neuf ans, il a d'abord étudié au Haverford College dans une ambiance libertaire. Ses parents étaient deux hippies - l'un des deux était artiste, l'autre pédiatre. Il a rédigé ensuite une thèse à la Johann Wolfgang Goethe Universität de Francfort, « Aggression in der Lebenswelt : Die Erweiterung des Parsonsschen Konzepts der Aggression durch die Beschreibung des Zusammenhangs von Jargon, Aggression und Kultur ». En clair, Karp est un spécialise du Lebenswelt, le « monde vécu », une philosophie de la vie théorisée par Edmund Husserl, mort en 1938, qui insiste sur la nécessité de vivre pleinement son existence.

Son doctorat en poche, Karp, par ailleurs francophone, crée, avec l'argent dont il a hérité après le décès de son grand-père, un premier fonds d'investissement à Londres, le Caedmon Group - le nom rend hommage à un poète anglais du VIIe siècle, dont l'histoire a été racontée par le moine érudit Bède le Vénérable. Il traque les plus prometteuses des start-up. Mais le 11 septemble 2001 lui fait l'effet d'une grande claque. Alex Karp se sent soudain investi d'une mission salvatrice. Il y a quelque chose à faire, avec Internet, avec les données, pour aider l'Amérique en danger. Il en parle avec son ami Peter Thiel, rencontré sur les bancs de la fac de droit de Stanford, où Karp avait effectué un autre doctorat à son retour d'Allemagne. Ils ont cohabité dans l'internat de Crothers Hall. Ils partagent le même goût pour la culture allemande et pour la philosophie. C'est avec Peter Thiel, le spécialiste de l'intelligence artificielle Stephen Cohen, l'entrepreneur Joe Lonsdale, qui est désormais membre du conseil d'administration de Hyperloop, et Nathan Gettings, un autre diplômé de Stanford, que Karp fonde Palantir. Aujourd'hui, cette entreprise est devenue son obsession. « Les seuls moments où je ne pense pas à Palantir, c'est quand je pratique la natation, le qi gong ou une activité sexuelle », explique Alex Karp au magazine Forbes.

Ce célibataire fan de tai-chi version Chen, le plus ancien style de cet art martial chinois, suscite l'admiration de ses troupes. « Il est notre conscience », ira jusqu'à expliquer l'ingénieur senior de Palantir Ari Gesher. Ce proche de Michael Dell est capable de déclarer que « la profession est culturellement corrosive » tout en planchant, avec Farry Tan, le dixième employé de l'entreprise, sur le design du logo qui représente « un orbe de connaissance qui vous donne la possibilité de lire à travers les secrets de vos ennemis ». Un des premiers investisseurs dans Palantir est le fonds de capital- risque In-Q-Tel, le bras financier de la CIA, qui mise 2 millions de dollars. Peter Thiel, qui avait déjà fait fortune grâce à la vente de PayPal, investit également un gros paquet de dollars, ainsi que son savoir- faire technique développé dans le service de paiement en ligne pour détecter les activités frauduleuses...

La recette de Palantir ? Le « data crush », c'est-à-dire rassembler, compiler, qualifier, croiser, recroiser une foule d'informations qui, a priori, n'ont rien à voir les unes avec les autres. Ses logiciels qui sont

autant de références à la science-fiction ou à l'univers des comics - Gotham, Metropolis... - transforment des données abstraites en informations tangibles et exploitables. Des données qui sont ensuite visualisées dans des cartes et des plans hyperdétaillés. En récupérant des data par tous les moyens, notamment sur les historiques de nos ordinateurs ou sur les réseaux sociaux, on établit des liens entre les individus, les lieux qu'ils fréquentent, leurs habitudes de vie et de consommation... Dans le jargon, on appelle cela le big data à signaux faibles. Palantir travaille par exemple avec la ville de New York pour anticiper l'écroulement des bâtiments les plus fragiles, ou encore, depuis six mois, avec la banque Credit Suisse pour déterminer lesquels de ses salariés sont susceptibles de détourner l'argent de l'établissement et les confondre, le cas échéant.

Cette entreprise, d'après le site d'information TechCrunch, travaille pour au moins 13 administrations américaines - dont la CIA, la NSA, le FBI ou les Marines. En fait, Palantir n'a cessé d'enrichir le profil de ses clients. Pas de certitude, car le secret est bien gardé. Mais Coca-Cola et BP seraient clients, ainsi que de nombreuses institutions financières américaines, comme JP Morgan ou encore le Nasdaq, Bridgewater Associates, l'assureur Axa, qui traque la fraude dans les déclarations de sinistres, ou le fabricant de confiseries Hershey's. En interne, les grands comptes sont affublés de noms de code : Sherlock désignait un moment Home Depot et American Express répondait au doux pseudo de Charlie's Angels. Vous entendez parler de Gouda ? Il s'agit en réalité de News Corp, le géant du divertissement et de la communication de Rupert Murdoch. Le millardaire australien s'est déplacé lui-même dans les bureaux protégés de Palo Alto. Grâce aux informations sur les abonnés et leurs habitudes collectées par Palantir, le groupe aurait réussi à réduire son taux de désabonnements. Un organisme canadien de recherche sur l'émergence du cyberespace, l'Information Warfare Monitor, utilise le logiciel offert par Palantir pour démasquer les réseaux de hackers, dont GhostNet. Autre exemple, les données de Palantir ont été utiles à l'Agence internationale de l'énergie atomique. Elle voulait obtenir certaines assurances, notamment que l'Iran et la Corée du Nord respectent bien le traité de non-prolifération...

« La vie des autres. » Palantir dispose, depuis quelques mois, d'un bureau à Paris. « Les entreprises françaises qui développent des systèmes ne sont pas encore capables de répondre à nos besoins, alors que nous devons acquérir ces big data immédiatement. Nos camarades européens sont dans la même situation. Le choix n'a pas encore été fait, mais, en tout état de cause, la solution sera temporaire », a expliqué Patrick Calvar, le directeur de la Sécurité intérieure, lors d'une audition à l'Assemblée, le 10 mai. Comme une façon de convaincre les sceptiques dans le cas où les services secrets français feraient appel à une entreprise américaine...

D'autant que Palantir compte parmi ses conseillers l'ex-secrétaire d'Etat Condoleezza Rice, l'ex-directeur de la CIA George Tenet ou David Petraeus, ancien général de l'armée américaine. « Croire que les données sensibles n'atterrissent pas au Pentagone, ce serait faire preuve d'une grande naïveté », assure Bernard Benhamou, secrétaire général de l'Institut de la souveraineté numérique. Il anticipe un scénario qui ressemblerait à celui du film « La vie des autres », mettant en scène un agent allemand espionnant tout de la vie de ses cibles : « Ce genre de société qui sait tout sur tout permet de faire pression sur les gens sans le savoir. » Pour Henri Verdier, le directeur informatique de l'Etat, la meilleure manière de ne pas abandonner le traitement de toutes nos informations aux Américains serait de nous

donner la capacité d'analyser nous-mêmes nos propres données. « Il ne faut pas réagir à la Vauban comme si on devait protéger une citadelle assiégée, mais plutôt sur le modèle des Anglo-Saxons en manoeuvrant de manière agile pour créer notre propre solution. »

Dans les bureaux de Palo Alto, on regarde souvent cette carte du monde dessinée à la manière du jeu de société Risk. Palantir a déjà des bureaux dans une dizaine de pays. En interne, chaque nation a un nom de code tiré de l'oeuvre de Tolkien. Arandor a ainsi été le surnom pour certains employés d'Australie, Almaren de Singapour, et Belfalas d'Italie. Le nom des salles, comme Galadriel, rend également hommage à l'écrivain britannique. Après seulement douze ans d'existence, Palantir a levé plus de 2,3 milliards de dollars auprès de différents investisseurs. Y a-t-il une bulle Palantir ? L'entreprise n'étant pas cotée, les informations précises sur les ventes, les clients ou les bénéfices sont invérifiables. Son PDG, Alex Karp, avait annoncé en 2013 que la compagnie ne serait pas introduite en Bourse, car « cela la rendrait très difficile à diriger ». Palantir peut sans cesse être challengé par de nouveaux concurrents, à l'instar de l'américain Lumify. Et il doit rendre des comptes sur l'exploitation des données. Récemment, il a par exemple été montré du doigt parce qu'il avait utilisé le scan de milliers de plaques d'immatriculation aux Etats-Unis...

« Beer pong. » Pour montrer que la mission de Palantir est planétaire et surtout sert la bonne cause, Alex Karp met l'accent sur la philanthropie. « Nous voulons éviter que des virus ne déciment des populations entières tout en respectant les libertés individuelles », explique le numéro un. On l'a récemment vu converser à la conférence Sun Valley, dans l'Idaho, avec la philanthrope Laura Arrillaga Andreessen. Bill Clinton a salué, dans une vidéo, la technologie maison pour mettre en place les secours après l'ouragan Sandy. En 2012, l'entreprise a par ailleurs travaillé avec Interpol pour lutter contre les abus sexuels sur les enfants.

De Palantir on aura aperçu des salles tapissées de posters de Fleetwood Mac, des photos d'un séminaire de ski à la Squaw Valley, la pièce où les salariés jouent au « beer pong », dont le but est d'envoyer une balle de ping-pong dans un verre et, en cas d'échec, de descendre d'une traite un shot de pale ale. Mais, au final, on repart avec autant de questions qu'à l'arrivée. Au moment du départ, une employée sort un appareil photo pour réaliser un cliché du visiteur. « C'est pour ma collection personnelle », dit-elle d'un ton rassurant. On quitte les lieux un peu chamboulé tout de même. Dehors, le vent continue de caresser les érables.

London Times
Hackers target British and US athletes
Saturday, 26 November 2016
Byline: Martyn Ziegler

London - Dozens of confidential emails from senior figures in the World Anti-Doping Agency and US antidoping have been released by the Russian hacking group Fancy Bears. The emails, seen by The

Times, contain private details about athletes from a range of sports and include details of suspicious samples, medical information and confidential discussions between anti-doping officials.
The security breach has led to emails and voicemail messages from the account of Wada's legal director Julien Sieveking being released by the Russian group, and will be a concern to the agency, which is still reeling from having its database hacked in September. That hack revealed dozens of athletes' therapeutic use exemptions allowing them to take banned drugs to treat medical conditions.

It is the second time the hackers have released emails from Usada. This time the Usada emails reveal: ? Possibly unusual blood values for some of the biggest names in American sport.

? Details on legal medications and supplements taken by dozens of athletes including by distance runner Galen Rupp, Mo Farah's training partner, such as thyroid medicine Cytomel that Usada and UK Anti-Doping want to see banned but is legal at present. ? Usada chief executive Travis Tygart suggesting officials "go robust" with an NFL player considering trying out for the US Olympic rugby sevens team.

The Wada emails contain numerous details about existing doping cases from around the world and whether they constitute doping violations.

The emails also show a Wada official stating on July 28 that Qatar's testing laboratory was going to be suspended the following week. As it turned out, that announcement was not made until this month -- and Wada was strongly criticised for making the announcement on the same day that Qatar was hosting an Olympic conference.

The leak also contains further exemptions obtained by British athletes to treat medical conditions -- there is no suggestion any of those concerned have done anything wrong. Sprinter Adam Gemili was given an exemption for a painkiller he was given after he tore his hamstring at the Birmingham Grand Prix in June 2015. Emily Scott, a British rugby sevens player, said she was given corticosteroids to treat rheumatoid arthritis, adding: "I know that I have done everything I can as a clean athlete and fully support the work of the anti-doping movement."

One Team Sky cyclist was given the diuretic furosemide in 2014 as part of a kidney scan when his major organs were inspected after a crash where he fractured a vertebrae.

Wada said the leak came from the same breach to its system as that which took place in August.

In a separate development, the German broadcaster ARD has published a 2014 letter sent to the IAAF by Russia's then athletics chief threatening to expose the organisation for blackmailing them over positive drugs tests. The letter claims that he had seen a list of athletes with biological passport violations, saying: "Surprisingly we found there some prominent British athletes including [an] Olympic champion."

The IAAF said it had no knowledge of anyone the letter was referring to.

Daily Telegraph (Australia)
MI5 urged to begin keeping tabs on far-Right extremists
Saturday, 26 November 2016

London - The security services have been urged to start monitoring far-Right extremists amid concern over the rising numbers of fanatics coming to the attention of the authorities.
Currently the police, not the MI5, have responsibility for monitoring political extremists.

But in the wake of the murder of Labour MP Jo Cox by neo-Nazi Thomas Mair, there have been calls for the security services to put the problem of the far-Right on a par with the Islamist terror threat. The number of Right-wing extremists referred to the Government's counterradicalisation programme, Prevent, has increased by more than 70 per cent in the past 12 months, figures show.

Rupert Sutton from the Henry Jackson Society, a think-tank that works to combat extremism, said "if far-Right groups such as National Action continue to develop ... I certainly think there would be a case to be made for MI5 to become more involved."

New York Times
U.S. Officials Defend Integrity of Vote, Despite Hacking Fears
Saturday, 26 November 2016
Byline: David E. Sanger

Washington - The Obama administration said on Friday that despite Russian attempts to undermine the presidential election, it has concluded that the results "accurately reflect the will of the American people."
The statement came as liberal opponents of Donald J. Trump, some citing fears of vote hacking, are seeking recounts in three states -- Wisconsin, Michigan and Pennsylvania -- where his margin of victory was extremely thin.

A drive by Jill Stein, the Green Party candidate, for recounts in those states had brought in more than $5 million by midday on Friday, her campaign said, and had increased its goal to $7 million. She filed for a recount in Wisconsin on Friday, about an hour before the deadline.

In its statement, the administration said, "The Kremlin probably expected that publicity surrounding the disclosures that followed the Russian government-directed compromises of emails from U.S. persons and institutions, including from U.S. political organizations, would raise questions about the integrity of the election process that could have undermined the legitimacy of the president-elect."

That was a reference to the breach of the Democratic National Committee's email system, and the leak of emails from figures like John D. Podesta, Hillary Clinton's campaign chairman.

"Nevertheless, we stand behind our election results, which accurately reflect the will of the American people," it added.

Supporters of Mrs. Clinton have enthusiastically backed the notion of challenging the results in the three states as a last-ditch effort to reverse Mr. Trump's clear majority in the Electoral College. They have seized on suggestions by some computer scientists that the states, which were crucial to Mr. Trump's victory, need to manually review paper ballots to assure the election was not hacked.

The campaign, uniting around the hashtag #AuditTheVote, has picked up momentum among grass-roots activists still mourning Mr. Trump's victory. But the pleas for recounts have gained no support from the Clinton campaign, which has concluded that it is highly unlikely to change the outcome.

In Michigan, Ms. Stein must wait for a Monday meeting of the state's Board of Canvassers to certify the results of the Nov. 8 balloting before filing for a recount. In Pennsylvania, where paper ballots are used only in some areas, election officials said that the deadline to petition for a recount had passed, but that a candidate could challenge the result in court before a Monday deadline.

The recount efforts have generated pushback by experts who said it would be enormously difficult to hack voting machines on a large scale. The administration, in its statement, confirmed reports from the Department of Homeland Security and intelligence officials that they did not see "any increased level of malicious cyberactivity aimed at disrupting our electoral process on Election Day."

The administration said it remained "confident in the overall integrity of electoral infrastructure, a confidence that was borne out." It added: "As a result, we believe our elections were free and fair from a cybersecurity perspective."

However, intelligence officials are still investigating the impact of a broader Russian "information warfare" campaign, in which fake news about Hillary Clinton, and about United States-Russia relations, appeared intended to influence voters. Many of those false reports originated from RT News and Sputnik, two state-funded Russian sites.

Those fake-news reports were widely circulated on social media, independent studies, including one set for release soon, have shown, sometimes in an organized fashion by groups that appear to have had common ownership. Individuals, conservative talk- show hosts and activists recirculated them, often not knowing, or apparently not caring, about the accuracy of the reports.

A study published just before the election on warontherocks.com, written by Andrew Weisburd, Clinton Watts and J. M. Berger, documented efforts by "trolls" to attack the reputations of those who challenged Russia's activities in Syria, and to spread rumors about Mrs. Clinton's health. The study said that an effort to track 7,000 social media accounts over two and a half years indicated that support for

Mr. Trump "isn't the end of Russia's social media and hacking campaign in America, but merely the beginning."

But the misinformation effort is far from black-and-white. Many people who spread false news have no connections to any foreign power, including a man in Austin, Tex., who posted a Twitter message saying that paid protesters were being bused to an anti-Trump demonstration there. Though the report quickly went viral, the buses, it turned out, were there for a corporate conference.

Other examples, including one studied by a group called Propaganda or Not, appear to have more concrete connections to Russia. In late August, stories suggesting that Mrs. Clinton might have Parkinson's disease were circulated on trupundit.com, which often runs pro-Russian material. It clearly twisted an email sent by one of Mrs. Clinton's top aides about a drug called Provigil that is used to treat sleepiness. It has also been prescribed to patients with sleepiness as a side effect from several different ailments, the email added, including "Parkinson's, Alzheimer's and multiple sclerosis."

That single reference was enough to create a fake story suggesting that Mrs. Clinton was being treated for Parkinson's.

The allegation was quickly shot down by several news organizations. It made little difference: Propaganda or Not, made up of former national security, intelligence and other professionals, and some workers at Google and other technology firms, concluded that it was reproduced tens of thousands of times, sometimes by botnets, and viewed millions of times.

But it is not known whether that news was circulated under Russian government direction, or simply by Russian sympathizers, or Mrs. Clinton's opponents.

The barrage of online efforts to influence the election this year has prompted broader concerns that similar attempts, directed by the Kremlin or its surrogates, could now be focused on elections next year in Germany and France. The goal, intelligence officials and outside experts fear, is to undermine the cohesiveness of the Western alliance, particularly NATO members, by calling into question the validity of democratic elections.

"We simply don't know what the effects of the 'fake news' and other disinformation was," said Jason Healey, an expert on cyberconflict at Columbia University. "If they were able to influence in favor of Trump by one or two percentage points in some places, they will be encouraged to try again for the French and the Germans."

The efforts have also prompted debate inside Facebook and other social media firms about their responsibility to filter out false news. But doing so is a complex task, akin to editing a news operation, and it comes with complex political calculations: Once social media firms begin editing here to American standards, they will be under pressure from authoritarian regimes to do the same to their standards.

In its statement, the administration focused chiefly on the threat of Russian manipulation of the vote on Election Day, not on the proliferation of propaganda and fake news.

Ms. Stein, of the Green Party, acknowledged on Thursday in an interview with the PBS "NewsHour" that it was unlikely that recounts could change the results. Still, she said that "this was an election in which we saw hacking all over the place," and that "at the same time, we have a voting system which has been proven to basically be wide open to hackers."

Times of India
India ranked ninth in global race of supercomputers
Monday, 28 November 2016

New Delhi - Supercomputers are broadly defined as the fastest computing systems at any given time and are used for scientific purposes that require handling of troves of data at high speed. This includes testing mathematical models using thousands of variables to infer complex phenomena like weather, climate change, nuclear reactions, origin of the universe and so on.
The standard unit to measure computational power is FLOPS- floating point operations per second. It is the number of mathematical operations involving fractions that a computer can do per second. For the most basic computers and smartphones, the computational ability is a few megaflops (more than a million operations per second). Chinese supercomputer Sunway TaihuLight - which is ranked the fastest in the world by Top500 (a supercomputer ranking project) - has a computational ability of 93 petaflops, more than a billion times faster than normal computers. Recently it was announced that Japan will spend $173 billion to build the world's fastest supercomputer system with a capacity of 130 petaflops.

First, the maximum speed at which electronic signals can travel cannot be faster than the speed of light. Second, because of frequent receiving and transmission of these signals, it was important to have a suitable cooling technique to control the temperature of the system. Both barriers were tackled by decreasing the lengths these signals were required to traverse by using circuit boards and innovation in cooling techniques. Other advancements involved introduction of vector arithmetic in computing.

In 1965, CDC 6600, a supercomputer designed by US engineer Seymour Cray was installed at the CERN in Geneva, Switzerland. CDC 6600 had a computational capacity of three megaflops. In the 1970s, the series CDC 7600 was introduced, which was 10 times faster than the earlier version. In 1976, the Cray-1 supercomputer was installed in the Los Alamos laboratory with a computation capacity of 160 megaflops.

Cray's designs used expensive technology and liquid immersion technology to achieve high speeds. W Daniel Hill, an MIT graduate proposed a decentralised control instead of one CPU, which meant several inexpensive processors could be arranged to achieve speeds comparable to the most expensive supercomputer designed by Cray. Hill designed the CM-1 in 1985, which used thousands of inexpensive processors to achieve the same speed as Cray's computer.

Of the 500 fastest supercomputers, the highest numbers are in the US and China, each having 171 such systems. Germany, Japan and France each have 20 or more such systems. India is ranked 9th with five of its supercomputers listed in Top500.

London Daily Telegraph
Petition to repeal new surveillance powers reaches 100,000 signatures
Monday, 28 November 2016
Byline: James Titcomb

London - A petition demanding that the UK's new sweeping surveillance powers are repealed has garnered more than 100,000 signatures, the level at which Parliament can debate it.
Theresa May's controversial Investigatory Powers Bill, which have been described as the most extreme snooping laws in a Western democracy, were approved by the House of Lords earlier this month and are set to pass into law in the coming weeks.

They require internet providers to store customers' web histories for 12 months and make those records available to police, and write computer hacking by spy agencies into law.

The bill also requires companies to break encryption in certain circumstances, although groups such as Apple, Facebook and Google have argued that the parameters for this are hazy.

The petition warns that "With this bill, they will be able to hack, read and store any information from any citizen's computer or phone, without even the requirement of proof that the citizen is up to no good.

"This essentially entitles them to free reign of your files, whether you're a law-abiding citizen or not!"

On Monday morning the petition had received more than 118,000 signatures. At the 100,000 mark means a petition can be considered for debate in the House of Commons, although there is no obligation for Parliament to do so, and several petitions that have hit the level have not been debated.

Others include a demand for a second EU referendum, with over 4 million signatures, and one saying Donald Trump should be blocked from entering the UK, with over 500,000.

Opponents of the Investigatory Powers Bill believe that it has barely been scrutinised due to the fallout from June's EU referendum.

It has been criticised on privacy grounds, with bulk data collection even of those not suspected of wrongdoing. Internet providers will not collect the individual web pages browsers visit, just the main domain (such as telegraph.co.uk), but this is still seen as an invasion of privacy.

Security experts have also raised fears that companies' databases of browsing histories would be a boon for hackers.

The petition's supporters have included Kim Dotcom, the flamboyant founder of Megaupload, and the Open Rights Group.

The bill also faces legal challenges from anti- surveillance groups.

New York Times
Pentagon: Looking for a Few Good Hackers
Monday, 28 November 2016
Byline: Editorial Board

Editorial - In June 2015, the Office of Personnel Management announced that foreign hackers had stolen the personnel records of millions of federal employees, one of the most damaging cyberattacks in history. Just weeks later, the office of the Joint Chiefs of Staff shut down its unclassified email system for several days after officials detected that it had been breached.
These serious intrusions came months after a group affiliated with the Islamic State briefly commandeered the Central Command's Twitter account and rebranded it as the "Cyber Caliphate."

Given the enormity of the problem, one of the responses by the Department of Defense might seem befuddling. They've asked hackers willing to play by strict rules to find vulnerabilities in some of the Pentagon's unclassified computer system.

Well-intentioned computer security experts routinely scan the internet in search of vulnerabilities, which they often map out and report. Until now, doing that on Pentagon sites carried the considerable legal risk of running afoul of the Computer Fraud and Abuse Act.

"Hack the Pentagon" kicked off in April with a monthlong trial program that attracted 1,400 so- called white hackers to fiddle with Department of Defense websites on the hunt for weak points that could be exploited to steal data or jam systems. Those hackers spotted 138 weaknesses, according to the Pentagon, and were paid $75,000 in rewards.

Encouraged by the results, the Defense Department last week announced a formal policy permitting outside computer experts to test for vulnerabilities in the system and report them to the department. Secretary of Defense Ashton Carter called the initiative "a 'see something, say something' policy for the digital domain." Those hackers won't be paid for their reports, but officials hope they will do it out of a sense of duty.

In addition, the department has started "Hack the Army," a program asking hackers who have been approved by the government to test the Army's recruiting websites for weaknesses.

While these efforts represent just one aspect of the federal government's effort to protect secret data more rigorously, Mr. Carter deserves credit for championing an unconventional approach.

"Hack the Pentagon" and "Hack the Army" allows defense officials to draw from a talent pool that includes people who would not ordinarily feel at home in the military's hierarchical culture. It may well turn into an unconventional recruitment pipeline for an organization that always benefits from outside perspectives and carefully calibrated disruption.

Washington Free Beacon
Twitter Grants Verification to Muslim Brotherhood's Violent, Anti-Semitic Online Mouthpiece
Monday, 28 November 2016
Byline: Adam Kredo

Washington - The social media website Twitter is facing criticism for its recent decision to grant verification to the Muslim Brotherhood's official mouthpiece, which routinely writes in favor of violent terror acts and disseminates anti-Semitic propaganda.
The Muslim Brotherhood-which has been designated as a terror outfit and banned by Egypt, Saudi Arabia, Russia, and elsewhere-operates in the online sphere via a website known as Ikhwan Web, which serves as the Brotherhood's "official" English-speaking feed.

Twitter recently granted verification to Ikhwan Web's online feed, giving the organization an air of legitimacy that leading lawmakers and experts described as reckless given the Brotherhood's history of supporting violent jihad and terrorism.

"Verifying the Muslim Brotherhood's Twitter feed helps further their narrative of civilization-Jihad," Sen. Ted Cruz (R., Texas), a Muslim Brotherhood critic who has authorized legislation to designate it in the United States as a terror organization, told the Washington Free Beacon.

"This maneuver makes the Brotherhood seem like a legitimate group while providing them cover to spread their radical version of Islam," Cruz added. "I look forward to working with the new administration to expose the Brotherhood's efforts to increase their influence in America."

Ikhwan Web's Twitter feed serves as a central hub for the Brotherhood's radical propaganda and official statements. A Free Beacon request for comment to Twitter's public relations department went unanswered.

Twitter has faced a wave of criticism for failing to shut down various accounts promoting radical jihad and terrorism against Western countries. Others have criticized the social media site for cracking down on accounts associated with conservative-leaning thinkers and writers.

Recent tweets indicate that the Brotherhood is, via its Twitter feed, advocating continued violence and resistance against Egypt's ruling government. It also is working to mainstream the Brotherhood as a legitimate resistance organization and governing body.

Ikhwan Web has a history of promoting violence in the Middle East, primarily in Egypt, where the Brotherhood led a bloody coup and continues to support violence against the country's ruling authority.

"It is incumbent upon everyone to be aware that we are in the process of a new phase, where we summon what is latent in our strength, where we recall the meanings of jihad and prepare ourselves, our wives, our sons, our daughters, and whoever marched on our path to a long, uncompromising jihad, and during this stage we ask for martyrdom," the Brotherhood said in a 2015 statement that was posted on Ikhwan Web.

The website also has a history of defending individuals accused of organizing terror attacks on U.S. soil.

Other recent articles posted by the group promote violence against the Israeli government and Jewish people, including one 2009 post quoting a Muslim Brotherhood leader as calling for "jihad" to "liberate" Jerusalem from Israeli control.

The Brotherhood falsely claims that Israel is attempting to vandalize Muslim holy sites and prevent access for adherents to the faith.

Other postings rally against "the ugly face" of Zionism.

Kyle Shideler, director of the Center for Security Policy's Threat Information Office, told the Free Beacon that Twitter's decision to grant legitimacy to the organization is "deeply concerning."

"This decision by Twitter to provide the Muslim Brotherhood with this literal blue check of approval is deeply disconcerting," Shideler said.

"At a time when Twitter is already facing criticism for banning individuals based solely on speech, Twitter has effectively lionized a group responsible for the burning of Coptic churches and the killing of Egyptian police and judiciary officials," Shideler added. "How is Twitter supposed to help defeat online radicalization when it essentially endorses the biggest source for Islamist radicals in the world?"

Wall Street Journal
For China's Huawei, Hurdles Loom As It Plans U.S. Smartphone Sales

Monday, 28 November 2016
Byline: Juro Osawa, Ryan Knutson i

Hong Kong - A Chinese technology giant, whose telecom-networking equipment is shut out of the U.S. because of security concerns, is taking its high-end smartphone to American consumers for the first time.
But a number of obstacles are blocking Huawei Technologies Co.'s path to success in the U.S. smartphone market.

U.S. carriers, which distribute more than 80% of handsets in the country, are reluctant to work with Huawei -- the world's third-largest smartphone maker by shipments behind Samsung Electronics Co. and Apple Inc. -- because of its low brand recognition and security concerns associated with its networking equipment, people familiar with the matter say. A 2012 congressional report recommended that U.S. carriers avoid using Huawei gear in their networks for fear that China might use it to spy on Americans.

Huawei has denied such accusations, saying it operates independently of Beijing.

There are also technical hurdles related to cellular standards that would make U.S. expansion costly for the Chinese company.

"We haven't figured out how to remove those obstacles," said a Huawei manager based in the U.S. "It's very challenging."

Huawei said this month that it would launch its high-end Mate 9 smartphone in the U.S. But the phone, which carries a 699 euro ($740) price tag in Europe, will likely be sold just through online retailers such as Amazon.com Inc., people familiar with the matter said. Huawei hasn't disclosed the price or exact release date in the U.S.

The U.S. is the biggest missing piece in Huawei's smartphone global expansion strategy. The company, founded by former People's Liberation Army engineer Ren Zhengfei three decades ago, has become a major force thanks to its growth in China -- the world's biggest smartphone market -- as well as Europe, the Middle East, Africa and Latin America. In the U.S., where it sells inexpensive models, it had a market share of just 0.4% in the third quarter, according to research firm Canalys. Apple was the U.S. market leader with 39%, followed by Samsung with 23%.

The U.S. is the world's largest market for high-end phones priced above $500, according to Canalys. Cracking that market would help Huawei in its mission to overtake Apple and Samsung within five years as the world's top smartphone maker.

"It takes time to build trust in the U.S.," Richard Yu, head of Huawei's smartphone business who has set that ambitious goal, said in an interview this month.

But there are technical challenges. To comply with the cellular standard used by Verizon Communications Inc. and Sprint Corp., Huawei would have to make substantial and costly changes to its mobile chips. Verizon and Sprint also see little upside in adding Huawei devices to their already crowded lineup of phones, given Washington's wariness toward the Chinese company, people familiar with the matter said.

Huawei is also in a patent dispute with T-Mobile US Inc., making collaborations between the two unlikely.

While Huawei is more hopeful about the possibility of working with AT&T Inc., one of the country's two biggest carriers along with Verizon, and has communicated with the telecom giant, it is unclear whether they can agree on a partnership, according to the U.S.- based Huawei manager.

AT&T and T-Mobile declined to comment.

Until now, Huawei has largely ignored the U.S. as it concentrated on more welcoming markets. In Western Europe, the Chinese company has spent heavily on advertising, working closely with local retailers and sponsored professional soccer teams. As a result, its market share there more than doubled to 13% in the third quarter from 6% a year earlier, according to research firm IDC.

Canberra Times
Security Headquarters plagued with clearance problems Cyber spooks quit ASIO
Sunday, 27 November 2016
Byline: Stephen Jeffery

Canberra - Australia's premier cyber security agency has released plans to leave ASIO's headquarters for larger, lower security premises, two years since it first moved into the custom-designed building. The hurdles to gaining clearance to work in or visit the Australian Cyber Security Centre (ACSC) in the classified Ben Chifley Building in Parkes hindered the organisation's recruitment and collaborative goals, a Department of Defence submission to the parliamentary committee evaluating the proposal said. The department proposed a $38.8 million relocation and fitout of the ACSC to Defence-leased buildings at Brindabella Business Park near Canberra Airport. If approved, the centre's new headquarters would incorporate multiple security clearance levels, a mix of classified, unclassified and public meeting rooms, and space for a major expansion of its workforce to about 650, flagged in this year's Cyber Security Strategy.
The centre, currently made up of about 260 cyber security specialists from the Australian Signals Directorate, the Attorney- General's Department, ASIO, the Australian Federal Police and the Australian Crime Commission, began operating on November 27, 2014, and was the first tenant to move into the Ben Chifley Building. But the Defence submission said the classified nature of the building had impeded the centre's ability to collaborate with businesses and researchers, a core element of the Cyber Security

Strategy. The need to be approved for high security clearance, which can take more than two years, was dissuading skilled workers from joining the ACSC, the submission said.

The strategy, released in April, stipulates that "organisations need easy and consistent interfaces with government agencies on cyber security" and mandated that the centre move to a new location. "The need for private industry partners to obtain security clearances - and even the overheads associated with organising visitor entry for short-term visits - currently make achievement of the government's intent considerably more difficult," the submission said. "Cyber security skills are in short supply and high demand ... very few people with the requisite skills will be prepared to wait for a role with ASD, particularly when private industry is able to offer very attractive remuneration."

The building has had a chequered history, including delayed construction, reported security breaches and a $200 million budget blowout. Most of ASIO's estimated 1800 staff had moved into the $700 million building by 2015, two years behind schedule. Smashed glass panels and malfunctioning alarms made unwanted headlines last year. Most of the work of the Australian Signals Directorate with the ACSC could be handled in a lower security environment, the Defence submission said, with its classified status seen as more of a "legacy".

It pointed to Britain's National Cyber Security Centre, which is being built in London as a mostly unclassified facility, as a comparison. Depending on when it is approved, the ACSC's new headquarters could be completed by the end of 2017, with initial workers moving into the building from June. The Parliamentary Standing Committee will accept submissions on the proposal until January 13, with public hearings expected to take place later in the new year.

Le Figaro
Des écouteurs audio qui jouent les espions
Monday, 28 November 2016
Byline: Didier Sanz

Jérusalem - Des chercheurs israéliens ont montré qu'il était possible de transformer les oreillettes en microphones et d'enregistrer les discussions dans un rayon de six mètres.
On savait que les pirates pouvaient activer à distance la webcam d'un ordinateur pour filmer son propriétaire et son environnement. Ce sont maintenant des écouteurs audio dont il faudra se méfier. Des chercheurs du centre de recherche en cybersécurité de l'université Ben Gourion ont, en effet, démontré que ces accessoires pouvaient être transformés en microphones, par une astuce de programmation, et enregistrer toutes les conversations alentour, même si la victime a pris la précaution de désactiver le microphone de son mobile ou qu'elle ne possède pas de microphone sur ses écouteurs. Ils ont ainsi développé un logiciel, baptisé « Speak(a)r » , qui agit comme un programme espion, détournant les caractéristiques du système audio.

À première vue, le principe n'est pas nouveau. Il est tout à fait possible de brancher des écouteurs sur une entrée audio pour s'en servir comme microphone, comme l'expliquent de nombreux forums sur Internet et comme le montrent plusieurs vidéos sur YouTube. La fine membrane des écouteurs, qui transforme habituellement les signaux électromagnétiques en ondes sonores, devient alors un capteur de vibrations, lesquelles seront ensuite converties sous forme de signal électrique.

De l'ordinateur au smartphone

Mais la grande originalité de ce logiciel est qu'il exploite la sortie audio ! Il s'attaque directement aux composants pour reprogrammer la sortie audio en entrée audio. Les écouteurs se comportent alors comme de véritables microphones, capables d'enregistrer à la fois les sons de proximité et les discussions dans un rayon de 6 mètres. Comme un logiciel espion, le programme des universitaires peut compresser les enregistrements et transmettre le fichier correspondant sur Internet. Pour illustrer leur trouvaille, les chercheurs ont déconnecté le microphone d'un PC, dans un bureau, ne laissant que les écouteurs branchés sur la sortie audio. Puis ils ont diffusé un clip vidéo sur un téléviseur et lancé leur logiciel. Le graphique affiché par l'ordinateur montre alors que la musique et les paroles sont directement enregistrées par les écouteurs, et que le résultat pourra être écouté clairement sur des haut-parleurs.

Pour l'instant, les essais n'ont porté que sur des ordinateurs équipés de circuits audio Realtek, qui sont les plus répandus. Mais la technique serait identique dans le cas des smartphones : il suffit d'étudier quels composants sont utilisés et la manière de les programmer pour obtenir le même résultat. Coller un ruban adhésif sur sa webcam comme le fait le PDG de Facebook, Mark Zuckerberg, enfermer son mobile dans un réfrigérateur comme le conseille Edward Snowden ou encore désactiver le microphone des appareils électroniques ne suffira plus... Il faudra désormais penser à débrancher systématiquement les écouteurs...

Associated Press
U.K. spy bill brings 'dark, dark days'
Sunday, 27 November 2016

London - In Britain, Big Brother just got bigger.
After months of wrangling, parliament has passed a contentious new snooping law that gives authorities - from police and spies to food regulators, fire officials and tax inspectors - powers to look at the Internet browsing records of everyone in the country.

The law requires telecoms companies to keep records of all users' web activity for a year, creating databases of personal information that the firms worry could be vulnerable to leaks and hackers.

Civil liberties groups say the law establishes mass surveillance of British citizens, following innocent Internet users from the office to the living room and the bedroom.

Tim Berners-Lee, the computer scientist credited with inventing the web, tweeted news of the law's passage with the words: "Dark, dark days."

The Investigatory Powers Bill - dubbed the "snoopers' charter" by critics - was passed this month after more than a year of debate and amendments. It will become law when it receives the formality of royal assent next week.

But big questions remain about how it will work and the government acknowledges it could be 12 months before Internet firms have to start storing the records.

"It won't happen in a big bang next week," Home Office official Chris Mills told a meeting of Internet service providers on Thursday. "It will be a phased program of the introduction of the measures over a year or so."

The government says the new law "ensures powers are fit for the digital age," replacing a patchwork of often outdated rules and giving law-enforcement agencies the tools to fight terrorism and serious crime.

In a move taken by few other nations, it requires telecommunications companies to store for a year the web histories known as Internet connection records - a list of websites each person has visited and the apps and messaging services they used, though not the individual pages they looked at or the messages they sent.

Julian Huppert, a former Liberal Democrat lawmaker who opposed the bill, said it "creates a very intrusive database."

"People may have been to the Depression Alliance website, or a marriage guidance website, or an abortion provider's website, or all sorts of things which are very personal and private," he said.

Officials won't need a warrant to access the data, and the list of bodies that can see it includes not just the police and intelligence services, but government departments, revenue and customs officials and even the Food Standards Agency.

"My worry is partly about their access," Huppert said. "But it's much more deeply about the prospects for either hacking or people selling information on."

James Blessing, chairman of the Internet Services Providers Association, said the industry has "significant questions" on how the law will work - including "how to keep the vast new data sets secure."

Bangkok Post

Internet control eyed

Tuesday, 29 November 2016

Byline: Aekarach Sattaburuth

Section: general

Bangkok - The National Reform Steering Assembly (NRSA) panel on media reforms has proposed that military and police officers handle both policy and operation in ensuring cyber security.
The proposal is included in the panel's report for a study conducted on a cyber security bill, presented at an NRSA meeting on Monday. The report was approved by the NRSA in a 141-1 vote with five abstentions.

Pol Maj Gen Phisit Pao-in, deputy chief of the panel, insisted the bill needs more details to be comprehensive. He said the cyber-security framework must be underlined, and it has to be consistent with strategic plans adopted by all security agencies.

A key agency must be identified to take care of cyber security situations in both normal and emergency situations, he said.

Military and police officers must play a role both in advocating policies and carrying out ground operations in dealing with the cyber security problems, Pol Maj Gen Phisit said.

After the new constitution is put into force, the prime minister should use his power under Section 265 of the charter to set up a national committee to maintain cyber security for a specific period of time before the bill is enacted, he said.

The approach is needed because it could take time for the bill to be approved by the National Legislative Assembly (NLA) and come into force, during which damage could arise to the country's security and the government's policy on the digital economy.

However, Kamnoon Sidhisamarn, an NRSA member, expressed concerns about empowering officials to deal with cyber security. "Would it be necessary for the officials to regulate the private sector in the whole process?" Mr Kamnoon asked. Details should be drawn up on how much the authorities can regulate and operate.

He also insisted a national committee on maintaining cyber security lacks the participation of public and private sectors.

Another NRSA member, Sompong Sakawee, said he was worried that the bill might affect the businesses of Line, Facebook, Instagram and Twitter and drive them away.

Pol Maj Gen Phisit insisted the bill is aimed at shielding the internet system from cyber attacks. He said the websites of Thai state agencies come under cyber attack every day, causing damage worth hundreds of millions of baht.

Under the bill, there will be a central standard measure set for each agency to adopt in protecting their computer systems, he added.

The NRSA also suggested stepped-up measures to boost military security and approaches to educate the public about cyber security laws.

The Australian

Professionalism key to tackling cyberthreats

Tuesday, 29 November 2016

Byline: Anthony Wong

Section: oped

"Speed is the essence of war. Take advantage of the enemy's unpreparedness; travel by unexpected routes and strike him where he has taken no precautions." So wrote Chinese military strategist Sun Tzu in his classic, The Art of War.
I was recently in China, in a region where Sun Tzu lived around 500BC. Despite the time difference, Sun Tzu's insights are highly applicable to modern warfare, which experts predict will increasingly be fought in cyberspace, using technology to block communications and cripple infrastructure.

The importance of cybersecurity precautions cannot be overstated, which is why the Australian Computer Society will tomorrow release our new guide, entitled Cybersecurity: Threats, Challenges, Opportunities. It seeks to raise awareness of cyberthreats, which can affect everyone from an individual with a smartphone through to business and enterprise, and even our entire nation.

At the Australia-US Cyber Security Dialogue in September, Prime Minister Turnbull said: "For each large enterprise, there are many small businesses putting a toe in the water of the online world. They are connected to you as suppliers, distributors and contractors. Many are far less secure, far less savvy, far less resourced than governments and big business. Or at least, than governments and big businesses should be." The ACS has long played an active role in raising awareness of cyberthreats, supporting the government with expert advice back in 2011 and providing a co-ordinating role for an industry response. At the time, we used this column to challenge the government to "establish a central authority to co-ordinate both the policy development and operational aspects of Australia's cybersecurity framework to ensure an integrated and congruent approach to any cyber-related initiatives".

That call was answered with the formation in 2013 of the Australian Cyber Security Centre, an umbrella body which brings together the cyber security activities of the key security-related agencies: the Australian Signals Directorate, Defence Intelligence Organisation, Australian Security Intelligence Organisation, Computer Emergency Response Team Australia, Australian Criminal Intelligence Commission and the Australian Federal Police.

We also welcome this month's appointment of Dr Tobias Feakin as Australia's inaugural Ambassador for Cyber Affairs to work closely with Dan Tehan, the Minister Assisting the Prime Minister for Cyber Security and Alastair MacGibbon, Special Adviser to the Prime Minister on Cyber Security, in providing leadership and advocacy on cyber security policy and strategy.

In October this year, the ACSC released its 2nd Threat Report, highlighting the severity and breadth of cyber intrusions in the 2016 financial year.

Between July 2015 and June 2016, CERT Australia responded to 14,804 cybersecurity incidents affecting Australian businesses, 418 involving systems of national interest and critical infrastructure. At the same time, the ASD responded to 1095 cybersecurity incidents in government systems that were serious enough to warrant operational responses.

We are seeing significant growth and convergence of technologies including big data, the Internet of Things, mobility, cloud computing, artificial intelligence, robotics and more. As technology continues to innovate, enhance, challenge and disrupt our world in new and different ways, cybersecurity will only grow in importance.

In May, Leon Strous, president of IFIP, the global body established in 1960 under UNESCO and of which the ACS is a member, took part in the strategic European Foresight Cyber Security Meeting. He highlighted the critical role that professionalism plays in building trustworthy, reliable and secure ICT systems.

Tomorrow, the ACS plays host to a ministers forum in Sydney where the Victorian Minister for Small Business, Innovation and Trade, Philip Dalidakis, will lead a panel of international cybersecurity experts

to explore "global approaches to building resilience, the cybersecurity ecosystem and staying on top of old and new threats".

The panellists include Elly van den Heuval, secretary to the Dutch Cyber Security Council, which is calling for the harmonisation of legal frameworks and duties of care to enable a consistent and reliable approach to cybersecurity and IoT, and to address issues of professionalism and standards.

As part of our commitment to security professionalism, the ACS supported Tehan at his inaugural address, A Cyber Storm at the National Press Club in Canberra last week.

Anthony Wong is ACS president and CEO of AGW Consulting, a multidisciplinary ICT, intellectual property legal and consulting practice.

China Daily

Crackdown targets cyber black market

Tuesday, 29 November 2016

Byline: Cao Yin

Section: general

Beijing -China has experienced an increase in cases of online data leaks in the past few years due to the development of the "cyber black market", according to a report by the Shanghai Academy of Social Sciences' Institute of Information.
The Annual Report on Development of Cyberspace Security in China, which the institute released on Monday, says that cases relating to information leaks have become more frequent since last year, such as the high-profile case involving Gfan - the country's largest online platform for Android systems - in which data of the platform's more than 23 million users, including their names, passwords and email addresses, were published on the internet.

It said that economic losses from June last year to June this year resulting from text message spam, online scams and information leaks totaled 91.5 billion yuan ($13.3 billion).

Such losses were attributed to the cyber black market, a commercial chain where participants such as hackers and network operators gain profits illegally, it said, adding that the industry is a growing multi-billion-US dollar economy.

"In the past, hackers conducted cyberattacks for fun, or to show off their hacking skills, but now they operate as businesses, gaining money through utilizing their techniques, such as stealing personal information and selling it," said Zhang Huaping, an associate professor specializing in cybersecurity at Beijing Institute of Technology.

"Cybersecurity issues used to relate to the actions of individuals, but in recent years, hackers have started making deals with network businessmen, earning a percentage of the profits," Zhang said.

On Thursday, a report on cybersecurity by Chinese internet giant Tencent said that online social platforms with an abundance of personal information have become the most popular space for those working on the cyber black market to gain illicit profits.

It estimated that at least 560,000 people engaged in the industry in the first six months this year, involving more than 148.2 billion yuan.

Qihoo 360, China's largest security software provider, said in November last year that at least 1.6 million people are engaged in the cyber fraud, with their annual output value surpassing 110 billion yuan.

Pei Zhiyong, a cybersecurity specialist at Qihoo 360, said: "A simple fraud operation needs a team of at least 10 people, while a fraud chain has more than 15 links. The work of each participant is clear. Some take charge of sending text message scams, while others are responsible for designing fraud programs, for example."

Experts said sometimes such fraud results is more than just financial losses.

In August, Xu Yuyu, an 18-year-old from Linyi, Shandong province, died of a heart attack after losing 9,900 yuan ($1,500) in a phone scam. The money had been saved to cover her college tuition fees.

Peng Yang, a professor specializing in big data and information security at Beijing University of Posts and Telecommunications, said that the cyber black market has disturbed normal market order as well as network competition.

"The fight against the cyber black market is not hard, as we can trace how data is released online," Peng said. "The problem is that there are no laws defining the industry as illegal."

Experts said the most effective way of addressing the problem is to pass legislation on protecting information and clarify governmental departments' obligations on law enforcement and supervision.

Kyodo News

Data breach from reported cyberattack not found: defense chief

Tuesday, 29 November 2016

Byline: Staff reporter

Section: general

Tokyo - Defense Minister Tomomi Inada said Tuesday a recently reported cyberattack was not found to have resulted in a data breach, but did not confirm media reports that a ministry communication network shared with the Self-Defense Forces was hacked.
Noting that the ministry and the SDF receive suspicious e-mails on a daily basis, Inada said at a press conference, "We have not confirmed any leakage of information or destruction of equipment at this point."

Kyodo News reported Sunday that the ministry and the SDF discovered around September that their shared communication network had suffered a cyberattack that enabled a hacker to penetrate the Ground Self-Defense Force's computer system, and that some information may have been leaked in the incident.

According to ministry sources, the Defense Information Infrastructure, a high-speed large-capacity communication network connecting SDF bases and camps, was subjected to the attack. The sources suspect the involvement of a state-backed attacker.

The infrastructure consists of a system connected to the Internet and another that is used for information sharing by people inside the organizations, but the two systems are not completely detached.

Inada declined to comment on specific cases, saying that doing so could reveal the country's response to cybersecurity issues. But she said the ministry is dealing with cyberattacks through such mechanisms as its Cyber Defense Group which monitors communication networks around the clock.

New York Times

Hate Speech Laws Test Facebook

Tuesday, 29 November 2016

Byline: Mark Scott, Melissa Eddy

Section: general

Berlin - Yorai Feinberg was going about his daily routine this month when his social media feeds and cellphone began lighting up.
It was the 78th anniversary of the Kristallnacht, the 1938 Nazi pogrom against Jews, and the Berlin restaurant owned by Mr. Feinberg, a 35-year-old Israeli, had been included without his knowledge on a map of the city that a far-right group had published on Facebook.

The social media post listed the names -- and addresses -- of local Jewish institutions and Israeli-owned businesses under the banner "Jews Among Us," in bright yellow Gothic script. Mr. Feinberg soon received anonymous phone calls telling him, "I hate Jews."

A standoff quickly developed between Facebook, the social media giant, and German authorities over what many here said was its inadequate response to the publication of the map. But Germany's rules on what may be said or published -- among the world's toughest, with long prison terms for denying the Holocaust and inciting hatred against minorities -- ensured that the post was eventually deleted.

The incident is one of several examples -- including threats of regulation and attempts to prosecute Facebook's chief executive, Mark Zuckerberg -- of how Germany has become an important test case globally for how the social network polices what may be published online, and how it should respond to inappropriate and illegal content.

Such steps in Germany are part of a growing push around the world to regulate what users are allowed to post online.

Mr. Feinberg did not report the incident to Facebook, convinced after previous anti-Semitic attacks that the social network would not act, he said.

"I have reported things to Facebook at least 20 times," he explained over coffee at his restaurant in a residential neighborhood in western Berlin. "And 100 percent of the time, they have refused to take it down. Facebook doesn't do anything."

Others identified in the map did complain. At first, Facebook did not remove the map, saying it complied with the company's "community standards," or guidelines for what it deems within the bounds of free speech.

But within 48 hours, after an outcry on social media, in local newspapers and from German lawmakers, Facebook relented. It deleted the far- right group's entire page, including the post that had listed the Jewish institutions and businesses across Berlin.

"We recognize that this is a work in progress," Richard Allen, Facebook's director of policy in Europe, said in an interview. "It was hate speech, and it should have been taken down."

In Germany, more than almost anywhere else in the West, lawmakers, including Chancellor Angela Merkel, are demanding that Facebook go further to police what is said on the social network -- a platform that now has 1.8 billion users worldwide. The country's lawmakers also want other American tech giants to meet similar standards.

The often-heated dispute has raised concerns over maintaining freedom of speech while protecting vulnerable minorities in a country where the legacy of World War II and decades under Communism still resonate.

It is occurring amid mounting criticism of Facebook in the United States after fake news reports were shared widely on the site before the presidential election. Facebook also has been accused of allowing similar false reports to spread during elections elsewhere.

Mr. Zuckerberg has denied that such reports swayed American voters. But lawmakers in the United States, Germany and beyond are pressing Facebook to clamp down on hate speech, fake news and other misinformation shared online, or face new laws, fines or other legal actions.

"Facebook has a certain responsibility to uphold the laws," said Heiko Maas, the German justice minister. In October, Mr. Maas suggested the company could be held criminally liable for users' illegal hate speech postings if it does not swiftly remove them.

Facebook rejects claims that it has not responded to the rise in hate speech in Germany and elsewhere, saying it continually updates its community standards to weed out inappropriate posts and comments.

It says such material represents a small fraction of the millions of posts daily, and argues there is a fine balance between protecting freedom of expression and stamping out internet hate speech.

"We've done more than any other service at trying to get on top of hate speech on our platform," Mr. Allen said.

Tussles with German lawmakers are nothing new for Facebook.

It has routinely run afoul of the country's strict privacy rules. In September, a local regulator blocked WhatsApp, the internet messaging service owned by Facebook, from sharing data from users in Germany with its parent company. The country's officials also have questioned whether Facebook's control of users' digital information could breach antitrust rules, accusations the company denies.

Facebook's problems with hate speech posts in Germany began in summer 2015 as more than one million refugees began to enter the country.

Their arrival, according to company executives and lawmakers, incited an online backlash from Germans opposed to the swell of people from Syria, Afghanistan and other war-torn countries. The number of hateful posts on Facebook increased sharply.

As such content spread quickly online, senior German politicians appealed directly to Facebook to comply with the country's laws. Even Ms. Merkel confronted Mr. Zuckerberg in New York in September 2015 about the issue.

In response, Facebook updated its global community standards, which also apply in the United States, to give greater protection to minority groups, primarily to calm German concerns.

Facebook also agreed to work with the government, local charities and other companies to fight online hate speech, and recently started a billboard and television campaign in Germany to answer local fears over how it deals with hate speech and privacy.

Facebook hired a tech company based in Berlin to monitor and delete illegal content, including hate speech, from Germany and elsewhere, working with Facebook's monitoring staff in Dublin.

"They have gotten better and quicker at handling hate speech," said Martin Drechsler, managing director of FSM, a nonprofit group that has worked with Facebook on the issue.

Despite these steps, German officials are demanding further action.

Ms. Merkel, who is seeking a fourth term in general elections next year, warned lawmakers last week that hate speech and fake news sites were influencing public opinion, raising the possibility of new regulations.

And Mr. Maas, the justice minister, has repeatedly warned that he will propose legislation if Facebook cannot remove at least 70 percent of online hate speech within 24 hours by early next year. It now removes less than 50 percent, according to a study published in September by a group that monitors hate speech, a proportion that is still significantly higher than those for Twitter and YouTube, the report found.

For Chan-Jo Jun, a lawyer in Würzburg, an hour's drive from Frankfurt, new laws governing Facebook cannot come soon enough.

Mr. Jun recently filed a complaint with Munich authorities, seeking prosecution of Mr. Zuckerberg and other senior Facebook executives on charges they failed to sufficiently tackle the widespread wave of hate speech in Germany. The company denies the accusations.

While his complaint may be dismissed, Mr. Jun says the roughly 450 hate speech cases that he has collected, more than half of them aimed at refugees, show that Facebook is not complying with German law. Despite its global size, he insists, the company cannot skirt its local responsibilities.

"I know Facebook wants to be seen as a global giant," Mr. Jun said. "But there's no way around it. They have to comply with German law."

Jerusalem Post

How hackers tried to 'poison' Syria's Assad

Tuesday, 29 November 2016

Byline: Yasser Okbi, Maariv Hashavua

Section: general

Jerusalem - Rumors of Syrian President Bashar Assad's demise spread quickly throughout the social media landscape Monday after the country's Ministry of Information became the target of a cyber attack.
"There was an attempt to poison his Excellency Bashar Assad. He was infected by a contagious, dangerous disease and is in grave condition," read a message apparently posted by hackers on the ministry's homepage for several hours. "Doctors are at the president's side and are trying to save his life."

News of the dictator's alleged ill health spread shortly after the posting, causing confusion among the government and military along with the social media sphere.

Locked out of the ministry's system for several hours, government employees turned to Facebook to deny there was an attack against Assad and update viewers on his actual, living condition.

"The announcement that President Assad was poisoned is false and has no basis," the social media post read, adding "the news was planted by a hacker."

The Jerusalem Post's sister publication Ma'ariv noted that as of Monday the message announcing Assad's poisoning had yet to be removed from the Syrian ministry's website.

It was not clear whether this was due to technical reasons or an attempt by authorities to locate the parties responsible.

The Guardian (London)

Julian Assange: Ecuador says no 'quick way out' of embassy impasse

Tuesday, 29 November 2016

Byline: Staff report

Section: general

Quito - The WikiLeaks founder Julian Assange has no "quick way out" of the Ecuadorean embassy in London where he took refuge more than four years ago, Ecuador's prosecutor has said.
An Ecuadorean state attorney accompanied by a Swedish prosecutor questioned Assange at the embassy on 14 November over allegations that he committed rape in Sweden in 2010.

Ecuador's prosecutor, Galo Chiriboga, said Ecuadorean officials would send the official transcript of Assange's evidence to Swedish authorities "in mid-December".

Assange, who is Australian, has said he fears deportation to Sweden and the United States, where he could be charged for the publication of hundreds of thousands of secret US diplomatic cables.

"Four years have passed and we are only at this stage, but that is no longer attributable to Ecuador, it is attributable to Swedish prosecutors. I do not think there is a quick way out," Chiriboga said.

Assange, who has denied the rape charges, is also wanted by British authorities for violating the conditions of his house arrest, which he fled to seek refuge at the embassy.

Ecuador's foreign minister, Guillaume Long, has said Assange should receive guarantees that he will not be extradited if he faces justice in Sweden.

A DNA sample had been taken by British police from Assange at the embassy for Swedish prosecutors to use in their investigation against him, Chiriboga said.

"Therefore Sweden will now have to request that DNA sample from the British police," the prosecutor said.

Washington Free Beacon

Pentagon Links Chinese Cyber Security Firm to Beijing Spy Service

Tuesday, 29 November 2016

Byline: Bill Gertz

Section: general

Washington - A Chinese cyber security firm is covertly working with Beijing's Ministry of State Security intelligence service in conducting cyber espionage operations, according to Pentagon intelligence officials.
The company known as Boyusec, officially the Bo Yu Guangzhou Information Technology Co., is also working with China's global telecommunications company Huawei Technologies, which has been identified by U.S. intelligence agencies as linked to the Chinese military.

According to an internal report by the Pentagon's Joint Staff J-2 intelligence directorate, Boyusec and Huawei are working together to produce security products that will be loaded into Chinese-manufactured computer and telephone equipment. The doctored products will allow Chinese intelligence to capture data and control computer and telecommunications equipment, said Pentagon officials familiar with the report.

"It's closely connected to the [Ministry of State Security] and Huawei and they are developing a start-up program that will use malware allowing for capturing and controlling devices," said one official of Boyusec.

No other details of Boyusec's activities could be learned.

The employment of a cyber security firm as cover for intelligence gathering has been used in the past by Russian intelligence. China appears to be following the same pattern, analysts say.

The Defense Intelligence Agency reported last spring that Russia's Kaspersky Labs was marketing security software for industrial control networks that the agency warned could create cyber vulnerabilities.

Government cyber actors from both China and Russia have been detected mapping American critical infrastructure networks, including the U.S. electrical grid.

Boysec's website reveals that the company is based in Guangzhou, China, and is a "cooperative partner" with Huawei, along with the Guangdong Provincial Information Security Assessment Center, a government bureau that conducts security assessments of software.

Guangzhou is a Chinese city located inland from Hong Kong in Guangdong province.

Boyusec did not respond to emails seeking comment.

A Joint Staff spokesman had no immediate comment.

Disclosure of Chinese security firm's links to the Ministry of State Security followed a report in the New York Times earlier this month that China had pre-installed software on some Android phones that covertly provided a backdoor to supply data from the devices to China every three days.

Security researchers at Kryptowire discovered that the secret reporting software was produced by a company called the Shanghai Adups Technology Co. and was found on more than 700 million phones, cars, and other smart devices.

The software is used on phones made by Huawei and another major Chinese telecommunications firm, ZTE.

Huawei was identified in a 2009 Pentagon report on China's military as one of several Chinese information technology companies that maintains "close ties to the [People's Liberation Army] and collaborates on R&D."

A report by the CIA-based Open Source Center in 2011 revealed that Huawei's chairwoman, Sun Yafang, worked at the Ministry of State Security's communications department before joining the company.

The report stated that Sun used her ties to the intelligence service to help Huawei fight off unspecified financial difficulties after the company was founded in 1987.

National Security Agency documents made public by former contractor Edward Snowden revealed that the agency had penetrated Huawei's communications networks and was spying on foreign countries' communications through Huawei equipment in Iran, Afghanistan, Pakistan, Kenya, and Cuba.

The NSA also expressed concerns in one document that Huawei equipment could be used by China for cyber attacks.

"There is also concern that Huawei's widespread infrastructure will provide the PRC with SIGINT capabilities and enable them to perform denial of service type attacks," stated an NSA briefing slide labeled "Top Secret."

The NSA revealed that the Huawei cyber threat also was outlined in a National Intelligence Estimate, a major report approved by the 16 U.S. intelligence agencies.

The document was titled "The Global Cyber Threat to the U.S. Information Infrastructure" and warned: "We assess with high confidence that the increasing role of international companies and foreign individuals in U.S. information technology supply chains and services will increase the potential for persistent, stealthy subversions."

John Tkacik, a former State Department official, said the company appears from its website to pose a security risk.

"If I were at the Pentagon or Cybercom, I would keep my eyes on Boyusec, and only blow the whistle on them if they were actively marketing services to U.S. companies," Tkacik said.

"If the United States had a functional offensive cyber capability, and if I caught them in flagrante, I'd quietly blow up their servers with a ransomware attack and let them figure out what happened."

Tkacik said a Chinese cyber security company working with a Chinese intelligence service is a "dog-bites-man story."

"I want to hear U.S. cyber warriors strike back, a man-bites-dog story, although if man ever bites dog maybe it's best not to let the cyber- PETA hand wringers get wind of it in the press," he said.

A congressional China commission annual report made public this month stated that the Ministry of State Security is the main civilian spy service under the State Council, the chief administrative authority of the Chinese government and the ruling Communist Party's Politburo Standing Committee, the seven-member collective dictatorship that runs China.

"The [Ministry] conducts a variety of intelligence collection operations, such as human intelligence (HUMINT) and cyber operations," the report says.

Regarding cyber espionage, "China has a large, professionalized cyber espionage community," stated the report of the U.S.-China Economic and Security Review Commission.

"Chinese intelligence services have demonstrated broad capabilities to infiltrate a range of U.S. national security (as well as commercial) actors with cyber operations," the report said.

The Ministry of State Security, according to the commission, was behind the hacking of the Office of Personnel Management, the government's personnel records repository, and the theft of some 22 million records on federal workers, which included sensitive background investigation data.

According to the report, China is using cyber attacks to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs.

The cyber thefts may benefit China's defense industry and high-technology sector as well as provide the Communist Party of China with insights into U.S. leadership perspectives on key China issues.

"Additionally, targeted information could inform Chinese military planners' work to build a picture of U.S. defense networks, logistics, and related military capabilities that could be exploited during a crisis," the report says.

In addition to both civilian and military cyber espionage units, other unofficial Chinese hackers have conducted cyber espionage operations targeting the United States.

These include Chinese nationalist hackers and criminal cyber spies.

"Some observers suggest China is shifting cyber espionage missions away from unofficial actors to centralize and professionalize these operations within its intelligence services," the report said.

Boyusec states on its website that it provides information security services, consulting, and security evaluations.

Its testing services include static application security testing and dynamic network security testing, including simulate cyber attacks.

Last year, Boyusec joined with the Guangdong information security office to create a joint laboratory for testing software and developing cyber defenses.

CBC News
Cybersecurity talent shortage on the radar of government, business
Wednesday, 02 November 2016
Byline: Julie Ireton

An international shortage of cybersecurity talent is expected to grow over the next few years, according to the Information and Communications Technology Council.
The council's vice-president of talent innovation, Sandra Saric, said there's an expected need for more than 1.5 million people to work in cybersecurity globally by 2020.

Solving the talent shortage was one of the challenges emphasized by government and private industry executives at a cybersecurity forum at the GTEC conference in Ottawa on Tuesday. It's an annual technology event that brings together business and government.

"Getting more people to take science, technology, engineering and mathematics courses and degree programs, and also training them to be cybersecurity savvy is probably the first challenge," said Scott Jones, assistant deputy minister responsible for the information technology security program with Communications Security Establishment Canada (CSEC).

Starting early

Saric said there's a need for computer scientists, analysts, investigators and psychologists, as well as communications and marketing professionals.

"We connect with the Ottawa police who have a cybercrime unit, they're having difficulty finding people. I've spoken to the RCMP who are also struggling ... it's across the board," she said.

Saric said the Information and Communications Technology Council, a Canadian non-profit, is working on developing talented students before they have even graduated high school.

The council has created cybersecurity competitions at high schools across the country to get students to develop these unique skills.

"It's about youth, regardless of what career they enter, cybersecurity is a critical component of their learning and the knowledge they need," said Saric, who presented at the cybersecurity forum.

Health information area of concern

But Jeff Curtis, the chief privacy officer at Sunnybrook Health Science Centre in Toronto, said his hospital needs talent now, not years down the road.

"People need to hear what's going on in the trenches, I'm here to bring that perspective," said Curtis.

He said the hacking of private health information is becoming a bigger concern for hospitals and health-care providers in Canada, noting hospitals hold a lot of valuable personal data and everyone is counting on the health-care centres to keep information safe.

In March the Ottawa Hospital reported a cyberattack after four of the hospital's computers in a network of 9,800 devices faced a hacker attempt.

The hospital said malware locked down the files after someone using the computer clicked a link that activated it, but it said no patient information was compromised.

In a statement at the time, the hospital said it was confident the appropriate safeguards were in place to protect patient information, but it would "continue to look for ways to increase security."

"We're just starting to look for scaled operations and the people to fill those positions," said Curtis about Sunnybrook.

"We have to catch up fast, and it's hard to find folks who not only have the hard skills in security, but also know the [hospital] sector as well."

iPolitics.ca
New national security committee could study RCMP surveillance of reporters: Goodale
Wednesday, 02 November 2016
Byline: Amanda Connolly

Ottawa - Public Safety Minister Ralph Goodale suggested Tuesday that if reports emerged of RCMP keeping tabs on journalists for reasons linked to national security, the government's planned new national security committee could look into them.
Along with Government House Leader Bardish Chagger, Goodale took questions from members of the House of Commons public safety committee Tuesday evening. The questions largely focused on critics' concerns about the government's ability to appoint the chair of the all- party committee, ministers' ability to veto requests for information, and the prime minister's authority to review the committee's reports and ask for redactions.

However, controversial recent reports of police surveillance of La Presse journalist Patrick Lagacé's iPhone also came up. Goodale pointing out that Lagacé's case falls under Quebec's political jurisdiction, but if similar cases should come to light involving the Mounties and national security, the new committee could investigate them.

"There may well be concerns about that from members of this future committee ... and it may well be that the committee would say we need to look at that," Goodale said. "First and foremost, the committee needs to decide what's important."

During a pre-committee scrum with reporters, Goodale was asked about the Lagacé case and why he would not say if RCMP have made similar requests for warrants to conduct surveillance on journalists.

RCMP also refused to disclose that information when asked to report the number of times the force has sought a warrant to conduct surveillance on journalists over the past year.

"For security reasons, we cannot provide operation details of this nature," a force spokesperson said. "Cases of RCMP investigations relating to reporters are extremely rare, and when such cases occur, these are conducted under close monitoring parameters guided by ministerial directives. We recognize the importance of the freedom and independence of the press, and we respect it."

The issue of disclosure by national security agencies -- including the RCMP -- to the new committee dominated questions Tuesday evening.

C-22 allows for the committee to request information from any government agency working on national security -- a much broader mandate than similar committees in ally countries like the United Kingdom or Australia have.

However, it also allows for several controversial circumstances where disclosure can be refused -- most notably, the case of a ministerial veto in the event a department or agency can convince a minister certain information cannot be shared.

As well, C-22 also requires the committee to submit its reports to the prime minister prior to sharing them with Parliament and allows the prime minister to require redaction in cases where national security could be at risk.

Committee members pushed hard for explanations of those exemptions and asked if the government was open to amending or tightening the wording on exclusions.

"We're prepared to look seriously at all amendments and give them fair consideration," Goodale said.

The only issue the government appears unwilling to negotiate on at this time is that of having a government-appointed chair.

Goodale announced in January that Ottawa South MP David McGuinty will chair the committee of parliamentarians, and that has sparked outrage from opposition critics who say the role should be elected by committee members, as is the case with parliamentary committees.

The U.K. model currently allows for that, although it didn't always: That power came in a significant 2013 statutory review of the Intelligence and Security Committee's mandate.

Goodale said that issue specifically might be reserved for adjustment at the five-year review of the committee built into C- 22.

When pressed on the matter by NDP critic Matthew Dube, Chagger said there is no model for this specific committee anywhere in Canadian history and it won't be an exact match for the current U.K. model.

"We aren't the UK," Chagger said.

The committee will continue its study of the bill over the next several weeks before moving to clause-by-clause considerations, which will then be referred to the government.

iPolitics.ca
Goodale ducks question about journalists under surveillance
Wednesday, 02 November 2016

Public Safety Minister Ralph Goodale won't say how many Canadian journalists might be under police surveillance.
In question period today, NDP leader Tom Mulcair raised the case of Montreal journalist Patrick Lagacé -- who learned recently that police had been monitoring his phone calls and location through GPS in his cellphone as part of an internal police probe. At least 24 warrants were issued on Lagacé's phone.

"'It's disgusting', as one of my colleagues said," Mulcair told the Commons, also citing the case of La Presse journalist Joel-Denis Bellavance, who has been tailed by police. Mounties followed Bellavance for nine days in 2007 in an attempt to track down a leak of classified documents.

"Can the minister of public safety tell us whether other journalists are being spied upon either by the police, the RCMP or CSIS?" Mulcair asked Goodale.

Goodale skirted the question, saying only that the issue is "entirely in the jurisdiction of Quebec, and this morning the premier of Quebec has made a very import pronouncement in that regard.

"We all, I'm sure, in this House believe profoundly in the freedom of the press. It is a value that is enshrined in the Charter of Rights and Freedoms."

He said police forces need to be "assiduous" in following the Supreme Court judgement which laid out rules to be followed in respect to press freedom.

According to the Journal de Montréal, police also reportedly tried to track down sources used by journalists Félix Séguin, Monic Néron and Fabrice de Pierrebourg.

Mulcair was not satisfied with Goodale's response. He said freedom of the press is not something a government can just "claim to support."

He asked how Canadians can believe the government believes in press freedom when the minister refuses to say whether there any journalists are under surveillance.

Goodale said the Supreme Court has rules on this issue which are laid out explicitly.

"It is very clear that freedom of the press is something that matters to all Canadians and this government and I expect every member of this House to defend that freedom," he said.

Mulcair replied by saying that defending that freedom means defending journalists like Bellavance. "That minister did nothing."

Montreal Gazette
Curbing online extremism 'like trying to block wind'
Wednesday, 02 November 2016
Byline: Caroline Plante

Montreal - Pulling hate material from the Internet will never be enough to curb the phenomenon of violent extremism, the head of free expression and international relations at Google told a conference on radicalization Tuesday.
"What we've seen over the past couple of years is a realization that simply taking the content down doesn't work because one website goes down, two or three more are up the very next day," Ross LaJeunesse said.

"Simply taking down the content doesn't address the feeling and the hatred which caused the speech in the first place. You need to engage the speakers who are promoting radicalization and hate online."

He acknowledged that Google, the U.S.-based company that runs a search engine and the video-sharing service YouTube, has a role to play and argued the company is taking that responsibility very seriously.
"We have started doing various programs, where, much like a regular advertising campaign, when someone searches for a key word that we think indicates they're looking for radical content, we then show them an advertising campaign about content that counters that speech," LaJeunesse said.

Also, "we don't allow violent images on YouTube, we don't allow pornography, we've always built YouTube to be a community where everyone is going to feel comfortable participating and speaking and watching content that they like."

LaJeunesse added people must differentiate between YouTube, which Google controls, and the Internet, which the company doesn't control. Many people equate Google with all of the Internet, he said.

When young people search the Internet, they're asking questions and are usually not confirmed radicals, the conference heard on Tuesday. They're at a stage where you can reach them, engage them, and present them with authentic, alternative voices.

Arguing that "blocking the Internet is a bit like trying to block wind," panellists agreed that instead of focusing on censorship, societies should teach young people to navigate through the overload of information on the Internet and help them determine what is credible and what is bunk.

"Basically, you want the younger generation to question everything," said Anantha Kumar Duraiappah, director of the UNESCO Mahatma Gandhi Institute of Education for Peace and Sustainable Development (MGIEP).

Duraiappah insisted the most important skill to have in the 21st century is critical inquiry, "deconstructing an argument and then reconstructing it to see if you're comfortable with it, being able to say 'That's not right.' " He said he'd also like young people to "fire their Gandhi neurons," in other words, express compassion and empathy, and develop the moral courage to change. All of that has to be in school curricula, Duraiappah argued, because it is what will help teenagers build their identities and belief systems.

While not promising to change the curriculum in Quebec, Premier Philippe Couillard said it is important to maintain an "analysis culture."

"We're doing it. Are we doing it enough? That's another question to be resolved," he said.

Couillard announced $10,000 for a "No to hate" campaign that will travel across Quebec schools and youth clubs in the months to come.

Ottawa Citizen
A Canadian parallel to FBI versus Clinton
Wednesday, 02 November 2016
Byline: Andrew Cohen

In the last fortnight of the presidential election of 1960, the race between John F. Kennedy and Richard Nixon was very close. Kennedy won the televised debates, but had not closed the deal.
Kennedy learned that Dr. Martin Luther King, Jr., had been arrested on a technicality - a traffic charge - and was in jail. On Oct. 26, Kennedy called King's wife, Coretta, to show his sympathy and offer his help. His brother, Robert F. Kennedy, made a call of concern to the judge.

Surprisingly, King was released. African-Americans voted for Kennedy overwhelmingly. They may have been the difference in a race that Kennedy won by some 118,000 votes.

The point: when elections are close, anything can tip the balance. Four days after the FBI revelation that it is reinvestigating

Hillary Clinton's emails, polls show no clear impact, though the announcement has changed the tone of this race.

The conversation is about her, not Donald Trump, and that is bad for her. When he is under scrutiny - his refusal to pay income taxes, his treatment of women, his views on Russia, minorities and nuclear arms - he loses. Now he has a stick and he is beating her, with glee. It isn't over.

If you doubt how an unseen hand can reverse a race, ask these Canadians: Ralph Goodale, Paul Martin, Stephen Harper.

Just weeks before the federal election on Jan. 23, 2006, the Liberals were leading the Conservatives. On Dec. 23, the RCMP faxed a letter to the office of Judy Wasylycia-Leis, the NDP's finance critic. She had asked about potential insider trading on government policy involving Goodale, who was minister of finance.

The response from Giuliano Zaccardelli, then commissioner of the RCMP, said a criminal investigation had been opened. On Dec. 29, after the NDP belatedly discovered the fax and made it public, the RCMP said in a news release: "In particular, the RCMP wishes to note that at this time there is no evidence of wrongdoing or illegal activity on the part of anyone associated to this investigation including Ralph Goodale."

Beyond bad grammar, it was a foolish statement, full of innuendo. It said, "Oh, we're looking at something bad, and it may involve Minister Goodale. We're not really sure but we thought we should drop his name anyway and create some mischief."

Martin had been in office for two years, the Liberals for 12 years. The investigation reinforced a perception of corruption and invited Canadians to consider the Conservatives, despite their reservations about Harper's "secret agenda." In polls taken in January, the Conservatives led. They won a minority government.

Did the RCMP sway the election? Two years later, a report from Paul Kennedy, the RCMP's public complaints commissioner, said the decision "had an adverse impact" on the vote and called it "a pre-meditated and calculated course of conduct." He said he had not "the slightest idea what was going through the commissioner's mind."

Yet this all passed with little notice - and without consequences.

In Canada, there was no outrage, no broader inquiry, no accountability.

In the United States, with a more adversarial system and much higher stakes, the FBI's conduct is now at the centre of the campaign. The director is under fire. Jurists, politicians and former attorneysgenerals here fill the editorial pages and television screens. They call the announcement unprecedented, improper and indefensible.

In Canada, Zaccardelli, who threw the election to the Conservatives, has said nothing. He still owes us an explanation. Wasylycia-Leis, who said it was "credible" to think Goodale was involved in the allegations, and who expressed righteous indignation at other injustices as an MP, says she has no regrets. She still owes Goodale, whose reputation was smeared, an apology. (She ran for mayor of Winnipeg in 2010 and was trounced, poetically).

More than a decade later, no one explains. No one apologizes. This is Canada's politics of passivity.

No chance of that happening down here.

Andrew Cohen, a Canadian journalist, author and professor, is a Fulbright Scholar at the Woodrow Wilson International Centre in Washington, D.C.

Montreal Gazette
Police spying on press deemed an 'overreach'
Wednesday, 02 November 2016
Byline: Linda Gyulai

Montreal - International journalist organizations are condemning the Montreal police department's spying on a La Presse journalist through his cellphone as a violation of freedom of the press and as an "extraordinary example of overreach" by the authorities.
They're also calling it a reminder to journalists to use data encryption and other means to protect their communications with their sources.

"This seems like an outrageous breach of precedent and a threat to media freedom in Quebec," Peter Bale, president of the Global Editors Network, said from Washington, D.C., on Tuesday when he learned of the Montreal police surveillance of columnist Patrick Lagacé's phone as part of what the police claim was part of an internal probe of Montreal anti-gang squad officers later charged with fabricating evidence.

Bale offered the same reaction to an incident involving the Sûreté du Québec's seizure of Journal de Montréal reporter Michaël Nguyen's computer in September after he reported on two judges who are under investigation by a provincial body that oversees the conduct of judges.

"These cases seem like an extraordinary example of overreach by the Quebec police and Montreal police," Bale said, adding that both cases are fundamentally about protection of journalists' sources. The Committee to Protect Journalists, based in New York, also condemned the surveillance of journalists in Quebec.

"Clearly, this is a violation of press freedom and we're concerned because the decision to spy on the journalist for information about his sources may have an implication on the free flow of information," Carlos Lauría, the organization's senior program coordinator for the Americas, said of the Lagacé case.

Canada offers no constitutional immunity to journalists to protect their sources. However, the Supreme Court of Canada in a 1991 ruling recognized the special role they play in a democracy and set out a series of legal tests to be applied by the courts on a caseby-case basis to decide whether a journalist has the right to guard the confidentiality of a source.

But the two Quebec examples of the authorities exceeding their powers are "all too typical of what we are seeing in many countries," Bale said.

"I think it is often harder in Commonwealth and U.K.-based systems like Canada, New Zealand and Australia, where you don't have an absolute constitutional protection" for journalists' sources, he said.

And in the United States, where the First Amendment protects freedom of the press and freedom of expression, journalists have come under repeated attack to reveal their sources, particularly in cases involving the nation's intelligence services, and even under the administration of President Barack Obama, Bale said.

"Oddly, you've seen with the Obama administration ... journalists and whistleblowers, which are often in combination, being treated remarkably aggressively by an administration that you might otherwise have thought was more open to concepts of freedom of speech and leaking in the public interest," he said.

Bale is also chief executive officer for the International Center for Public Integrity, which oversees the International Consortium of Investigative Journalists, which released the Panama Papers, containing confidential details of more than 200,000 offshore accounts.

The team of journalists that worked on the Panama Papers worked on the Internet, he said, but they managed to protect their material from leaking out before they were ready to release it by using such tools as two-factor authentication - meaning a password and then a second-level access code - to access their database.

ICIJ journalists also use encrypted emails and burner phones, and they know to turn offlocation services on their mobile devices when they're meeting sources, Bale said.

The Committee to Protect Journalists offers a technology security guide to help journalists prevent their material from being confiscated or destroyed or having their emails and phone signals interrupted by the police or criminal organizations.

It recommends tools like Signal to encrypt messages.

"Journalists, even in countries like Canada and the United States, should use source protection methods in their communications and records," Lauría said.

"They should consider when and how to contact sources, whether to call them on a land line, a cellphone or visit them in their office or at home, where to open a secure email or chat message, and consider using a simple code or pseudonym in written or electronic files."

Other resources for journalists include: journalism.co.uk and Freedom of the Press Foundation, which manages an opensource whistleblower submission system that media outlets can use to securely accept documents and communicate with anonymous sources.

"But the moment you connect anything to the Internet, you're vulnerable," Bale said. Sometimes, simple and old-school work better than encryption, he said, such as by putting documents on a USB stick or working with paper.

"I think it's about being paranoid, and rightly paranoid," Bale said. "Maybe I'm not paranoid enough."

La Presse+
Enquête publique et projet de loi réclamés à Ottawa
Wednesday, 02 November 2016
Byline: Vincent Brousseau-Pouliot

Ottawa -- La pression s'accentue sur le gouvernement Trudeau à la suite de l'affaire Patrick Lagacé. Le NPD veut une enquête publique. Le sénateur indépendant André Pratte et le Bloc québécois entendent tous deux déposer un projet de loi sur la protection des sources journalistiques si le gouvernement n'en propose pas un, a appris La Presse. Et le commissaire à la protection de la vie privée du Canada souhaite aussi des lois plus claires en matière de protection des sources journalistiques.
Le gouvernement Trudeau estime « prématurée » la question d'une intervention législative, mais le ministre fédéral de la Sécurité publique Ralph Goodale a annoncé hier qu'il « examinera » la directive ministérielle de 2003 demandant aux forces policières de porter une « attention spéciale » au statut des médias dans le cadre d'enquêtes sur la sécurité nationale. Le cabinet du ministre Goodale n'était pas en mesure d'indiquer hier si cet « examen » comprendrait des consultations publiques.

« Le ministre examine la directive ministérielle [...] afin de s'assurer que les plus grands soins sont pris lorsque des enquêtes criminelles et du journalisme se recoupent et que la valeur canadienne fondamentale de la liberté de presse est protégée », a indiqué Scott Bardsley, attaché de presse du ministre Goodale, qui se dit « toujours ouvert à recevoir des représentations » sur le sujet.

Plusieurs parlementaires auront des suggestions pour le gouvernement Trudeau. Au Sénat, le sénateur indépendant André Pratte, qui a été journaliste pendant 37 ans (la grande majorité du temps à La Presse) avant d'être nommé au Sénat au printemps dernier, se dit « prêt à déposer un projet de loi privé » si le gouvernement n'a pas l'intention de revoir les lois en vigueur.

« Compte tenu de ce qu'il s'est passé [dans le cas de Patrick Lagacé], les législateurs ne peuvent pas juste dire "c'est préoccupant, c'est inquiétant". Il faut examiner les lois actuelles pour voir si elles sont suffisantes. »

-- Le sénateur André Pratte

« Ce qui est particulièrement inquiétant, ajoute le sénateur André Pratte, c'est que le SPVM et les juges estiment avoir agi à l'intérieur de la législation actuelle. Mon préjugé favorable porte vers une clarification de la loi. »

Un projet de 2007 revit

Le Bloc québécois déposera au cours des prochaines semaines un projet de loi privé sur la protection des sources journalistiques. Sa version préliminaire, déposée lundi au bureau du légiste de la Chambre des communes, reprend de façon quasi identique un projet de loi présenté par l'ex-député bloquiste Serge Ménard en 2007.

Ce projet de loi C-426, mort au feuilleton en raison des élections en 2008, aurait permis aux journalistes de ne pas divulguer leurs sources, leurs renseignements recueillis ou d'être l'objet d'une perquisition sauf dans de rares exceptions (ex. : si la police a tout fait pour obtenir la source autrement et si la divulgation est dans l'intérêt public).

« C'est un outil essentiel. Le cadre actuel ne protège pas suffisamment bien ces sources d'information là. Il faut une réponse législative parce que c'est un problème majeur qui concerne l'ensemble de la population. »

-- Rhéal Fortin, chef par intérim du Bloc québécois

Serge Ménard serait « très heureux » de voir une nouvelle version de son projet de loi à l'étude au Parlement. « J'ai voulu mettre dans une loi les principes de la Cour suprême », dit Serge Ménard, qui estime qu'il faudrait moderniser son projet de loi pour traiter notamment de géolocalisation.

Avant de modifier la loi, les néo-démocrates veulent d'abord une enquête publique. « On voit clairement des histoires de la sorte à répétition, dit le député Matthew Dubé. Nous sommes très ouverts à un changement législatif au besoin, mais ce n'est pas la première étape. Il faut une enquête publique pour déterminer si les forces policières respectent la liberté de la presse. Est- ce la directive ministérielle qui fait défaut ou si c'est la GRC qui ne respecte pas la directive ? »

La Presse+
Québec veut resserrer les règles de surveillance
Wednesday, 02 November 2016
Byline: Denis Lessard; Philippe Teisceira-Lessard

Québec -- L'espionnage des sources des journalistes porte atteinte à la valeur fondamentale de la liberté de la presse, a souligné le premier ministre Philippe Couillard au milieu d'une nouvelle journée de tourmente pour le chef de police Philippe Pichet.
Devant les révélations « graves » sur la filature électronique du journaliste de La Presse Patrick Lagacé, Québec a annoncé la mise en place de trois mesures pour resserrer les contrôles de ces mandats de surveillance.

Enregistrement de Mario Guérin du SPVM

« On fait face à un enjeu majeur pour une société démocratique. Je veux assurer la population et les médias que je les soutiens dans leur travail, dans la protection des sources journalistiques », a soutenu M. Couillard en point de presse, flanqué de ses ministres de la Justice et de la Sécurité publique, Stéphanie Vallée et Martin Coiteux.

Philippe Pichet, lui, a promis de s'accrocher à son poste. Il devra toutefois répondre de ses actes à l'hôtel de ville, où le bureau du maire Coderre a annoncé sa convocation.

« Des gens sont morts pour la liberté de presse, c'est une liberté fondamentale, et elle inclut la protection des sources », a affirmé Philippe Couillard. « Il est hors de question de banaliser » une atteinte à une valeur aussi importante, a-t-il souligné.

« Parmi les libertés durement gagnées au fil des siècles, se trouvent la liberté d'expression et la liberté de presse. »

-- Le premier ministre Philippe Couillard

« Le mot "préoccupé" est faible », a dit M. Couillard, appelé à décrire sa réaction quand il a pris connaissance des révélations de La Presse, « il n'était pas question pour moi d'arriver avec une réponse administrative, de dire : les règles ont été suivies. »

Groupe d'experts

Québec entend mettre sur pied un « groupe d'experts » où les médias auront conjointement à choisir leur représentant. Les policiers aussi y auront un siège. Le groupe devra faire des recommandations d'ici le printemps prochain - son mandat sera défini bientôt par la ministre Vallée.

Le comité sera présidé par un juge qui a de l'expérience dans les questions touchant les médias. Le choix du président sera discuté au préalable avec les partis de l'opposition.

La Commission parlementaire des institutions devra par la suite étudier les recommandations du groupe, un exercice public par définition. « Une grande partie de leur travail sera de faire le recensement de ce qui se fait mieux ailleurs », a dit le premier ministre, avouant ne pas savoir si le groupe aurait le pouvoir de convoquer des témoins ou de saisir les documents dont il estime avoir besoin, comme une commission d'enquête.

À la période des questions, M. Couillard a souligné qu'il « serait fort surpris » que le comité ne propose pas de changements législatifs au gouvernement.

Contrôle resserré des mandats

Le ministre de la Sécurité publique, Martin Coiteux, donnera plus tard cette semaine une directive aux trois corps de police qui peuvent demander des mandats de perquisition à un juge - Montréal, Québec et la Sûreté du Québec. Avant de se présenter devant un juge, les policiers devront avoir soumis leur demande à la Direction des poursuites criminelles et pénales.

Les mandats de surveillance visant les journalistes seront soumis désormais au même niveau que ce qui est déjà en place pour les avocats, les juges ou les députés. « La demande devra passer par le filtre du DPCP qui devra évaluer si le niveau de preuve et de soupçon justifie une pratique intrusive », a expliqué M. Couillard.

Il faut, selon lui, « hausser considérablement » les exigences pour obtenir un mandat de surveillance visant un journaliste. M. Coiteux soutenait ne pas savoir si d'autres journalistes, dans le passé, avaient pu être visés par un mandat de surveillance.

La police « inspectée »

Le ministère de la Sécurité publique procédera à une « inspection des processus, avec une attention particulière pour les cas touchant les journalistes », mise en place par les trois corps policiers, sur leurs pratiques pour les mandats de surveillance. Le rapport du Ministère sera transmis au comité d'experts pour alimenter leur réflexion.

Les polices de Québec, Montréal et la Sûreté du Québec sont les seuls corps de police à pouvoir demander des mandats pour intercepter des communications. On va commencer par le SPVM.

« Aujourd'hui, est-ce qu'on a un objectif pour dire : telle personne doit être condamnée ? Aujourd'hui, non... Mais on veut faire toute la lumière. Si nos pratiques actuelles ne sont pas adéquates, on aura des recommandations pour les changer. »

-- Martin Coiteux, ministre de la Sécurité publique

Tant M. Couillard que le ministre Coiteux n'ont pas voulu commenter le travail de Philippe Pichet, le directeur du SPVM, mis sur la sellette lundi. On voulait éviter de commenter un cas où des recours judiciaires sont toujours en cours - les policiers visés par l'enquête controversée ont été accusés.

M. Couillard n'a pas voulu dire s'il faisait toujours confiance au directeur. « Il faut faire attention au lynchage, aux procès bâclés devant l'opinion publique. Il faut surtout parler à nos partenaires municipaux », a-t-il dit. La Ville « doit réfléchir là-dessus, mais surtout, gardons notre calme », a souligné le premier ministre.

Pour le ministre Coiteux, il serait difficile à Québec de forcer une revue de cette nomination « sur la base des informations qu'on a ». Il a expliqué avoir parlé avec le maire Coderre lundi et hier. « Le Service de police de la Ville de Montréal relève avant tout de la Ville, les questions doivent d'abord être adressées à la Ville et au SPVM », a-t-il soutenu.

Le chef demeure

Ces déclarations n'ont pas fait ciller le principal intéressé.

« Oui, je l'ai », la légitimité pour rester en poste, s'est limité à dire M. Pichet en après-midi, refusant de répondre aux questions des médias.

Dans la tourmente depuis la veille, il participait à une réunion habituelle de la Commission de la sécurité publique de Montréal, où les élus municipaux peuvent poser des questions aux responsables de la police.

« Ce que j'ai fait ce matin, j'ai convoqué mon comité de direction à 9 h. On a donné différents mandats. J'ai demandé à ce qu'on fasse un paquet de vérifications parce que vous avez soulevé de bons points », a-t-il dit en sortant de la réunion.

M. Pichet devra toutefois revenir devant cette même Commission pour s'expliquer plus longuement.

« La Commission de la sécurité publique [sera] mandatée afin d'étudier toutes les façons ou les procédés que le Service de police a lorsqu'il fait enquête [surtout avec la situation actuelle] sur les journalistes », a

dit Anie Samson, responsable de la Sécurité publique au sein du conseil exécutif. « Le Service de police aura à expliquer leur méthode. »

Mme Samson a affirmé que M. Pichet avait « entièrement [leur] confiance ».

Montreal Gazette
Quebec tightens rules for monitoring of journalists
Wednesday, 02 November 2016
Byline: Philip Authier

Montreal - With the premier saying journalistic freedom is a fundamental right, the provincial government is tightening the rules that allow police to obtain warrants to conduct surveillance of reporters.
And in a sign of how seriously Quebec considers the situation, Public Security Minister Martin Coiteux has ordered inspections of Quebec's main police forces including Montreal's and the Sûreté du Québec to verify their investigation practices.

"Concerned is too weak a word," Premier Philippe Couillard said Tuesday at a hastily called news conference.

"For me what is happening is serious. It's not something that can be treated lightly.

"We are faced with a major issue for a democratic society. I want to reassure the population and the media that I support them in their work, in the protection of journalistic sources.

"People have died in the name of freedom of the press. It is a fundamental freedom."

But despite calls from the opposition that the government either fire or suspend Montreal's police chief, Philippe Pichet, the government tread carefully, with Coiteux noting people have rights but refusing to affirm his confidence. Pichet's future is also chiefly the responsibility of Montreal and its executive committee, Coiteux said.

"We are not going to indulge in a public lynching operation," Coiteux said standing with Couillard. Later, Pichet told reporters in Montreal in his mind he still has the legitimacy to stay on the job despite the revelation of police spying on reporters including La Presse columnist Patrick Lagacé. The news has rocked the province and made international headlines.

Couillard announced new directives will be issued this week making it more difficult for the three police forces in Quebec that are allowed to make such requests to get warrants to conduct surveillance on journalists. From now on such requests have to be handled with kid gloves in much the same manner as they are for MNAs, lawyers and judges.

All requests now will be filtered by crown prosecutors at the Directeur des poursuites criminelles et pénales, which will determine if police suspicions are founded and not intrusive fishing expeditions.

"The level of difficulty to get such a warrant needs to be increased," Couillard said.

He also announced the creation of a panel of experts presided by a judge to make recommendations on improving the system. Couillard said he wants to give the committee, which will include police and media representatives, the time to do a good job.

Its report is due by the spring of 2017. Couillard did not exclude new legislation to protect journalistic sources.

Couillard's moves were met with a mix of approval and criticism by the two opposition parties, with Parti Québécois Leader Jean-François Lisée saying Quebec should send in the Bureau des enquêtes indépendantes, a provincial agency, to investigate the force's actions.

While Lisée supported the creation of the panel, he told Couillard in question period that all the parties should have a say in who sits on it.

There was no satisfying Coalition Avenir Québec Leader François Legault, who demanded the government hold a complete public inquiry into the actions of Montreal police.

He criticized Couillard for not saying one way or another whether he still has confidence in Pichet.

"I think right now there's a breach of confidence," Legault said. "Mr. Pichet must think about resigning."

Couillard's remarks came one day after it was revealed Montreal police spied on Lagacé through his cellphone, obtaining his call records and tracking his movements as part of what police called an internal probe of anti-gang squad officers.

It was later revealed police have been spying on other reporters using similar tactics. Some journalists have taken to using three or four cellphones each to avoid the police scans.

The Féderation professionelle des journalistes du Québec (FPJQ) said Monday it was "revolted" by the revelations and is pushing the government to launch a public inquiry on the way surveillance court orders are doled out.

Mark Bantey, a specialist in media law (who is also the Montreal Gazette's lawyer), said he was stunned by the scope of the warrant involved in the Lagacé case. He said it seems the police were more worried about who was leaking information to the press than the actual crime.

"It sure looks like they (the police) have gone overboard because they're not out there investigating a crime, but trying to determine who in the police department is leaking information to the press. You can't use search warrants to get that sort of information," Bantey said in an interview Tuesday. "There's an obligation to exhaust all other possible sources of information before targeting the media."

As for Couillard's new directive about obtaining search warrants, he called it a first step that was unlikely to bring an immediate change to police practices.

A better solution might be to adopt new legislation - a shield law - that protects media sources, he said.

Canadian Press
Tracking of journalist highlights need for guidance to courts: privacy czar
Wednesday, 02 November 2016
Byline: Jim Bronskill

OTTAWA _ Police surveillance of a Montreal journalist's smartphone suggests a need for clearer federal guidance to the courts, Canada's privacy czar says.
Parliament has a role to play in instructing the courts on when to grant police a warrant to obtain sensitive data, privacy commissioner Daniel Therrien told a House of Commons committee on Tuesday.

"This is a very worrisome issue," Therrien said under questioning at a meeting of the Commons information, ethics and privacy committee, which is conducting a review of the federal Privacy Act.

Montreal-based La Presse newspaper said this week it had learned at least 24 surveillance warrants were issued for columnist Patrick Lagace's iPhone this year at the request of city's police service.

The surveillance flowed from an internal probe into allegations police anti-gang investigators fabricated evidence.

Three warrants reportedly authorized police to get the phone numbers for all Lagace's incoming and outgoing texts and calls, while another allowed them to track the phone's location via its GPS chip.

"It's one thing to say that the courts are involved," Therrien said. "That's a good start. But this case leads me to believe that that's not adequate in itself. It may be useful to give the court tools so that they're better able to exercise their power."

Public Safety Minister Ralph Goodale said Tuesday the Supreme Court of Canada had already explicitly laid out the test that must be satisfied when police investigations intersect with media freedoms.

Goodale played down the need for any further direction.

"It's pretty clear in the Charter of Rights. I don't know how you could make it more clear than to embed it in the Constitution of Canada," he said after a cabinet meeting.

"If there are those in the federation of journalists or others who have recommendations to make about how this can be more abundantly emphasized, I would certainly be glad to receive their recommendations."

During question period in the Commons, NDP Leader Tom Mulcair pressed Goodale to reveal whether other media members were being monitored by police or spies, but the minister did not say.

"We're not talking about police stumbling into journalists," Mulcair said. "We're talking about police surveillance of the media in Canada in the 21st century. How can we believe this government respects press freedom when the minister refuses to say whether or not other journalists are currently under surveillance?"

Among Therrien's recommended revisions to the federal privacy regime is a call for agencies involved in law enforcement to publish regular reports on the requests they make to telecommunications companies for information about subscribers.

Therrien noted that many communications outlets produce such transparency reports about the data they hand over to police and spies.

"It's one thing for companies to do it. But the ones who should really be transparent are those who ask for and use the information," he said.

"I'm not asking them to reveal law-enforcement secrets, things that would impede lawful investigations, but there is a way for departments to be more transparent."

Globe and Mail
Quebec acts to protect press freedom after police tracking of journalists
Wednesday, 02 November 2016
Byline: Ingrid Peritz

The Quebec government has moved quickly with a series of measures to try to restore confidence in the judicial system and protect press freedom amid a widening controversy over the surveillance of journalists by police.
Premier Philippe Couillard announced his government would immediately send directives to the province's three largest police forces aimed at making it harder to obtain a search warrant against a journalist.

"People have died for the freedom of the press," Mr. Couillard said. "It's a fundamental freedom."

The announcement came in the aftermath of damaging disclosures that high-profile Quebec journalist Patrick Lagacé had been the target of a months-long covert police operation that tracked the calls and texts on his iPhone, and allowed law enforcement to follow his movements through the phone's GPS. Montreal police were seeking the source of an internal leak to the media.

The scope of the controversy appeared to grow on Tuesday after a Montreal daily said three of its journalists had also been the object of police attention. Citing police sources, Le Journal de Montréal said police brass did not obtain court warrants but had scrutinized the call logs of its officers to find out who had been speaking to the reporters.

The continuing revelations have caused a firestorm both in Quebec and in Ottawa. They also led to calls for the resignation of Montreal's police chief, Philippe Pichet, including from rank-andfile members of his force. The union representing Montreal police say a clampdown to find the sources of leaks to the media is evidence of a "witch hunt."

"There was already a very weak climate of confidence toward Chief Pichet and his administration, but now this confidence is broken," Yves Francoeur, head of the Montreal Police Brotherhood, told Radio-Canada.

Mr. Couillard sidestepped questions about the Lagacé case but, repeatedly invoking his commitment to a free press, announced three steps. The province will set up an expert panel headed by a judge that will include representatives of the police and media; it will make recommendations to the National Assembly that could include legislative changes.

The Ministry of Public Security will also begin an "inspection" of procedures at the province's largest forces - Montreal, Quebec City and the provincial Sûreté du Québec. The precise mandate was not clear.

And rules to obtain the kind of warrant that put La Presse columnist Mr. Lagacé in the police's sights - a process that has come under heavy criticism - will be tightened. Officers will have to get clearance from the Quebec public prosecutor's office before seeking a warrant before the courts.

"The level of difficulty to obtain a surveillance warrant for a member of your profession deserved to be increased," Mr. Couillard told a press conference in Quebec City. Journalists would be given the higher level of protection afforded to lawyers, judges and provincial legislators, he said.

In Ottawa, Public Safety Minister Ralph Goodale told reporters his government is open to toughening the rules that govern how and when the federal government can investigate members of the media.

"We'll look at the ministerial directive at the federal level to ensure that is appropriate and sufficient in the circumstances. If we think some additional adjustment needs to be taken, we'll make it," he said.

RCMP Commissioner Bob Paulson added he was not aware of "any ongoing investigations or surveillance activities against any journalists."

The role of justices of the peace is facing intensified scrutiny in light of the Lagacé controversy in Quebec. Police obtained 24 warrants to target the Montrealbased journalist, some from Justice of the Peace Josée De Carufel, a long-time lawyer for the Quebec government who had worked in the public prosecutor's office before being named in 2012.

A report this year found that 94 per cent of those nominated to become justices of the peace in the past nine years came from jobs in the civil service, including the prosecutor's office. The absence of private-sector candidates raises a problem with "the appearance of institutional bias," the report said. "The fact that the very large majority of justices of the peace had previously worked for the government could lead people to question their impartiality," it said.

Danièle Roy, head of the Montreal Association of Defence Lawyers, raised concerns about the "appearance of justice."

"Since most of them come from the public prosecutors' office and worked with police officers all their lives, you can ask yourself if they don't tend to be a little more indulgent toward them," she said.

Experts raised questions about the court's willingness to grant the warrants to monitor Mr. Lagacé.

"A search warrant is a gross invasion of privacy, and they [justices of the peace] have the authority to grant them," said lawyer Mark Bantey, a media law specialist in Montreal.

He said a judge or justice of the peace has to be convinced there are "reasonable grounds" that a search warrant will yield evidence related to the commission of a crime.

"I don't even think they satisfied the basic test [for Mr. Lagacé]. The real purpose was to find out his sources, not who committed a crime."

Montreal Gazette
Snowden to speak at McGill
Wednesday, 02 November 2016
Byline: Staff reporter

Montreal - The timing couldn't be better.
With many Quebecers in an uproar over police spying on La Presse reporter Patrick Lagacé, McGill University on Wednesday will welcome whistleblower Edward Snowden, who is wanted in the United States for giving classified material on U.S. surveillance programs to journalists.

Speaking via video link, Snowden, a former government contractor at the U.S. National Security Agency, will discuss surveillance in Canada.

The free public lecture is being organized by Media@McGill, an interdisciplinary hub focused on the study of contemporary media.

It will take place on Wednesday at 7 p.m. in the Leacock Building, 855 Sherbrooke St. W. Seats will be first come, first served, with a lineup starting at 5:30 p.m. Snowden's leaks revealed how the U.S. and other countries monitor global private communications.

He is now living in exile in Russia to avoid prosecution in the U.S. Last month, Snowden criticized Prime Minister Justin Trudeau for not repealing Canada's anti-terror law.

On Monday, Snowden tweeted about the Lagacé surveillance, quoting a Montreal Gazette story and warning journalists that police are spying on them to identify sources.

Snowden spoke via video link at Bishop's University in Lennoxville last fall.

For more information on his McGill lecture, visit Media@McGill's website.

Montreal Gazette
Police union wants chief's resignation
Wednesday, 02 November 2016
Byline: Michelle Lalonde

Montreal - The head of the Montreal police union said police Chief Philippe Pichet should be fired for allowing his officers to spy on journalists, calling the decision to track the cellphones of La Presse columnist Patrick Lagacé and at least three other reporters "unforgivable."
"It was a serious error in judgment and it is unforgivable," Yves Francoeur, head of La Fraternité des policiers et policières de Montréal told the Montreal Gazette Tuesday. "The SPVM is the second largest police service in Quebec and the fifth largest municipal

force in North America, so we need a strong leader."

La Presse reported Monday that police requested 24 search warrants to track Lagacé's iPhone since January, which allowed police to access the numbers Lagacé had called or received calls from and track him by activating a GPS mechanism on his phone.

At least three other journalists have since learned they were under similar surveillance by police - Félix Séguin of TVA, Monic Néron from 98.5 FM, and freelance journalist Fabrice de Pierrebourg.

Francoeur said the police chief should have been well aware that courts have already established the principle that surveillance operations on journalists should be as rare as those on lawyers and judges, and can only be justified in cases involving serious crimes, when all other methods have been exhausted.

"Trying to justify spying on journalists as part of an effort to resolve problems of internal management just doesn't hold water," Francoeur said.

He added that the union was aware that officers were being threatened by upper management about speaking to journalists in recent months.

"We sent a letter to our members telling them that if they were called into meetings about this (talking to journalists) that they should contact their union so we could provide them with a lawyer. We knew there was a climate of fear, a paranoia about leaks."

He added that as chief of such a large municipal force, Pichet sits on provincial, national and international committees that advise smaller forces and governments on major global issues such as terrorism and communication with media outlets.

"I don't see how Pichet can represent us now. He has lost all credibility and legitimacy." At a press conference where he announced he had ordered an inspection of the SPVM's surveillance policies, Premier Philippe Couillard stopped short of endorsing Pichet's leadership. Pichet was besieged by reporters on his way into a closed-door meeting of Montreal's public safety commission at city hall Tuesday afternoon. Asked if he felt he had the legitimacy to remain as police chief, Pichet replied tersely: "Yes, yes, I have it."

Pichet told reporters that he had seen the premier's news conference and would "fully collaborate" with the measures announced.

He added that he had met with his deputies Tuesday morning and that "verifications" of various questions that have dogged the department since news of the Lagacé story broke on Monday have been ordered.

"We have to check and validate whether all of this information is good," he said. "We can't answer those questions in a couple of hours."

Néron, a justice reporter at 98.5 FM since 2013, told the Montreal Gazette she had been tipped off months ago that her phone might be tapped by police. After she produced a column in June criticizing SPVM management for "muzzling" longtime police communications director Ian Lafrenière by transferring him to a new job, sources contacted her to warn her her phone might be tapped. She didn't believe it at first.

"But it defied understanding that we (journalists) would be spied on. And I was more focused on the threats and pressure that police officers were experiencing internally, and I put aside the idea that we could be targeted, thinking it couldn't happen. But you better believe it can happen."

But Deputy Director Bernard Lamothe told reporters that checks were being made into the reports that three other journalists were monitored by the Montreal police department.

"The information we have today is that three journalists are not under investigation," he said. "The checks we're making involve going back in time to see if, in the course of different investigations - not major cases, but what I'd call more simple cases, more regular cases ... a journalist had been looked at."

Earlier Tuesday, the directors of Quebec's major media organizations called on the provincial government to act to protect journalists' sources after learning that Montreal police were tracking Lagacé.

They published an open letter calling on Pichet to reveal which other journalists have been or are being spied on by police.

Among the signatories to the letter were the Montreal Gazette, Radio-Canada, La Presse, Le Devoir, the Journal de Montréal, Le Soleil and CTV News.

The media organizations called on the government to make it more "burdensome" for police to obtain a warrant for surveillance of a journalist.

Fourteen Montreal legal experts are also calling on the Quebec government to launch a public inquiry into spying on media outlets and reporters.

In a statement Tuesday, they said police surveillance of Lagacé "constitutes a serious infringement of constitutional guarantees."

They called the surveillance "a dangerous precedent" and complained that judicial power is often used to curtail freedom of the press. "Since our legal system is based on trust that citizens place in the courts, we have a responsibility to ensure that everyone's rights and freedoms are respected," the legal experts said.

The legal experts are Marc-Antoine Cloutier, Julien David Pelletier, Yves Ménard, Julius Grey, Patrick Taillon, Daniel Turp, Frédérick Bérard, Rémi Bourget, Félix-Antoine D. Michaud, Sophie Tremblay, Marie-Eve Gagné, Mireille Beaudet, Marie-Hélène Dubé et Catherine Ranalli. James Mennie and Kevin Mio of the Montreal Gazette contributed to this report mlalonde@postmedia.com

CBC News

How Montreal police may have been able to spy on a journalist
Wednesday, 02 November 2016
Byline: Staff reporter

The Quebec government says it wants to make it more difficult to obtain a search warrant that would target a journalist, raising the bar to a higher level - on par with lawyers and judges.
The move, announced by Premier Philippe Couillard, comes after it came to light that La Presse journalist Patrick Lagacé was being spied on by Montreal police.

Through 24 issued surveillance warrants, the SPVM was able to obtain the identities of the people he spoke and texted with as well as to track his whereabouts via his iPhone's GPS.

But how were the Montreal police able to obtain that in the first place?

Cyberbullying law to blame?

It will only by known on Nov. 24 how the Montreal police obtained the warrants from a justice of the peace. That's the date the warrants will be unsealed.

Though some have pointed to the contentious anti-terrorism legislation, Bill C-51, as a catalyst for more invasive police tactics in Canada, Christopher Parsons, managing director of the Telecom Transparency Project at Citizen Lab, says a bill originally passed to curb cyberbullying may be to blame.

Bill C-13 amended the Criminal Code to allow police to, among other things, track an object, person, or transmission of data if the authorities have the suspicion or belief that doing so could assist an investigation.

Pasons said that Bill C-13 was "sold to the Canadian public as necessary to stop cyberbullying," but applies to the general public.

"These orders that were used to conduct surveillance on the journalist and his respective sources, those are all powers that can be used in ongoing investigations, so most Canadian citizens will be subject to them," he said.

What's more, the target of such surveillance "won't necessarily be notified that they were targeted by the surveillance unless charges are brought against them," Parsons told CBC. "So the police could conduct surveillance and the target would never know."

Parsons said Bill C-13 is serious legislation that was rushed through Parliament.

Critics already expressed concern that the bill gave police too much surveillance power when it was on the cusp of being approved in December 2014.

"What it really means we need to do is evaluate the existing powers, evaluate whether or not they should be granted to the police in their current format," Parsons said, adding that no one really knows how these surveillance powers are being used.

"We have an absolute deficiency in accountability, to be honest, at both the provincial and federal level," he said.

The justice of the peace

Regardless of the laws the police used to justify requesting the warrants, a justice of the peace had to approve them.

That's not so hard to do, according to criminal defence lawyer Jeffrey Boro, who added that in Lagace's case, "it was particularly easy."

That's because police only wanted to monitor Lagacé's metadata - tracking the numbers of all incoming and outgoing calls and texts. They did not want the content of his data, which would require a wire tap.

The latter "is the tool of absolute last resort," Parsons said, and the police would need to go to court instead of seeing a justice of the peace.

"Usually police know which justice to go see if they want to have a liberal interpretation of what it is they want to know," Boro said, adding that justices ask fewer questions and offer up less of a challenge.

"They take advantage of that when they have touchy cases," Boro said of the police.

To get the justice they want, police can find out when they're on duty and time their requests accordingly, he added.

"There's a certain familiarity that, let's say, is born between the parties, and the result is a certain laxity," Boro said.

The justice that approved most the surveillance warrants that targeted Lagacé's phone records used to work for the Crown Prosecutor, an agency that works closely with the office.

Parsons says Couillard's promise to better protect journalists from surveillance would be "relatively novel," but there are still unanswered questions as to what those protections are.

However, the fact that Montreal police chose to spy on Lagacé in the first place may point to "the cultures that have been built up within policing or security services," Parsons said.

Even CSIS, he said, "tends to place the monitoring of journalists alongside monitoring of academics or monitoring certain government officials, so they're fairly protected."

"The very fact that they were using these very, very invasive tools to monitor where the journalist was going and whom they were speaking with struck me as fairly extraordinary."

The Express Tribune
New leak shows Pakistani ISPs may have been hacked by the NSA
Wednesday, 02 November 2016
Byline: Tech Desk

Islamabad - A group called the Shadow Brokers has released a new cache of data purporting to be taken from the NSA in a Medium post titled "Trick or Treat" -- revealing hundreds of IP addresses apparently compromised by the NSA as part of its operations.
Interestingly, the majority of the nodes are located overseas, including compromises in China, Russia, India, or Pakistan, presumably to make it difficult for targets to attribute any attack launched through the network. At least four Pakistani Internet Service Providers (ISPs) are also part of the leaked list.

As with any anonymous leak of stolen data, it's possible the information was fabricated or altered in transit, although previous Shadow Brokers publications have proven to be genuine. The Medium post is also signed with PGP, thus verifying that it was written by the same source as previous Shadow Brokers drops.

In Pakistan, the compromised ISPs include PTCL gateway exchange in Lahore, Paknet (which was merged into PTCL in 2007), Multinet and Micronet.

The data dumped online by the group contains 352 distinct IP addresses and 306 domain names that purportedly have been hacked by the NSA. As indicated by the timestamps included in the leak, the servers were targeted between August 2000 and August 2010.

According to details, PTCL ITI Lahore 5 was targeted in May 2003, while Micronet and Multinet's severs were attacked in year 2000 and 2002, respectively. Interestingly, all compromised ISPs were running on Solaris, a Unix operating system originally developed by Sun Microsystems.

The development comes after online publication The Intercept reported in August that NSA hacked Pakistan's National Telecommunications Corporation (NTC) to spy on Pakistani civilian and military leadership.

According to an April 2013 NSA presentation, NSA hackers used SECONDDATE - a tool designed to intercept web requests and redirect browsers on target computers to an NSA web server - to breach

targets in NTC's VIP division. It said the targets contained documents pertaining to "the backbone of Pakistan's Green Line communications network used by its civilian and military leadership."

The identity of the Shadow Brokers is still unconfirmed, but a number of analysts have suggested the campaign is a way for Russia to undermine NSA capabilities. The most recent message from the group plays with that impression further, writing, "Amerikanskis is not knowing USSA cyber capabilities is being screwed?"

Fars News Agency
Iran Ready to Defuse Cyber Threats
Wednesday, 02 November 2016

Tehran - Deputy Head of Iran's Civil Defense Organization Brigadier General Mohammad Hassan Mansourian underlined his organization's full preparedness to confront the cyberattack and cultural invasion threats.
"Iran's Civil Defense Organization can defuse cyberattacks and cultural invasions," Brigadier General Mansourian said.

He underlined that the advanced countries are currently making huge investments in the field of civil defense.

Mansourian underscored that the cyberattack and cultural invasion should only be responded by the national civil defense system.

In May 2015, Head of Iran's Civil Defense Organization Brigadier General Gholamreza Jalali announced that the country has set up cyber defense workgroups to better coordinate measures for defending nuclear facilities against enemies' cyber attacks.

"The country's vital cyber infrastructures have been identified and separate cyber workgroups have been formed in all fields," Jalali told reporters in Tehran.

"For instance a cyber defense workgroup was set up in the nuclear field for Natanz nuclear installations and no serious incident has threatened this section in the past two years," he added.

In relevant remarks in October 2014, Jalali revealed that a US cyberattack on Iran's nuclear enrichment facility in Natanz failed due to his organization's tough defensive measures.

"The first cyberattack, codenamed Olympic Games, was carried out on Natanz and was declared by the US President, but it met our heavy (defensive) response," Jalali told reporters in a press conference in Tehran.

The senior commander said the US changed its cyber commander following the failure in the cyberattack on Natanz, adding that the US general was forced to retire several months ago "due to the wrong information and data that he had presented to President Obama". And this was the result of our direct confrontation with them, General Jalali added.

The US was the principal player in the most sophisticated cyber-attack ever known and has been orchestrating a campaign against Iran designed to undermine the country's nuclear program.

The New York Times came up with an in-depth report on June 1, 2012 saying that from the very first month Barack Obama took over as US President, he secretly ordered increasingly sophisticated attacks on Iran's computer systems that run the country's main nuclear enrichment facilities.

The disclosures about Obama's role in the cyberwar against Iran appear to show beyond doubt that the US, with the help of Israel, was behind the Stuxnet virus attack on Iran's centrifuge machines - used to enrich uranium. The revelation then indicated that Washington and Tel Aviv were also behind the Flamer and Duqu virus attacks discovered by experts in May 2012.

Codenamed Olympic Games, the attacks were spearheaded by the US government under the Bush administration. Stuxnet targeted Siemens industrial equipment to spin hundreds of centrifuges beyond their breaking points and eventually disable Iran's nuclear efforts.

According to the report, Obama decided to speed up the attacks, even after the worm escaped from Iran's Natanz plant in 2010 and later ended up on the Internet.

During a meeting following the worm's escape, Obama even considered that the worm should be stopped thinking that America's most ambitious attempt to slow the progress of Iran's nuclear efforts had been fatally compromised. Should we shut this thing down? Obama asked members of the President's national security team.

However, he finally decided to go ahead with the cyberattacks. What followed thereafter was the Natanz plant being hit by several newer versions of the worm.

The report is said to be based on 18 months of interviews with current and former American, European and Israeli officials involved in the program as well as with outside experts, who provided contradictory assessments of how successful the attack was in slowing down Iran's progress of developing nuclear weapons.

While internal Obama administration estimates claim the effort was delayed by 18 months to two years, some other experts, both inside and outside the government, said that Iran's enrichment levels had steadily recovered. A year later, Iran enriched uranium to the 20-percent grade, way beyond the 5-percent purity level that was done in Natanz in 2012.

The Australian Financial Review

Government agencies the new 'honey pots' for cyber spies

Wednesday, 02 November 2016

Byline: Fleur Anderson

Canberra - More than 40 per cent of Australia's government agencies have inadequate awareness of cyber security risks and could become the new "honey pots" of state-sponsored online espionage and cybercrime, a new investigation by private-sector cyber security experts has found.
The Australian National University's National Security College found smaller government agencies and medium-sized business were the weakest link in Australia's cyber security defences because they are not vigilant enough about "low-level" threats like malware and denial of service attacks.

Lead researcher Dr Tim Legrand, working in partnership with Macquarie Telecom Group, found it was very likely many attacks were not being reported to the federal government's Computer Emergency Response Team. This is despite a $230 million cyber security strategy introduced by Prime Minister Malcolm Turnbull in April.

"This means authorities may lack the accurate and comprehensive information needed to appropriately prioritise national cyber defence initiatives," the research paper said.

The security of government computer systems is in doubt after the Bureau of Meteorology was hacked last year by a foreign power, which installed malicious software to steal documents and compromise other government networks, and the botched 2016 Census which was "attacked" but not hacked by traffic from Singapore.

In addition, the Australian Federal Police and the Department of Innovation, Industry and Science - one responsible for catching cyber criminals and the other for cyber policy - to meet the government's own standard for cyber security in an Auditor-General's audit in May this year.

The latest report, to be launched on Wednesday by minister assisting the PM on cyber security Dan Tehan, found widespread weaknesses in security practices, and poor awareness by senior management.

Of 22 government agencies surveyed, 84 per cent have an individual chiefly responsible for cyber security but only 64 per cent of these sit on an executive team or board which indicated cyber risk management was not at the highest decision-making level.

About 41 per cent of the agencies' executives were described as having poor or limited knowledge of cyber risk and not one agency reported reviewing their cyber security monthly or weekly, in contrast with 31 per cent of the private sector which reviewed its security at least monthly.

"All businesses and agencies are interconnected to other businesses and parts of government in the modern digital economy, and becoming more so every day," Macquarie Government managing director Aidan Tudehope said.

ABC News
Senior Canberra bureaucrats under pressure to improve security processes
Wednesday, 02 November 2016
Byline: Lexi Metherell

Canberra - The Federal Cyber Security Minister says he will press heads of government departments to improve their security processes as research reveals they are a "weak link" in national defences against cyber attacks.
The ANU's National Security College and Macquarie Telecom Group surveyed employees responsible for cyber security at about 60 government agencies and medium-sized businesses.

About 40 per cent said their boards had limited or poor knowledge of cyber risks like hacking, espionage, malware or data breaches, and only around 60 per cent of cyber security managers are at executive levels.

Dr Tim Legrand from the National Security College said cyber security arrangements in the sectors are "shaky".

"There's a distinct lack of knowledge and awareness of the forms of vulnerabilities in cyber space that governments and private industry face," he said.

That lack of knowledge can lead to events like the attack that took the census offline, a case in which the Australian Bureau of Statistics , according to Dr Legrand.

"Often those who are in control of contracting out services don't know what they don't know," he said.

"They don't have sufficient levels of knowledge about the risks to be able to adequately assess a procurement contract, and I think that came through quite clear with what happened with the census attack."

Senior executives unprepared

After a , the Government announced in April it would spend $230 million on preventing cyber attacks.

The Minister Assisting the Prime Minister on Cyber Security, Dan Tehan, who is launching the report, said the Government would tell heads of departments to take cyber security seriously.

"What I will be doing is writing to all cabinet ministers asking them to point out to their departmental heads and agency heads the need for them to take cyber security very seriously," he said.

"[I will also urge] the need for them to make sure that there is reporting occurring at senior levels of the executive, and that there is someone responsible at the senior level of the executive for cyber security."

The managing director of the Australian Institute of Company Directors, John Brogden, admitted boards were playing catch-up.

"There's no doubt that the issue of cyber security has landed with a thud on the board table," Mr Brogden said.

"It's a worldwide problem being driven very strongly by organised crime, and it's true that in too many cases boards and companies are simply too slow to understand the size of the threat."

Mr Brogden said part of the issue was that technology so rapidly evolved and boards could not keep up.

"At the moment, the best guarantee any board can get from its management is that we're safe against cyber attacks now," he said.

"Literally the moment we say it, we don't know whether we're safe this afternoon tomorrow or next week because the technology's changing all the time."

Gulf Times
Qatar, UK working on digital system against cyber-attacks
Wednesday, 02 November 2016
Byline: Satyendra Pathak

Doha - British cyber-security experts are working in close cooperation with the Ministry of Interior (MoI) officials to map out 'digital defence' mechanism to protect FIFA 2022 World Cup from cyber- attacks, a London-based security advisor has said.
"We want to work closely with the Qatar government in preparing for the 2022 FIFA World Cup. The lessons of how and what we did to protect 2012 Olympics from cyber threats, we are very keen to share it with Qatar," Richard Freeman, senior police and security advisor at UK Defence and security organisation, told Qatar Tribune on the sidelines of the Milipol Qatar 2016 exhibition in Doha.

Large scale events such as the upcoming 2022 World Cup are more vulnerable to cyber-attacks, the expert said, adding that the UK is sharing classified intelligence with Qatar to deepen ties between the two countries' security agencies in the face of a burgeoning international threat from cyber warfare.

Cyber-security is still one of the biggest IT issues in Qatar with majority of organisations lacking the internal capabilities to protect against sophisticated cyber-attacks, he said. Freeman said that the Supreme Committee for Delivery & Legacy officials interact with British officials on a regular basis to protect information related to World Cup preparations from cyber espionage.

"The nature of cyber-attacks has changed over the years. Cyber espionage, which is stealing intellectual property, has emerged as one of the major threats. We prevented many such attacks before and during the 2012 Olympics. Qatar needs to invest heavily in protecting data, which is most valuable to them in organising the mega event," the expert said.

Citing awareness as a major tool to prevent cyber-attacks, Freeman said that British experts are also working with Qatari officials to create awareness among Qatari residents and citizens about such threats and ways to deal with them.

Talking about the importance of Milipol Qatar exhibition in cementing ties between British and Qatari entities, the expert said many British firms have struck many deals during the previous editions of the mega exhibition.

This year around 12 British companies are showcasing innovative products, he said, adding that booth visitors have shown great interest in the products on display. "UK companies are looking to enhance opportunities in Qatar through industrial partnerships and long term joint ventures.

We have a strong track record in organising major sporting events and we will continue to work with Qatar as they prepare for the 2022 World Cup and develop national security capabilities to support the wider 2030 vision," he said.

The Japan News
Train a cohort of IT security experts to fight cyberterrorism ahead of 2020
Wednesday, 02 November 2016
Byline: Staff reporter

Editorial: Both the public and private sectors should cooperate in nurturing manpower to protect the security of our information society.
The Economy, Trade and Industry Ministry has established a new national qualification system in which those who have advanced knowledge and skills in the field of cybersecurity will be registered as "IT security support providers." Examinations for qualification in this field will begin next fiscal year.

To fight cyberterrorism during the 2020 Tokyo Olympics and Paralympics, the ministry hopes to train at least 30,000 cybersecurity specialists.

Crimes committed via the internet have become more diverse. Hackers have stolen customer lists and credit card information from the computers of public organizations and private companies, and have tampered with websites. In some cases, they have demanded large sums of money in exchange for the data they have stolen.

The main tasks of IT security support providers would be to serve as a control tower to determine the weaknesses of in-house cybersecurity systems, augment their protection and make sure they can withstand cyber-attacks. They are also required to promptly deal with any breaches in security.

The planned examinations will be of the highest degree of difficulty among the tests related to information processing that have been conducted by the central government. Previous examinations have only resulted in the issuance of a certificate showing a passing grade, and did not extend a registered national qualification to the successful examinee.

Registered IT security specialists will be obliged to take annual training courses and pass an exam to upgrade their knowledge and maintain a high level of cybersecurity skills. It will be necessary to enhance the qualification's credibility in society by constantly reviewing the content of lectures to ensure they are up-to-date and of the highest level.

Firms must join in

The inauguration of the new national qualification system would be meaningless unless enterprises and organizations effectively use qualified experts. The government plans to draw up a list of registered security support providers, so business enterprises can refer to it when hiring IT security professionals.

It is important, first of all, to make it widely known that registered security specialists are at work.

Another essential need is for company managers to change their mind-sets. According to a 2013 survey conducted by an auditing firm that operates internationally, companies with executives who energetically take in-house cybersecurity measures totaled 59 percent in the world as a whole, while among Japanese enterprises it was a mere 27 percent.

If private information leaks from a business enterprise as a result of a cyber-attack, the company's credibility will be impaired. Taking cybersecurity measures is an important investment to ensure corporate defense.

If enterprises offer cybersecurity professionals preferential employment conditions, it will help generate a virtuous cycle of highly talented people aiming to become IT security support providers.

There are fears that the Tokyo Olympic and Paralympic Games may be easy targets of cyberterrorism.

In regard to ticket sales, competition management and other matters, the Olympics cannot be held without information technology. If a security system related to an event comes under a cyberterrorist attack, the Games will be thrown into utter confusion.

Reinforcing the security of transportation networks and financial systems is also vital. The skills of IT security support providers will be tested everywhere.

Jerusalem Post
Israel unprepared for 'dramatic uptick' in cyber threats
Wednesday, 02 November 2016
Byline: Yonah Jeremy Bob, Lidar Gravé-Lazi, Sharon Udasin

Jerusalem - Israel is woefully unprepared for the "dramatic uptick" in cyber threats confronting it, according to State Comptroller Joseph Shapira.
In a report released on Tuesday, Shapira explained that more and more of the country relies on electronic platforms, which are vulnerable to cyber attacks. He referred to the recent worldwide massive cyber hacks, and possibly to the cyber hacking interference in the US presidential election, to show the increasing volume and sophistication of the attacks.

The comptroller said that other than certain critical infrastructure sectors, which are well-protected, much of the country is still heavily exposed to cyber attacks.

Shapira's report, which deals mostly with economic issues, also criticized the Education Ministry, after an investigation found serious deficiencies in the management of the ministry's budget.

The report noted that the budget is one of the country's largest, at NIS 48.9 billion in 2015, not including the budget for higher education, and at NIS 50.9b. in 2016.

The comptroller said the last few years have seen a steady increase in the education budget in comparison with other OECD countries, but that despite this, Israel still has one of the largest educational gaps in the world.

The report cited the need to optimize the budget to minimize gaps in education, and bring the Israeli education system up to par with other OECD countries.

"The government in general, and the education and finance ministries in particular, have a duty to optimally realize all the resources intended for the education system, while constantly reviewing the allocation and outputs and the degree of attainment of the government's goals in the fields of education and society," the report concluded.

In another section, the report said that the Company for Location and Restitution of Holocaust Victims' Assets has "inadequately" prepared for the termination of its activities, set to end in December 2017.

The report found numerous failings by the company in tracking down and restoring assets to Holocaust victims' heirs.

The company's cost of operations up to the end of the year is estimated at some NIS 186m., most of which comes from the assets of those who perished in the Holocaust.

Since its establishment, the company has identified assets of Holocaust victims from various sources in Israel, totaling NIS 1.8b., although it has only returned NIS 280m. to heirs - approximately 15.6% of the total property located.

Shapira's report also took a look at a number of infrastructure issues, including a critique of the country's decentralized water corporations, the deficiencies of research institutes within the National Infrastructure, Energy and Water Ministry, malfunctions with the Transportation Ministry's driver's licensing department, and shortcomings in that ministry's budgetary planning.

Another area of focus was the country's natural gas distribution system, which the report described as failing to expand to meet the needs of consumers.

Shapira sharply criticized the government for the troubling rise in traffic fatalities over the past several years, finding particular fault with the operation of the National Road Safety Authority.

The comptroller also slammed the IDF for inadequate attention to safety issues, in particular the outbreak of fires and the failure to fully investigate them.

Moreover, he criticized the IDF for a lack of attention to proper recruiting and sorting of recruits according to their capabilities and potential contributions.

The IDF responded that it is already working on improving on both issues. The report also contained a section on upkeep and oversight of building in the Old City's Jewish Quarter.

Times of Israel
Watchdog says Israel unprepared for civilian cyber-threat
Wednesday, 02 November 2016
Byline: Shoshanna Solomon

Jerusalem - A new report by the Israel's State Comptroller Yosef Shapira has found that the nation is mostly unprepared to protect its civilian cyberspace in view of the growing intensity of cyber-threats globally.

"The findings of this report suggest that there are gaps between the intensity of the threat to the entire civilian cyberspace and the rate of response in terms of organization and staging of the state's defense, except for a few areas and sectors such as critical state infrastructure," the report said.

From September 2013 to July 2015 the State Comptroller's office held an audit on the country's preparations for the protection of cyberspace. The team examined a number of issues, including the formulation of a comprehensive defense approach to cyberspace; regulation of responsibility for dealing with the cyber-realm; regulation of the cyber-market; the setting up of bodies and systems for cyber-protection; and the level of protection required.

The team also evaluated the protection of the computer systems that are critical state infrastructure.

The audit was held at the National Cyber Bureau, which was set up in 2011 and is part of the Prime Minister's Office, and at the Shin Bet security agency and a number of government agencies and other entities.

The National Cyber Bureau was mandated with regulating responsibility for cyberspace and submitting a proposal for a comprehensive defense approach. Its establishment has in fact expanded the government's cyber-activities, the report said. Even so, the report found "gaps" between the intensity of the threat to the civilian cyberspace and the state's ability to respond.

The report said the government's implementation of decisions about the cyber-realm was slow and did not keep up with the rising threat against Israel; decisions regarding where cyber-defense responsibilities lie were "not clear enough"; and there were "significant flaws" in the work of the cyber bureau.

The report recommended that the cyber bureau set up an operational framework with yearly or multi-year milestones and define the scope of the civilian cyber-threat and how to address it.

A steering committee should make sure the Shin Bet's safety recommendations are implemented for critical national infrastructures and a system for reporting progress to the government is in place, including a set of quantitative measures for progress.

The government should "learn lessons"and "promote the required tasks in the field of cyber security preparedness," the report said. Large parts of the report, presented on Tuesday to Knesset Speaker Yuli Edelstein, were not allowed to be published due to confidentiality issues, the comptroller's office said.

Los Angeles Times
FBI faces high bar in Clinton case; Legal scholars say charges are unlikely, partly because of Comey's past remarks.
Wednesday, 02 November 2016

Byline: Del Quentin Wilber

Washington - Even if FBI agents discover classified information on a newly seized laptop, Hillary Clinton is unlikely to face criminal charges, according to legal experts and former federal prosecutors.
That's largely because the Justice Department and FBI Director James B. Comey have already declined to prosecute based on a legal conclusion that there was no evidence that Clinton and her aides intended to violate laws governing the handling of classified information, a key element of such a criminal offense.

To change the calculus, the FBI would have to find correspondence that clearly demonstrates Clinton or her aides knowingly broke the law, exchanged materials they knew to be classified or attempted to interfere with the investigation by withholding or destroying evidence, according to former federal prosecutors and legal scholars.

"Such an email itself would have to be one of those things you would be saying, 'I can't believe you wrote that down,' " said Roscoe Howard Jr., a former federal prosecutor and U.S. attorney for the District of Columbia during the George W. Bush administration. "I would be shocked if they found such a thing."

The chances of the bureau missing such evidence after what Comey had described as a comprehensive inquiry would be slight, former prosecutors said.

"Short of a truly inculpatory email, the existence of which I find hard to fathom, I don't see a situation that comes out of this that justifies the hoopla," said Stephen Vladeck, a law professor at the University of Texas.

The analysis comes as federal agents and analysts are scrambling to review emails found on a laptop used by former Rep. Anthony Weiner and his estranged wife, Huma Abedin, one of Clinton's closest aides. Agents came across Abedin's correspondence while searching the computer for evidence that the disgraced former lawmaker may have violated federal laws when exchanging sexually explicit messages with a 15-year-old girl.

During its nearly yearlong inquiry, the FBI interviewed dozens of witnesses, conducted forensic tests and examined tens of thousands of messages that passed through the private email server used by Clinton and some of her aides while she was secretary of State.

In the end, agents uncovered classified information in 193 emails that were part of 81 email chains, though none of the emails were marked with a classified header. Of those chains, the department concluded that eight should have been treated as top secret, the highest level of classification, the FBI reported.

"So if there were 100 examples of classified information before and now they find 10 more, how is that going to change the analysis?" asked Peter Zeidenberg, a former federal prosecutor who signed a public letter critical of Comey's decision last week to publicly reveal the new inquiry. "It's the same question. It's the same issue. That's even assuming the emails they find on the laptop are classified emails. There may all be duplicates, or emails that don't have any classified information. We don't know."

And even if agents discover evidence that warrants an indictment, Comey's past public statements could undermine a future prosecution, legal experts said.

Defense lawyers would certainly seek all records associated with his public announcement in July, when he declared Clinton's actions were "careless" but not criminal.

An about-face by the FBI would permit defense attorneys to attack the thoroughness of the entire investigation, pointing out that it failed to turn up Abedin's emails on a laptop she shared with her husband.

"A classic defense in any criminal case is to accuse the investigating law enforcement agents of 'shoddy police work.' " said Mary Pat Brown, a former federal prosecutor. "When there are inconsistencies in the evidence itself, or any delays or missteps in collecting evidence, the government's case is vulnerable to attack."

Comey's unusual move to publicly discuss the case with reporters and Congress in July was in part to demonstrate that the bureau's inquiry was meticulous and independent.

But Vladeck said his action could now backfire. "Those statements make it difficult for there ever to be a prosecution," he said. "Comey laid a trap for himself in July."

Perceptions that the new emails won't dramatically change the case are part of the reason Clinton supporters were so incensed by Comey's surprise and vague announcement last week that the bureau would examine the materials over the coming weeks.

Agents are hoping to have a preliminary assessment of the Abedin emails completed by election day, though it remains unclear whether the FBI will make a further public statement about the case, despite calls for more information from Democrats and Republicans.

Agents will need to sort out Abedin's emails, discard duplicates and then examine what's left to see whether anything is relevant to the Clinton inquiry, a federal law enforcement official said.

The laptop contains hundreds of thousands of emails -- most of them Weiner's -- and it will take weeks to fully vet them, the official said.

London Times
Cyberforce seeks 50 elite brains
Wednesday, 02 November 2016
Byline: Mark Bridge

London - Workers with no background in technology will be recruited to an "elite" force to defend the nation against cyberattacks through a ten- week bootcamp.
As part of a £1.9 billion National Cyber Security Programme announced yesterday, the government will launch the free training course in London next year to turn people looking for a career change into codebreakers.

In a move reminiscent of the War Office's use of a Telegraph cryptic crossword to recruit for Bletchley Park in 1942, the government will use psychometric tests to identify 50 brilliant brains. Once selected, they will complete exercises including dealing with a nationwide cyberattack. They will also study the mindset of hackers.

The government said that, if successful, the GCHQ-certified scheme would later be introduced nationwide. According to the SANS Institute, the private company running the bootcamp, it will cram two years' worth of training into the ten-week schedule.

Students on the course would be tracked by leading cybersecurity employers and would be ready to secure jobs on completion.

It added that the programme was targeted at "high-aptitude people" looking to retrain -- including soldiers, doctors and nurses.

Matt Hancock, the minister for digital and culture, said: "This new academy will give students the skills the nation needs to fight cyberattacks and help us achieve our ambition of making the UK the safest place to live and do business online."

The course is part of a package of measures including the creation of a cybersecurity research institute and funding for start-ups working on novel security tools. In its National Cyber Security Strategy document, the government identified "Russianlanguage organised criminal groups" in eastern Europe and state and statesponsored groups as major threats. Speaking at a technology conference, Philip Hammond, the chancellor, spoke in dramatic terms about the risks if Britain did not prepare adequately to meet the threat from cyberattacks that could potentially bring down the power network. He said: "We would be left with the impossible choice of turning the other cheek, ignoring the devastating consequences or resorting to a military response."

David Emm, principal security researcher at Kaspersky Lab, said: "The steps taken by the government to educate individuals across different job disciplines are indeed positive. However, as the government has

very specific national security needs in mind, they are in the best position to determine what level of training is sufficient."

London Daily Telegraph
Russia is organising a cyber-coup in America
Wednesday, 02 November 2016
Byline: Con Coughlin

Column - In the world of global espionage it used to be the case that, if you wanted to stage a coup, what you needed was a rebel group that was prepared to drive its tanks through the gates of the presidential palace and overthrow the ruler.
The Cold War saw the CIA spend a fortune funding groups dedicated to overthrowing regimes deemed to be either unfriendly to Washington or too close to the Soviet Union. Iran, Iraq, Guatemala, Vietnam, Laos, Haiti, Zaire, Cuba, Chile: no corner of the world was spared Langley's determination to shape the global political landscape to Washington's liking.

Nor were the Americans alone in fomenting unrest and discord. The Soviet Union was just as active in its efforts to proselytise the merits of communism, while the primary role of Britain's MI6 intelligence service was to infiltrate the highest echelons of Moscow's military and intelligence establishments, a mission where it achieved remarkable success.

If the old Cold War marked the high-water mark for the oldfashioned military coup, then the new one that Russian President Vladimir Putin seems determined to launch against the West will be fought with a higher level of sophistication.

No one in Washington seems in any doubt that Moscow has been behind the release of thousands of Hillary Clinton's personal emails that are seriously undermining her attempt to win the presidential election for the Democrats. As with Edward Snowden, the whistleblower who exposed sensitive details concerning America's intelligencegathering operations, the Clinton revelations have been made through Julian Assange's WikiLeaks website.

This has resulted in the unlikely scenario where Donald Trump, the maverick Republican contender, is now publicly heaping praise on a website that prides itself on its Leftwing, anti-establishment credentials. Does Mr Assange really want to go down in history as the man who put Donald Trump in the White House? The more troubling point, though, is the direct impact Russia's skillfully managed cyber-offensive on the American political system could have on next week's poll.

Mrs Clinton has made it clear on the campaign trail that, if she wins, she will take a more robust approach towards Moscow than we have seen from the White House during Barack Obama's presidency. Denying Mrs Clinton victory, then, is very much in Russia's interests, particularly if it results

in a victory for Mr Trump, who has yet to provide a satisfactory explanation about the close links between his own advisers and the Russian government.

Irrespective of who wins next week's contest, though, the real concern is that the precedent has been set whereby a hostile government can seek to change the political landscape of a rival nation without having to fire a shot in anger.

For in the increasingly sophisticated cyber age in which we live, it is far easier and cheaper to undermine opponents through carefully targeted internet attacks than assembling and funding rebel armies. Moscow's ability to undermine the fundamental infrastructure of government is well known in Ukraine, where a Russianbased cyber attack closed down the country's power grid.

But it is the ability of cyber warriors to invade the political space that is causing most concern.

Apart from interfering in the American democratic process, Russian hackers were most likely behind a massive cyber attack on Germany's lower house of parliament this year which resulted in its computer systems being closed down for days.

Andrew Parker, the head of MI5, says Britain, too, is a major target for Moscow, with the Russians willing to use "propaganda, espionage, subversion and cyberattacks" to undermine the Government. Nor is Russia the only country employing cyber as a tool of aggression. China, North Korea and Iran are among a number of countries that are known to have developed sophisticated cyber capabilities.

As the most sophisticated cyber attacks are directed from countries with authoritarian regimes, the challenge for Western democracies is to be able to defend themselves without having to compromise the liberties of their citizens.

The first line of defence for countries like Britain against cyber Armageddon is for firms and individuals to take far greater care with their internet security, whether regularly changing passwords or updating anti-virus software.

The sheer scale of the threat, though, means that governments must be just as prepared to protect themselves against unwelcome interference in their political institutions as they are for attacks against their national infrastructure.

Otherwise the day will surely come when powerful democratic states are brought to their knees simply by clicking a mouse.

The Guardian (London)
Cybersecurity firm fails to find links between Donald Trump and Russian bank
Wednesday, 02 November 2016

Byline: Julian Borger

Washington - A US cybersecurity firm hired by a Russian bank to investigate allegations of a secret line of communication with the Trump Organization said on Tuesday there was no evidence so far of substantive contact, email or financial links.
Mandiant, which is owned by the California-based company FireEye, said it examined internet server logs presented to the bank by media organisations investigating the link.

The online magazine Slate published a story on Monday about communication between a server hosting Trump domain addresses and a server owned by the Moscow-based Alfa Bank, owned by two oligarchs, Mikhail Fridman and Pyotr Aven. Aven worked with Vladimir Putin in city government in St Petersburg in the early 1990s.

The Slate story, quoting a range of cybersecurity experts, said the communication between the servers suggested it was human rather than robotic, and that it was intended to be secret and exclusive.

In a statement, FireEye said it had been presented with a log of the communication between the servers over a period of 90 days, listing the separate contacts.

"The information presented is inconclusive and is not evidence of substantive contact or a direct email or financial link between Alfa Bank and the Trump campaign or Organization," the statement said. "The list presented does not contain enough information to show that there has been any actual activity opposed to simple DNS lookups, which can come from a variety of sources including anti-spam and other security software."

The statement continued: "As part of the ongoing investigation, Alfa Bank has opened its IT systems to Mandiant, which has investigated both remotely and on the ground in Moscow. We are continuing our investigation. Nothing we have or have found alters our view as described above that there isn't evidence of substantive contact or a direct email or financial link between Alfa Bank and the Trump campaign or Organization."

The allegations have triggered debate among security experts in the US, in the midst of a fierce political row over the role of the FBI. Democrats have decried the decision of the FBI director, James Comey, to notify Congress of the discovery of new emails relevant to its inquiry into Hillary Clinton's use of a private server while secretary of state, without making public parallel investigations into Trump's ties to Russia.

Computer scientists quoted in the Slate story said that the Trump server had a capacity for mass email but was only being used for a small amount of traffic, nearly 90% of which was with servers from a single organisation, Alfa Bank.

"The parties were communicating in a secretive fashion. The operative word is secretive. This is more akin to what criminal syndicates do if they are putting together a project," said Paul Vixie, a software expert and one of the creators of the domain name system (DNS) that guides communication on the internet.

Robert Graham, a cybersecurity expert and head of Errata Security, dismissed the claims as "nonsense". He said the domain in question, trump-email.com, was actually controlled by Cendyn, a company that handles marketing for hotels, including Trump's hotels.

Graham also argued that there was no sign of human communication between the servers, which appeared to be looking up each other's IP (internet protocol) addresses, the first step towards establishing communication. The logs show that two Alfa Bank servers sent a total of more than 2,700 lookup requests to the Trump email server.

"The requests are spread out evenly throughout the day, with no correlation to time zones," Graham said in an email. "This would indicate automated tools looking up incoming spam addresses, not humans sending email. If it were sign of human activity, we would see spikes around 9am when people got to work and 1pm when they got back from lunch."

John Bambenek, a consultant with Fidelis Cybersecurity, who has also studied the logs, said there were unanswered questions about their provenance and authenticity.

"The identity of the person bringing the data can be more important than the data," Bambenek said. "I'm suspicious of the claims that this was gathered legally. They tell an interesting story, but it's not clear whether there is selection or filter applied ... I smell smoke. I just don't know where the smoke is coming from.'

L Jean Camp, a professor of informatics at Indiana University, said there were still a lot of unanswered questions about the communication between the servers.

"It doesn't act like a marketing server. Because you wouldn't use a heavy-duty mailer with over 80% of its communication with just one organisation," Camp said. "I don't know of any marketing campaign that would do that."

According to Slate, the Trump email domain was hastily reconfigured after a New York Times reporter approached Alfa Bank about the connection in September. On Tuesday, the New York Times reported that the FBI had spent weeks looking into the Alfa-Trump logs but concluded that "there could be an innocuous explanation, like a marketing email or spam, for the computer contacts".

Washington Times
Huma Abedin handled classified data on computer shared with Anthony Weiner

Wednesday, 02 November 2016
Byline: Ben Wolfgang, Andrea Noble

Washington - Emails released by the State Department over the past 18 months show that Huma Abedin frequently handled classified information -- suggesting a major reason why the FBI has been eager to get a full look at the personal computer she shared with her now-estranged husband.
That computer has become the center of a major political flap in the final week before Election Day. Ms. Abedin's boss, former Secretary of State Hillary Clinton, is trying to fend off concerns that there is a smoking gun still to be found among her top personal aide's messages.

But the track record indicates a reason for concern: Of the messages Mrs. Clinton turned over to the State Department, nearly 5,000 were sent to, or received from, Ms. Abedin. More than 180 of those contain information now determined to be "confidential," and one message is deemed to contain "secret" information.

In the "secret" message, Ms. Abedin forwards to Mrs. Clinton information about a 2009 ballistic missile test by North Korea.

"It is frankly remarkable that the FBI and Justice Department are only now investigating Abedin's connection to Clinton's mishandling of classified information," said Tom Fitton, president of the watchdog group Judicial Watch, which has sued to try to get to the bottom of the Clinton-Abedin connection at the State Department.

The Weiner investigation is the latest involving the Clintons and those in their circle. It joins a reported investigation earlier this year into the Clinton Foundation; another into campaign donations to Virginia Gov. Terry McAuliffe, a longtime fundraiser and political ally; and the renewed look at Mrs. Clinton's handling of classified information.

Whether anything on the Abedin-Weiner computer is relevant to the investigation into Mrs. Clinton, which the FBI closed in July, is heatedly debated.

Mrs. Clinton's team insists there is nothing to be found, and they have excoriated FBI Director James B. Comey for publicly announcing less than two weeks before an election that he is looking at the new emails.

Ms. Abedin's attorneys say the longtime Clinton aide -- who is virtually guaranteed to get an influential White House post if Mrs. Clinton defeats Republican Donald Trump on Election Day -- was wholly unaware that any of her messages were on Mr. Weiner's computer.

"From the beginning, Ms. Abedin has complied fully and voluntarily with State Department and law enforcement requests, including sitting for hours-long interviews and providing her work-related and potentially work-related documents," her attorney, Karen Dunn, said in a statement Monday night. "She

only learned for the first time on Friday, from press reports, of the possibility that a laptop belonging to Mr. Weiner could contain emails of hers."

She said Ms. Abedin will be "forthcoming and cooperative" with the latest FBI investigation, which surely will drag past the election.

Mrs. Clinton briefly addressed the controversy on Monday by acknowledging that voters had questions about the FBI inquiry, But during an appearance in the battleground state of Florida on Tuesday, Mrs. Clinton dropped all references to the investigation and instead slammed Mr. Trump's past statements about women.

"Some of what we've learned, some of this stuff is very upsetting," she said before reciting some of Mr. Trump's most inflammatory comments.

Mr. Trump and fellow Republicans, meanwhile, have tried to keep attention focused on the FBI's renewed probe, saying it shows voters what to expect if Mrs. Clinton wins the White House.

Indeed, the Clinton family and its allies have faced an extraordinary number of investigations over their quarter-century in Washington.

"There's an interesting circumstantial case to be made how much smoke there has been surrounding the Clintons over the years," said Chris Jenks, a law professor at Southern Methodist University and a former attorney adviser at the State Department.

In addition to the investigation of Mr. Weiner, whose sex- related text messages may have been sent to a juvenile, the FBI also reportedly pushed this year to open public corruption probes of the Clinton Foundation, citing concern about rewarding donors with special political access and favors.

The Justice Department, which last year found insufficient evidence to open a case, declined to investigate, CNN reported.

"We are not aware of any investigation into the Foundation by the Department of Justice, Federal Bureau of Investigation, or any United States Attorney's Office and we have not received a subpoena from any of those agencies," the Clinton Foundation said in a statement.

But the difference of opinion between FBI agents and Justice Department prosecutors roiled investigators, according to The Wall Street Journal, which this week reported that agents from the FBI's New York field office continued to pursue a case until at least as recently as August. That month, a senior Justice Department official called Andrew McCabe, the bureau's second in command, "to voice his displeasure at finding that New York FBI agents were still openly pursuing the Clinton Foundation probe during the election season," The Journal reports.

News also leaked this year that the FBI was investigating Mr. McAuliffe, who in addition to being a political ally also served as a board member of the Clinton Global Initiative, an endeavor of the family's charitable foundation.

News reports from May indicated that the investigation involved $120,000 worth of donations made to Mr. McAuliffe's 2013 campaign by Chinese businessman Wang Wenliang. Mr. Wang's companies also donated $1 million to $5 million to the Clinton Foundation, and investigators were reportedly probing the legality of the campaign contributions.

When news of the probe leaked in May, Mr. McAuliffe said he had "no personal relationship" with Mr. Wang and that a team of lawyers vetted his campaign donations, finding that Mr. Wang had held a green card since 2007, making him eligible to donate.

The Washington Post reported this week that federal investigators have also been looking into Mr. McAuliffe's time on the board of the foundation.

Analysts say the sheer number of investigations surrounding Mrs. Clinton will raise questions in the minds of voters. Because those investigations are likely to continue into next year, they could dog Mrs. Clinton if she wins the White House.

Rep. Jason Chaffetz, Utah Republican and chairman of the House Oversight and Government Reform Committee, has already said there is plenty of room for investigations.

Mr. Jenks, the SMU professor, said that could immediately strain relations between Congress and Mrs. Clinton and her staff.

"It's going to be painful," he said.

Metro.co.uk
Russian hackers have launched repeated cyber attacks on UK government intranet, senior source says
Tuesday, 01 November 2016
Byline: Toby Meyjes

London - Russian hackers have launched sustained cyber attacks on the UK government intranet, a senior source has revealed, amid growing tensions between the countries.
The hackers have tried repeatedly to access the government's intranet, the source told metro.co.uk, as well as disrupt the gov.uk web addresses its various departments use.

It is understood that the attacks have targeted all government departments rather than one in particular and the threat posed by Russian cyber attacks is one of the biggest the UK government faces.

It comes on the same day the director general of MI5 Andrew Parker said the Kremlin was becoming 'increasingly aggressive' in its approach to its foreign policy, including cyber attacks.

And just last week it was feared an attack had been launched on the government website after it crashed on more than one occasion, although it is understood this was due to a coding error.

The government has not directly commented on the threats to the intranet but they do tally with Mr Parker's claim that Russia had been carrying out a 'high volume' of 'out of sight' activity.

He told the Guardian: 'It is using its whole range of state organs and powers to push its foreign policy abroad in increasingly aggressive ways - involving propaganda, espionage, subversion and cyber- attacks.

'Russia is at work across Europe and in the UK today. It is MI5's job to get in the way of that.'

But those claims were denied by Kremlin spokesman Dmitry Peskov who said they do not 'correspond to reality'.

He said: 'We do not agree with them, and claims regarding cyber-attacks we have already commented on.

'No-one has yet given any evidence so we cannot consider claims that are not founded on evidence.'

Metro.co.uk did approach the Kremlin about the specific allegations but has not yet had a response.

The head of MI5's claims come as the Investigatory Powers Bill returned to the House of Commons on Tuesday so MPs could consider amendments made by peers.

Ministers are determined to complete the Bill's passage through Parliament by the end of the year, when many of the spying powers in the compromise Data Retention and Investigatory Powers Act 2014 expire.

Elsewhere, Chancellor Philip Hammond unveiled the Government's new cyber-security strategy, insisting the UK would 'strike back' if it comes under attack.

Part of the strategy will see increased funding for the education of IT professions on the threats facing the UK.

James Tolfree, from Cryptzone, said the Government's apparent change in thinking was positive for UK cyber security.

US News and World Report

Clinton Emails Could Help ex-NSA Contractor Who Took Terabytes Home, Attorneys Say
Tuesday, 01 November 2016
Byline: Steven Nelson

Washington - In the four years Hillary Clinton sent and received State Department correspondence using a private and insecure email system, Harold T. Martin III allegedly stockpiled classified information inside his Maryland home and an unlocked shed.
Martin faces charges for alleged theft of government documents and mishandling classified information that carry up to 11 years in prison, and he's been behind bars since his August arrest, with prosecutors saying they intend to file more serious Espionage Act charges, often used by the Obama administration to go after leakers and whistleblowers.

Though prosecutors have not alleged the now-fired Booz Allen Hamilton contractor -- who worked for the National Security Agency six years before a transfer to the Pentagon last year -- is a spy or that he shared the information or allowed it to be accessed by a third party, they do allege he could be responsible for one of the largest security violations ever and knowingly mishandled classified records working various jobs over two decades.

Defense attorneys for prominent whistleblowers, accused leakers and careless clearance-holders say that unless more damning evidence emerges they could see Martin making a successful plea for leniency by pointing to the Justice Department's decision this summer not to prosecute Clinton.

There are, of course, key differences in the cases, with volume the most glaring. The FBI found that Clinton, the Democratic nominee for president, sent or received 110 emails that had classified information at the time they were sent, with eight email threads containing top secret information. Martin, by contrast, allegedly had many printed pages marked as being classified and 50 terabytes of potentially classified data (equivalent to roughly 500 million pages), much of it believed to be considered top secret.

Martin also allegedly confessed knowing he was not allowed to take the information home and that he initially lied to investigators. Clinton, by contrast, insists she never knowingly sent or received classified information using her private email server and repeatedly told the FBI she could not recall specifics.

"The Clinton case and the Martin [case] do have different facts. However, it is problematic that the severity of punishment in these cases has been based not on the facts of each case, but whether or not the accused is powerful and politically connected," says Jesselyn Radack, an attorney who has represented whistleblowers Edward Snowden, Thomas Drake and John Kiriakou.

"The defense could seek leniency given the conclusion in the Clinton email case that extreme carelessness was not enough for charges," she says.

Indeed, after the FBI announced in July that it would not recommend charges against Clinton, some defense attorneys said they would seek "the Clinton deal," a sarcastic term meaning leniency for alleged misconduct.

FBI Director James Comey said in July that Clinton was "extremely careless" and had put classified information at risk of interception, but that the bureau could not establish that she intentionally mishandled records, and that without intent "no reasonable prosecutor" would bring a case. He subsequently told Congress that Clinton lied to the public, but not the bureau -- a crime that ensnares many defendants.

The first test of the so-called "Clinton deal" defense came in August when former Navy machinist mate Kristian Saucier unsuccessfully requested probation after admitting he took photos of a nuclear submarine. He was sentenced to one year in prison for unlawfully retaining national defense information by keeping the photos, which were discovered on an old phone at a landfill.

Saucier is currently in prison for the photos, which he insisted were taken as innocent keepsakes to show his future children, but his attorneys say a forceful push to connect Saucier's case to Clinton's may have worked. The judge, who rebuffed a six-year sentence requested by prosecutors, noted the comparison from the bench.

"Whether it worked or not is up in the air... was there some leniency based on that? I don't know, it's possible," says Greg Rinckey, one of Saucier's attorneys.

As Martin is accused of doing, Saucier admitted he knew he was not allowed to take the photos and that he initially lied to investigators. He also admitted destroying evidence.

Rinckey says a clear takeaway for low-level officials unacquainted with criminal investigations is that they should not answer interrogator questions without an attorney present. Sometimes they mistakenly believe they can talk their way out of trouble, he says, and in so doing provide evidence against themselves.

"I think this Clinton defense would be used in this NSA individual's case on sentencing. Is it going to protect him from being convicted? No. But on sentencing is it going to be used? I think it will be," Rinckey says.

Another test of the "Clinton deal" defense is approaching as Marine Reserves Maj. Jason Brezler challenges the military's decision to fire him for storing on his personal computer a report about a corrupt Afghan official, which he sent as a warning to troops before an apparent sexual abuse victim of the official murdered three Marines.

Mark Zaid, a defense attorney who has represented many whistleblowers and people accused of mishandling classified information, says he could see Martin's attorneys being successful citing Clinton when asking for a lower sentence.

Examples of powerful people accused of mishandling records can help put the case into context, Zaid says.

Zaid says he secured a "Petraeus deal" for a client -- probation and a fine -- after former CIA Director David Petraeus was given that penalty last year when he admitted providing highly classified information to a biographer with whom he was having an affair and then lying about it to the FBI.

Zaid says many people with security clearances are accused of improperly taking home records, either for personal reasons or to finish work assignments on a deadline, but that the massive scale of Martin's stash points to intent. He says his client who cited Petraeus, who he declined to name, took home classified information to read, some of it dating back to the Cold War.

"It's unfortunate that the courts tend to look at the smaller fries as the ones to try to set the bigger examples," Zaid says. "What I'd like to see is the higher ups are leading by example and their punishment is meant to send a signal to everyone beneath them."

James Wyda, a federal public defender representing Martin, did not respond to a request for comment, but in court filings has described him as a patriot who did not damage U.S. national security.

Martin reportedly was caught when authorities investigated the theft of computer code from the NSA that was posted online earlier this year by the Shadow Brokers, an individual or group that offered additional code for sale before calling off an auction.

Prosecutors have given some hints that Martin may be more than a classic hoarder. In arguing against pre-trial release, they note although he does not have a valid passport, he did have 10 guns -- some previously unknown to his wife and including a loaded handgun in his car. Also in his car, authorities found "a printed email chain marked as 'Top Secret' and containing highly sensitive information."

On the back of the printed emails are "handwritten notes describing the NSA's classified computer infrastructure and detailed descriptions of classified technical operations," prosecutors said, as well as "descriptions of the most basic concepts associated with classified operations, as if the notes were intended for an audience outside of the intelligence community unfamiliar with the details of its operations."

"The Hillary Clinton story isn't over yet," Rinckey adds. "It's going to depend on what they find on Anthony Weiner and Huma [Abedin]'s laptop."

The FBI informed Congress on Friday that it is reviewing additional emails that may be relevant to the Clinton email probe. Those emails reportedly were found on a computer used by Weiner, the estranged husband of top Clinton aide Abedin. Weiner resigned from Congress in 2011 after tweeting a photo of his crotch. After repeatedly sending sexual messages on Twitter, he came under FBI investigation for communications with a minor.

The Guardian (London)
UK must build cyber-attack capability, chancellor says
Tuesday, 01 November 2016
Byline: Jessica Elgot

London - The UK must strike back at hostile states in cyberspace and be capable of mounting sophisticated cyber-attacks of its own in place of military strikes, the chancellor has said.
Philip Hammond said that unless the UK could match the cyber-attack abilities of foreign rogue states, the alternatives would only be to ignore digital attacks on Britain's infrastructure or use military force.

Launching the government's £1.9bn national cybersecurity strategy, Hammond said the UK had to develop "fully functioning cyber-attack capability".

He said: "If we do not have the ability to respond in cyberspace to an attack that takes down our power networks, leaving us in darkness, or our air traffic control, leaving us in darkness, we would be left with the impossible choice of turning the other cheek and ignoring the devastating consequences or resorting to a military response."

Hammond said the world's next great conflict was likely to at least begin in cyberspace, before guns were loaded.

"There is no doubt in my mind that the precursor to any future state-on-state conflict will be a campaign of escalating cyber-attacks, to break down our defences and test our resolve before the first shot is fired," he said in a speech on Tuesday at Microsoft's Future Decoded conference.

Hostile states appeared to believe cyber-attacks were far less risky, Hammond said. "Kinetic attacks carry huge risk of retaliation and may breach international law, but in cyberspace those who want to harm us appear to think that they can act scalably and deniably," he said.

Hammond said the new funding, which doubles the amount set out in 2011 in a similar strategy, will "allow us to take even greater steps to defend ourselves in cyberspace and to strike back when we are attacked".

Speaking before the launch, Cabinet Office minister Ben Gummer said cyber warfare was "no longer the stuff of spy thrillers and action movies ... Our adversaries are varied - organised criminal groups, 'hacktivists', untrained teenagers and foreign states."

The funds will focus on defences for critical infrastructure such as energy and transport. Websites impersonating government departments will be shut down much more quickly, and efforts will be made to crack down on spoof email accounts used in fraud cases. The reforms include a new cyber-innovation centre in Cheltenham.

Hammond's announcement came as Russia rebuffed claims made to the Guardian by the head of MI5, Andrew Parker, that the Kremlin is behind hostile manoeuvres against Britain.

Parker told the Guardian that Moscow was "using its whole range of state organs and powers to push its foreign policy abroad in increasingly aggressive ways - involving propaganda, espionage, subversion and cyber-attacks. Russia is at work across Europe and in the UK today. It is MI5's job to get in the way of that."

"Those words do not correspond to reality," said Kremlin spokesman Dmitry Peskov on Tuesday. "Until someone produces proof, we will consider those statements unfounded and groundless."

US News and World Report
Clinton Emails Could Help ex-NSA Contractor Who Took Terabytes Home, Attorneys Say
Tuesday, 01 November 2016
Byline: Steven Nelson

Washington - In the four years Hillary Clinton sent and received State Department correspondence using a private and insecure email system, Harold T. Martin III allegedly stockpiled classified information inside his Maryland home and an unlocked shed.
Martin faces charges for alleged theft of government documents and mishandling classified information that carry up to 11 years in prison, and he's been behind bars since his August arrest, with prosecutors saying they intend to file more serious Espionage Act charges, often used by the Obama administration to go after leakers and whistleblowers.

Though prosecutors have not alleged the now-fired Booz Allen Hamilton contractor -- who worked for the National Security Agency six years before a transfer to the Pentagon last year -- is a spy or that he shared the information or allowed it to be accessed by a third party, they do allege he could be responsible for one of the largest security violations ever and knowingly mishandled classified records working various jobs over two decades.

Defense attorneys for prominent whistleblowers, accused leakers and careless clearance-holders say that unless more damning evidence emerges they could see Martin making a successful plea for leniency by pointing to the Justice Department's decision this summer not to prosecute Clinton.

There are, of course, key differences in the cases, with volume the most glaring. The FBI found that Clinton, the Democratic nominee for president, sent or received 110 emails that had classified information at the time they were sent, with eight email threads containing top secret information. Martin, by contrast, allegedly had many printed pages marked as being classified and 50 terabytes of potentially classified data (equivalent to roughly 500 million pages), much of it believed to be considered top secret.

Martin also allegedly confessed knowing he was not allowed to take the information home and that he initially lied to investigators. Clinton, by contrast, insists she never knowingly sent or received classified information using her private email server and repeatedly told the FBI she could not recall specifics.

"The Clinton case and the Martin [case] do have different facts. However, it is problematic that the severity of punishment in these cases has been based not on the facts of each case, but whether or not the accused is powerful and politically connected," says Jesselyn Radack, an attorney who has represented whistleblowers Edward Snowden, Thomas Drake and John Kiriakou.

"The defense could seek leniency given the conclusion in the Clinton email case that extreme carelessness was not enough for charges," she says.

Indeed, after the FBI announced in July that it would not recommend charges against Clinton, some defense attorneys said they would seek "the Clinton deal," a sarcastic term meaning leniency for alleged misconduct.

FBI Director James Comey said in July that Clinton was "extremely careless" and had put classified information at risk of interception, but that the bureau could not establish that she intentionally mishandled records, and that without intent "no reasonable prosecutor" would bring a case. He subsequently told Congress that Clinton lied to the public, but not the bureau -- a crime that ensnares many defendants.

The first test of the so-called "Clinton deal" defense came in August when former Navy machinist mate Kristian Saucier unsuccessfully requested probation after admitting he took photos of a nuclear submarine. He was sentenced to one year in prison for unlawfully retaining national defense information by keeping the photos, which were discovered on an old phone at a landfill.

Saucier is currently in prison for the photos, which he insisted were taken as innocent keepsakes to show his future children, but his attorneys say a forceful push to connect Saucier's case to Clinton's may have worked. The judge, who rebuffed a six-year sentence requested by prosecutors, noted the comparison from the bench.

"Whether it worked or not is up in the air... was there some leniency based on that? I don't know, it's possible," says Greg Rinckey, one of Saucier's attorneys.

As Martin is accused of doing, Saucier admitted he knew he was not allowed to take the photos and that he initially lied to investigators. He also admitted destroying evidence.

Rinckey says a clear takeaway for low-level officials unacquainted with criminal investigations is that they should not answer interrogator questions without an attorney present. Sometimes they mistakenly believe they can talk their way out of trouble, he says, and in so doing provide evidence against themselves.

"I think this Clinton defense would be used in this NSA individual's case on sentencing. Is it going to protect him from being convicted? No. But on sentencing is it going to be used? I think it will be," Rinckey says.

Another test of the "Clinton deal" defense is approaching as Marine Reserves Maj. Jason Brezler challenges the military's decision to fire him for storing on his personal computer a report about a corrupt Afghan official, which he sent as a warning to troops before an apparent sexual abuse victim of the official murdered three Marines.

Mark Zaid, a defense attorney who has represented many whistleblowers and people accused of mishandling classified information, says he could see Martin's attorneys being successful citing Clinton when asking for a lower sentence.

Examples of powerful people accused of mishandling records can help put the case into context, Zaid says.

Zaid says he secured a "Petraeus deal" for a client -- probation and a fine -- after former CIA Director David Petraeus was given that penalty last year when he admitted providing highly classified information to a biographer with whom he was having an affair and then lying about it to the FBI.

Zaid says many people with security clearances are accused of improperly taking home records, either for personal reasons or to finish work assignments on a deadline, but that the massive scale of Martin's stash points to intent. He says his client who cited Petraeus, who he declined to name, took home classified information to read, some of it dating back to the Cold War.

"It's unfortunate that the courts tend to look at the smaller fries as the ones to try to set the bigger examples," Zaid says. "What I'd like to see is the higher ups are leading by example and their punishment is meant to send a signal to everyone beneath them."

James Wyda, a federal public defender representing Martin, did not respond to a request for comment, but in court filings has described him as a patriot who did not damage U.S. national security.

Martin reportedly was caught when authorities investigated the theft of computer code from the NSA that was posted online earlier this year by the Shadow Brokers, an individual or group that offered additional code for sale before calling off an auction.

Prosecutors have given some hints that Martin may be more than a classic hoarder. In arguing against pre-trial release, they note although he does not have a valid passport, he did have 10 guns -- some previously unknown to his wife and including a loaded handgun in his car. Also in his car, authorities found "a printed email chain marked as 'Top Secret' and containing highly sensitive information."

On the back of the printed emails are "handwritten notes describing the NSA's classified computer infrastructure and detailed descriptions of classified technical operations," prosecutors said, as well as "descriptions of the most basic concepts associated with classified operations, as if the notes were intended for an audience outside of the intelligence community unfamiliar with the details of its operations."

"The Hillary Clinton story isn't over yet," Rinckey adds. "It's going to depend on what they find on Anthony Weiner and Huma [Abedin]'s laptop."

The FBI informed Congress on Friday that it is reviewing additional emails that may be relevant to the Clinton email probe. Those emails reportedly were found on a computer used by Weiner, the estranged husband of top Clinton aide Abedin. Weiner resigned from Congress in 2011 after tweeting a photo of his crotch. After repeatedly sending sexual messages on Twitter, he came under FBI investigation for communications with a minor.

The Guardian (London)
UK must build cyber-attack capability, chancellor says
Tuesday, 01 November 2016
Byline: Jessica Elgot

London - The UK must strike back at hostile states in cyberspace and be capable of mounting sophisticated cyber-attacks of its own in place of military strikes, the chancellor has said.
Philip Hammond said that unless the UK could match the cyber-attack abilities of foreign rogue states, the alternatives would only be to ignore digital attacks on Britain's infrastructure or use military force.

Launching the government's £1.9bn national cybersecurity strategy, Hammond said the UK had to develop "fully functioning cyber-attack capability".

He said: "If we do not have the ability to respond in cyberspace to an attack that takes down our power networks, leaving us in darkness, or our air traffic control, leaving us in darkness, we would be left with the impossible choice of turning the other cheek and ignoring the devastating consequences or resorting to a military response."

Hammond said the world's next great conflict was likely to at least begin in cyberspace, before guns were loaded.

"There is no doubt in my mind that the precursor to any future state-on-state conflict will be a campaign of escalating cyber-attacks, to break down our defences and test our resolve before the first shot is fired," he said in a speech on Tuesday at Microsoft's Future Decoded conference.

Hostile states appeared to believe cyber-attacks were far less risky, Hammond said. "Kinetic attacks carry huge risk of retaliation and may breach international law, but in cyberspace those who want to harm us appear to think that they can act scalably and deniably," he said.

Hammond said the new funding, which doubles the amount set out in 2011 in a similar strategy, will "allow us to take even greater steps to defend ourselves in cyberspace and to strike back when we are attacked".

Speaking before the launch, Cabinet Office minister Ben Gummer said cyber warfare was "no longer the stuff of spy thrillers and action movies ... Our adversaries are varied - organised criminal groups, 'hacktivists', untrained teenagers and foreign states."

The funds will focus on defences for critical infrastructure such as energy and transport. Websites impersonating government departments will be shut down much more quickly, and efforts will be made to crack down on spoof email accounts used in fraud cases. The reforms include a new cyber-innovation centre in Cheltenham.

Hammond's announcement came as Russia rebuffed claims made to the Guardian by the head of MI5, Andrew Parker, that the Kremlin is behind hostile manoeuvres against Britain.

Parker told the Guardian that Moscow was "using its whole range of state organs and powers to push its foreign policy abroad in increasingly aggressive ways - involving propaganda, espionage, subversion and cyber-attacks. Russia is at work across Europe and in the UK today. It is MI5's job to get in the way of that."

"Those words do not correspond to reality," said Kremlin spokesman Dmitry Peskov on Tuesday. "Until someone produces proof, we will consider those statements unfounded and groundless."

La Dépêche du Midi
Pourquoi un tel fichier ? Que contient-il ? Qui peut le consulter ? Quelle conservation ?
Wednesday, 02 November 2016
Byline: Journaliste maison

Paris - Le fichier des « Titres électroniques sécurisés » (TES) vise à remplacer deux fichiers existants : le Fichier national de gestion (FNG) relatif aux cartes nationales d'identité et celui du système TES lié à la délivrance des passeports. Le nouveau fichier qui a été créé par le décret n° 2016-1 460 du 28 octobre 2016 collectera toutefois davantage de données que les deux fichiers qu'il remplacera (lire ci-contre). L'un des objectifs affichés par le gouvernement est de lutter contre la fraude et ce dernier assure qu'il n'y aura pas d'identification administrative, mais une authentification automatisée et élargie.
Les données pourront être consultées par les agents chargés de réaliser les documents mais aussi par une très impressionnante liste de personnes, « pour les besoins exclusifs de leurs missions. ». Ainsi les agents des services de la police nationale et les militaires des unités de la gendarmerie nationale chargés des missions de prévention et de répression des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme, individuellement désignés et dûment habilités auront accès au fichier. Idem pour les agents des services spécialisés du renseignement. Idem pour les agents de la direction centrale de la police judiciaire, individuellement désignés et dûment habilités (à l'exclusion de l'image numérisée des empreintes digitales). Les données pourront être par ailleurs partagées par le système de sécurité de Schengen et par Interpol. « Dans le cadre de ces échanges, des données à caractère personnel peuvent être transmises aux autorités compétentes des États membres d'Interpol aux seules fins de confirmer l'exactitude et la pertinence du signalement d'un titre perdu, volé ou invalidé. »

Les informations contenues dans le TES seront conservées pendant 15 ans pour les passeports et 20 ans pour les cartes d'identité (10 ans et de 15 ans lorsque le titulaire du titre est un mineur).

Les données relatives au demandeur ou au titulaire du titre. Il s'agit là du nom de famille, du nom d'usage, des prénoms; de la date et lieu de naissance; du sexe; de la couleur des yeux; de la taille; du domicile ou de la résidence ou, le cas échéant, de la commune de rattachement de l'intéressé ou de l'adresse de l'organisme d'accueil auprès duquel la personne est domiciliée; des données relatives à sa filiation (les noms, prénoms, dates et lieux de naissance de ses parents, leur nationalité). Il y a aussi le cas échéant, le document attestant de la qualité du représentant légal lorsque le titulaire du titre est un mineur ou un majeur placé sous tutelle; l'image numérisée du visage et celle des empreintes digitales qui peuvent être légalement recueillies; l'image numérisée de la signature du demandeur de la carte nationale d'identité; l'adresse de messagerie électronique et les coordonnées téléphoniques du demandeur (lorsque celui-ci a choisi d'effectuer une pré-demande de titre en ligne ou a demandé à bénéficier de l'envoi postal sécurisé, ou sur déclaration de l'usager lorsqu'il souhaite être informé par ce moyen de la disponibilité de son titre). Le cas échéant, le code de connexion délivré par l'administration au demandeur pour lui permettre de déclarer la réception de son passeport lorsque ce titre lui a été adressé par courrier sécurisé.

Les informations relatives au titre d'identité. Il s'agit du numéro du titre; du type de titre; du tarif du droit de timbre; de la date et du lieu de délivrance; de l'autorité de délivrance; de la date d'expiration. Le fichier TES peut aussi mentionner, avec la date, l'invalidation du titre et son motif (perte, vol, retrait, interdiction de sortie du territoire, autre motif), la restitution du titre à l'administration, sa destruction. Le fichier mentionne également les justificatifs présentés à l'appui de la demande de titre. D'autres données techniques sur l'établissement, la demande et la remise du titre sont inscrites dans le fichier.

Les données relatives au fabricant du titre et aux agents chargés de la délivrance du titre. Il s'agit là de répertorier les nom, prénom et références de l'agent qui enregistre la demande de titre; l'identifiant du fabricant du titre.

Enfin, le ficher comporte l' image numérisée des pièces du dossier de demande de titre.

South China Morning Post
Cyber law aimed at foreign hackers
Tuesday, 01 November 2016
Byline: Viola Zhou

Beijing - Beijing has proposed a revised internet law to punish foreigners who hack Chinese websites as it steps up its campaign against cyberattacks it blames on the West.
Although it was hard for governments to identify those behind cybercrimes, the move paved the way for China to take legal action against other states, analysts said.

The proposed cybersecurity law changes would let the government freeze assets of foreign individuals or groups if they damaged China's key information infrastructure, Xinhua reported. Police would apply "other necessary punishment" to those outside the country who attacked, intruded, disrupted or harmed Chinese websites, according to the revised draft quoted in the report.

The draft had been sent to the Standing Committee of the National People's Congress for approval, Xinhua said.

China claims to be a victim of global cybercrimes, reporting growing numbers of attacks from overseas every year. Last year, authorities found more than 64,000 "control points" that had been controlling Chinese websites with malware from abroad, a 52 per cent rise from 2014, according to a government website.

In 2013, Xinhua called the US the top source of hackers who planted malware in its servers.

Hong Kong security analyst Michael Gazeley said hackers usually launched attacks through other people's servers so it was hard to bring them to justice.

Beijing denies Washington's claims that it is behind cyberattacks on US government, military and corporate computers.

In 2014, China accused the US Justice Department of "fabricating facts" after it charged five members of the PLA over attacks on six US corporations.

Liu Deliang, an internet law professor at Beijing University of Posts and Telecommunication, said that while it was difficult to freeze hackers' assets, the threat of doing so was a warning to institutions and countries that might launch cyberattacks on China.

Khaleej Times
Hackers turn to connected devices to launch attacks
Tuesday, 01 November 2016
Byline: Bernd Debusmann Jr.

Dubai - Cyber security experts warn that the rapid proliferation of cameras and other "Internet of Things" (IoT) devices may mean an increase in cyber attacks as the world - particularly the UAE - moves towards the concepts of "smart cities".
Such fears were starkly highlighted earlier in October, when hijackers used hundreds of thousands of Internet-connected household devices and cameras to launch a devastating cyber attack in which many popular websites, including Twitter, Netflix, Amazon and the New York Times were significantly slowed down or completely knocked offline.

In a separate incident, in September 145,000 hacked cameras were used to bring down security news website KrebsOnSecurity for over 24 hours.

"The Internet of Things has become a crucial part of our day-to-day activities, especially with the introduction of what we call smart cities, such as is the trend in Dubai and the UAE," said Mohammed Abukhater, Regional Director for the Middle East and North Africa at FireEye, a security company. "Aside from all of the good things the Internet of Things brings to us, such as cameras and connected devices ... all of them have a risk."

"Most people are not aware of the risk," he added. "But recent attacks have specifically targeted simple devices that are connected to the Internet. Those then can be utilised to attack more important or more sensitive websites or organisations."

Abukhater noted cyber criminals and hackers have increasingly turned to connected devices as platforms for their attacks, as they lack sophisticated security measures.

"These are simple devices that give benefits to people, but they are lacking security measures," he noted. "From a vendor's point of view, they need to quickly meet people's needs so they introduce easy-to-manage devices."

"These are good targets for attackers to use in many ways," he added. "Some of them can use them to generate massive amounts of junk data that can be directed to important websites, and overwhelm servers."

Abukhater noted that there is a variety of motives for such cyber attacks. In some cases, it could be politically motivated. In other cases, the primary motive could be theft. In one recent instance, hackers managed to overwhelm a jewellery shop's security system, allowing thieves to enter.

Additionally, Abukhater noted that the massive proliferation of Internet-enabled security cameras may mean an increase in cyber attacks in the UAE. According to market research company 6Wresearch, the market for surveillance cameras in the UAE will rise to $197.8 million by 2021.

"This shift puts us at risk of being targeted by hackers, for personal reasons, political reasons, or even state-sponsored attacks," he said.

"But the good thing here is that the government of the UAE and Dubai are putting very good protection measures," he added. "But you can never guarantee a 100 per cent secured environment against such hackers."

Gulf News
IT security spend in Mena to reach $1.3b this year
Tuesday, 01 November 2016
Byline: Naushad K. Cherrayil

Dubai - Spending on Information security technology and services is on pace to reach $1.3 billion in 2016 in the Middle East and North Africa, an increase of eight per cent over 2015.
Greg Young, research vice- president at Gartner, said that increased awareness about the business impact of security incidents is causing organisations to focus their security strategy on detection and response approaches, which is driving this growth.

"Enterprises in the region are the targets of some of the world's most advanced attacks, as well as the highest rate of attacks. Organisations are trying to increase detection, blocking, and advanced defences while faced with limited availability in the security workforce," he said.

According to recent stats, the UAE is now the second most targeted country after the US. However, Young said that spending growth is not that great when compared to last year, and it is not that organisations are investing much but the organisations can consume only this much.

There is a big shortage in skilled workforce and approximately 50 per cent of positions are going unfilled. About 86 per cent of senior IT and business professionals believe there is a shortage. It takes longer to hire them and they don't stay that long, he said.

By 2019, Gartner expects 30 per cent of large enterprises to increase their security consulting services as they transition into digital business.

"Large organisations in the region continue to invest in building out security operations capabilities either in house or by leveraging external services offered by managed security services providers," he said.

He said that organisations recognise the inevitable adoption of cloud and virtual IT and shift their defences to an adaptive security architecture. Organisations should look for, and secure, shadow IT whereby IT has been adopted outside the normal IT procurement and management processes.

Gartner expects a third of successful attacks experienced by enterprises will be on their shadow IT resources by 2020.

He said that targeted attacks, ransomware and denial of service attacks are the most relevant threats to enterprise today, however they are enabled by failing patch vulnerabilities and overloading security personal with alerts.

"99.9 per cent of attacks in the coming years will be based on product vulnerabilities that were known for at least a year by security and IT professionals," he said.

CNBC
FBI's Comey opposed naming Russians, citing election timing: Source
Tuesday, 01 November 2016
Byline: Eamon Javers

Washington - FBI Director James Comey argued privately that it was too close to Election Day for the United States government to name Russia as meddling in the U.S. election and ultimately ensured that the FBI's name was not on the document that the U.S. government put out, a former bureau official tells CNBC.
The official said some government insiders are perplexed as to why Comey would have election timing concerns with the Russian disclosure but not with the Huma Abedin email discovery disclosure he made Friday.

In the end, the Department of Homeland Security and The Office of the Director of National Intelligence issued the statement on Oct. 7, saying: "The U.S. intelligence community is confident that the Russian

Government directed the recent compromises of emails from U.S. persons and institutions, including from U.S. political organizations. ... These thefts and disclosures are intended to interfere with the U.S. election process."

An FBI spokesperson declined to comment on Comey's role in the decision- making surrounding the Oct. 7 statement.

According to the former official, Comey agreed with the conclusion the intelligence community came to: "A foreign power was trying to undermine the election. He believed it to be true, but was against putting it out before the election." Comey's position, this official said, was "if it is said, it shouldn't come from the FBI, which as you'll recall it did not."

Comey took a different approach toward releasing information about the discovery of emails on a laptop that was used by former congressman Anthony Weiner and his estranged wife Huma Abedin, the official said.

"By doing a press conference, and personally testifying and giving his opinion about the conduct, he made this about James Comey and his credibility," the official said. "You can see why he did it, from his perspective, once he had had that press conference."

The official said FBI investigators can get a "preliminary read" of the newly discovered emails within a couple of days and come to an initial conclusion about whether there is classified material in the files. "The questions is whether they will decide to share that read or not," the official said. "Normally in the FBI we would not, but we're not in normal land anymore."

Comey's decision to announce the new investigative steps has come under severe criticism from Democrats, including Hillary Clinton who addressed the issue at a rally Monday.

"I'm sure a lot of you may be asking what this new email story is about and why in the world the FBI would decide to jump into an election with no evidence of any wrongdoing with just days to go. That's a good question," Clinton said. "I am sure they will reach the same conclusion they did when they looked at my emails for the last year. There is no case here."

The Donald Trump campaign, meanwhile, has praised Comey for continuing to investigate Clinton. "The right thing to do is whatever the FBI thinks," said Trump campaign manager Kellyanne Conway on CNBC Monday morning. "It's not for us to say speed it up because of the election or slow it down because of the election."

BBC News
UK to increase national cyber-defence grid
Tuesday, 01 November 2016

Byline: Staff report

London - Automatic defences to stop hackers hijacking websites or spoofing official domains will get a boost from a £1.9bn government cybersecurity strategy.
Chancellor Philip Hammond will give details of the plans in a speech later.

Other defences that intercept booby-trapped emails or shut down thieves impersonating bank websites will also be expanded.

The strategy will also help enlarge specialist police units that tackle organised online gangs.

Some cash will go towards education and training of cybersecurity experts.

Mr Hammond is expected to formally launch the scheme, called the National Cyber Security Strategy, on Tuesday.

The plans will set out action needed to protect the UK economy and the privacy of British citizens, and will also encourage industry to ramp up efforts to prevent cyber-attacks.

Mr Hammond said Britain "must now keep up with the scale and pace of the threats we face".

"Our new strategy... will allow us to take even greater steps to defend ourselves in cyberspace and to strike back when we are attacked," he added.

Ben Gummer, paymaster general, said in a statement: "No longer the stuff of spy thrillers and action movies, cyber-attacks are a reality and they are happening now.

"Our adversaries are varied - organised criminal groups, 'hacktivists', untrained teenagers and foreign states."

Finding talent

The £1.9bn to pay for the national strategy was allocated last year and will fund the programme until the end of 2020.

In its strategy, the government explained what some of the money has been spent on already.

With the aid of industry, it has set up automated systems that limit how much malware and spam reaches UK citizens. Other projects have helped the government verify where emails come from to thwart specific tax fraud campaigns aimed at the UK.

Future spending plans involved cash for recruiting more than 50 specialists who will work at the cybercrime unit at the National Crime Agency. These will help tackle organised gangs and aim to raise the cost of engaging in hi-tech crime to make it much less attractive.

The cyber-plan will also involve the creation of a Cyber Security Research Institute that aims to unite researchers across the UK's universities to work together on improving defences for smartphones, laptops and tablets.

Security-based start-ups will also get help via an innovation fund that will commercialise work on novel tools and defences.

A national scheme will also be set up to retrain "high-aptitude professionals" as cybersecurity experts.

Prof Alan Woodward, a computer security expert from the University of Surrey, said he hoped the government spent cash on the "high volume, low sophistication attacks" that plague people and cause the majority of financial losses.

"I hope the £1.9bn will be spent in growing talent," he said. "The government talk about 50 recruits here and 50 there. I'm afraid we need many more."

Prof Woodward said it was getting "increasingly difficult" to persuade young people to study computer science and getting them to try cybersecurity was "a real headache".

"I would really like to see money put into reaching young people early enough to influence the subjects they decide upon at school and pairing an image for them of just how interesting and rewarding a career in cybersecurity can be," he said.

The Guardian (London)
Philip Hammond to spend extra £1.9bn fighting cyber-attacks
Tuesday, 01 November 2016
Byline: Anushka Asthana, Jessica Elgot

London - Outdated computer systems are allowing malicious hackers to target everyone from companies at board level to individuals in their living rooms, according to the chancellor, who is promising to strike back against cyber-attacks.
Philip Hammond will use a speech on Tuesday to unveil a £1.9bn package designed to boost Britain's defences against a growing online threat, which he will say is invading personal privacy and putting national security at risk.

Speaking before the launch, Hammond said Britain must "keep up with the scale and pace of the threats we face" and insisted that the new funding will "allow us to take even greater steps to defend ourselves in cyberspace and to strike back when we are attacked".

The money - which almost doubles the amount set out for a similar strategy in 2011 - will be used to improve automated defences to safeguard citizens and businesses, support the cybersecurity industry and deter attacks from criminals and "hostile actors".

Hammond will say the steps are needed because the cost of crimes in cyberspace globally is $445bn (£365bn), and will argue that society is becoming more vulnerable because of the way in which devices connect.

The government also fears that "old legacy IT systems used by many organisations in the UK" are increasingly susceptible to hackers who find them easier to crack.

Hammond will promise government support but insist that chief executives have a duty to ensure their companies are secure.

The Cabinet Office minister, Ben Gummer, said: "No longer the stuff of spy thrillers and action movies, cyber-attacks are a reality and they are happening now. Our adversaries are varied - organised criminal groups, 'hacktivists', untrained teenagers and foreign states.

"The first duty of the government is to keep the nation safe. Any modern state cannot remain secure and prosperous without securing itself in cyberspace. That is why we are taking the decisive action needed to protect our country, our economy and our citizens."

The money for the new national cybersecurity strategy will be used to focus on defence, including protecting critical infrastructure such as energy and transport.

It is intended that websites impersonating government departments will be shut down much more quickly, and efforts will be made to crack down on spoof email accounts used in fraud cases.

The second plank of the policy will be to target those who persistently attack Britain, with a promise to deploy more than 50 specialist cybercrime investigators, currently being recruited.

There will also be more funding to improve the security of smartphones, tablets and laptops.

The reforms include a new cyber- innovation centre in Cheltenham.

Tim Berners-Lee, the founder of the world wide web, speaking on Radio 4's Today programme on Tuesday said: "Clearly we have seen the internet can be attacked and the United Kingdom needs to have

strong, but responsible and accountable police forces and GCHQ has to have the tools to defend us and defend the open internet.

"I don't think we'd want to make a first strike, but when you are being attacked by a whole lot of domestic appliances, then the way you defend yourself is striking back, by taking over those machines yourself. On the internet, offence and defence really are very related.

"If you buy something and plug it into the internet, for example your webcam, is that it comes with a password set in a factory. So if you as a consumer buy one and plug it in, you better put a password on it not because someone particularly wants to look in your own house, but because an automated machine could be taking over all webcams."

Le Devoir
Hydro-Québec cherche à se prémunir contre la menace des cyberattaques
Friday, 02 December 2016
Byline: Karl Rettino-Parazelli

Montréal - La société d'État s'associe à une nouvelle chaire de recherche
Les systèmes informatiques d'Hydro-Québec sont souvent la cible de cyberattaques, qui sont pour l'instant demeurées sans conséquences. Face à une menace réelle et croissante, la société d'État a néanmoins senti le besoin de participer à la création d'une chaire de recherche, lancée jeudi à Montréal, pour prévenir les attaques de demain.

L'Université Concordia a annoncé la mise sur pied de la Chaire de recherche industrielle sur la sécurité des réseaux électriques intelligents et les attaques cyberphysiques, qui est notamment le fruit d'un partenariat avec Hydro- Québec et l'entreprise Thales, laquelle se spécialise dans la protection des systèmes informatiques. Elle est dotée d'un budget de 2,2 millions de dollars sur cinq ans, dont 500 000 $ proviennent d'Hydro-Québec.

Protéger le réseau

Le titulaire de la chaire, le professeur Mourad Debbabi, mettra à contribution une équipe de 25 chercheurs pour développer des techniques permettant de détecter, de prévenir et d'atténuer des cyberattaques. L'objectif est d'améliorer la sécurité de l'ensemble du réseau électrique québécois, dit-il.

" Toute plateforme qui intègre des technologies de l'information et de la communication est susceptible d'être attaquée, explique celui qui travaille dans le domaine de la cybersécurité depuis près de 20 ans. Ce n'est pas quelque chose d'hypothétique. C'est une menace qui est réelle. "

"Attaques quotidiennes"

Pour s'en convaincre, note-t-il, on n'a qu'à penser à la cyberattaque qui a paralysé une partie du réseau électrique ukrainien en décembre 2015. L'utilisation d'un logiciel malveillant a plongé dans le noir près de 700 000 personnes, ce qui en ferait la plus importante attaque du genre à survenir dans le monde, estiment les analystes.

" Toute infrastructure qui est pilotée par des logiciels et qui emmagasine des informations variées est la cible d'attaques quotidiennes dans le monde. Hydro-Québec fait partie du lot. Il y a en permanence des tentatives d'intrusion ", affirme sans détour le directeur principal de l'Institut de recherche d'Hydro-Québec, Jérôme Gosset.

" En date d'aujourd'hui, Hydro-Québec n'a pas eu à déplorer de conséquences ", précise-t-il.

La société d'État refuse de dévoiler le nombre de cyberattaques auxquelles elle est confrontée annuellement en invoquant des raisons de sécurité. Elle fait cependant valoir qu'elle met tout en oeuvre pour protéger ses systèmes et bloquer les tentatives d'intrusion.

En bref, les attaques potentielles pourraient généralement prendre deux formes : l'interruption du service, ce qui entraînerait des pannes de courant, ou encore la collecte des données des clients, lesquelles sont par exemple récoltées grâce aux compteurs intelligents.

Dans sa documentation présentant la technologie de ces compteurs de nouvelle génération, Hydro-Québec se montre rassurante en indiquant que " les données transmises sont sécurisées, car elles sont cryptées et anonymes. C'est seulement dans les systèmes d'Hydro-Québec que ces données sont décryptées, puis associées à un client particulier au moyen d'une clé unique. "

" Nous avons tout un tas de systèmes de surveillance et de contrôle pour éviter que des personnes malveillantes ne s'infiltrent, renchérit M. Gosset. Ce qu'on cherche à faire avec la chaire, c'est de préparer l'avenir, de faire évoluer les technologies de défense, de comprendre comment les cyberattaques peuvent évoluer et de préparer des solutions pour garantir la continuité du service. "

Ottawa Citizen
Shared services vows to improve as email project pushed out to 2018
Friday, 02 December 2016
Byline: James Bagnall

Ottawa - For once, Shared Services Canada met its deadline. On Thursday, as promised, the federal government's computer services agency said how it would correct certain deficiencies in its operations identified early this year by Auditor General Michael Ferguson. In a report it delivered to the House of Commons committee for public accounts, the agency promised it would do a better job providing key information-technology services to the 43 departments it deals with, and spelled out the level of service the latter could expect. For instance, government call centres, data centres, email and other telecommunications services are to be available 24 hours a day, 365 days a year - with outages to be fixed in most cases in less than four hours.
But these are statements of intent about services, to be judged later as to progress. Shared Services has yet to finalize its revised plan for actually upgrading the government's electronic backbone, the more difficult part of its mandate. This part of the plan will be presented to the public accounts committee after it wins approval from the Liberal cabinet. It's not clear when that will be.

The report presented Thursday by Shared Services suggests the upgrade overall isn't proceeding well. For one thing, Shared Services is now targeting March 2018 for the delivery of the $400-million government-wide email system that was supposed to have been completed by March 2015. Contractors Bell Canada and CGI Group have encountered a number of technical roadblocks owing in part to revisions in the email platform. This is one of three key jobs assigned to Shared Services.

Not only is Shared Services trying to consolidate 63 email systems into one, it is also decommissioning more than 500 data centres to make way for a handful of super centres, and streamlining government telecommunications services ranging from mobile phones to video conferencing.

The original target for getting all this done was 2020, including the transfer of some 14,000 software applications from old data centres to new ones. Shared Services insiders no longer believe this target can be met.

On top of this, Shared Services is facing the potential loss of part of its mandate.

Treasury Board, the cabinet committee responsible for setting the government's IT policy, finally responded last June to pressure from individual federal departments upset at Shared Services' less-than-stellar progress in modernizing its IT networks.

Treasury Board opened the door to eventually allowing private sector firms such as Amazon Web Services and Microsoft to perform the role of data centre. They would do so by offering pay-as-you-go storage (hosting) services through what the industry calls the cloud - networks of third party computers shared by multiple customers or federal departments.

Details were few but these will be on offer in coming weeks when Shared Services issues a request for proposals for the provision of cloud services. The most likely scenario for the moment is that Shared Services will continue to build and operate its new data centres in Borden, Barrie and Buckingham, Que. Crucially, however, Shared Services would also play the role of broker, which means it would no longer be the monopoly supplier of data services. The agency would vet qualified cloud suppliers and make sure that federal departments' plans for using them are sound.

Shared Services noted Thursday in its response to the auditor general that it "will challenge its customers (federal departments) to build the right cases for using cloud services, while serving as public stewards to ensure that services delivered always meet the government's highest standards of security, availability and value."

The danger for Shared Services is that its 43 customers - the federal departments forced to rely on the agency for data storage - will eventually exercise their right to choose. Exactly when will depend on the soon-to-berevealed cloud services procurement. Treasury Board revised its cloud services policy after commissioning a report from Gartner Group, a consultancy. Gartner was not impressed by Shared Services' ability to keep current on a number of technology fronts. It predicted that even if the agency configured its new data centres to offer cloud services, Shared Services' ability to innovate, reduce costs and react to sudden changes would be "constantly outpaced" by third-party providers such as Amazon Web Services.

There will likely always be a role for Shared Services in storing classified data, but this represents a small minority of the government's total. For the rest, it may have little choice but to compete for the business by trying to get better at what it does. Indeed, there was more than a hint in its response to the auditor general that Shared Services was seeking a role that would secure its place at the centre of the government's IT world.

"Notwithstanding the many challenges, the creation of SSC remains a sound government decision," the agency reminded us Thursday. "The idea that each federal organization would modernize its IT infrastructure by building independent systems one by one is simply not viable," it added.

But, increasingly, Shared Services recognizes that viability also depends on being able to deliver. It has precious few months to show that it can. jbagnall@postmedia.com Twitter.com/JamesBagnall1

Al Jazeera
Qatari news website raises 'censorship' concerns
Friday, 02 December 2016

Doha, Qatar - An English-language news website in Qatar has raised the issue of "censorship" after it was blocked by the country's two internet service providers simultaneously for reasons unknown. Doha News, which has operated for eight years in the capital, said in a statement on Thursday the site's URL has been inaccessible by internet users inside the country since Wednesday - with the exception of those with access to a VPN (virtual private network) or unfiltered corporate internet. The website was available to those outside of Qatar, however.

Omar Chatriwala, a co-founder of Doha News, told Al Jazeera: "We're reaching out to authorities to understand why this has happened. Although there's been no public or official comment on the matter, our initial discussions with them have indicated this won't be immediately resolved."

The two internet service providers, Vodafone Qatar and state-controlled Ooredoo, declined to comment.

Earlier, when the site's administrators tried to divert followers to another domain name, the new URL was also blocked soon after, the Doha News statement said. "We are incredibly disappointed with this decision, which appears to be an act of censorship," it said.

There was no immediate response from the Qatari government. Some Qataris took to social media saying they were upset at the news site being blocked, while others said they supported the move because of overly critical reporting by Doha News.

Times of India

Congress Twitter hacking: Server traced to Bengaluru, IP address in Scandinavia
Friday, 02 December 2016
Byline: Somreet Bhattacharya

New Delhi - Delhi police registered two FIRs on Thursday following a complaint that the Twitter handles of Congress and its vice-president Rahul Gandhi were hacked. Police said a case under Section 66 of the IT Act was registered and a probe has been initiated.
Sources said that preliminary investigation revealed that the server from where the hackers had logged in was based in Bengaluru. However, the IP address they used was found to be in Norway or Sweden.

Police suspect that Rahul's account might have been accessed from a device that did not have an updated anti-virus software or from a compromised IP address. They said that the hackers might have logged in from multiple IP addresses to make tracking difficult.

Sleuths suspect that a malware existed on the computer system from which both the accounts were accessed. They called the modus operandi "spear phishing", where the email account used to create the Twitter handle or the Twitter account itself is hacked using phishing software.

A cyber security team under DCP Anyesh Roy has been formed to probe into the full dump of the INC mail id. A request has been sent to Twitter to access the related information that the hackers had used to create their Twitter profile.

The Hindu
For hackers, it's open season on Congress
Friday, 02 December 2016
Byline: Devesh K. Pandey

New Delhi - The Congress's website was on Thursday taken down and hundreds of e-mail and Twitter accounts of its members, including those of several senior leaders, were disabled following a series of massive cyber attacks on the server that hosts the services. The hackers have threatened to make public the e-mail contents by Christmas.
Based on complaints, the Delhi Police have registered two FIRs under Section 66 of the Information Technology Act and sought the service provider log records and IP addresses of the devices that were used to access the accounts.

The Ministry of Electronics and Information Technology is also investigating the digital footprints of the hackers.

The cyber attacks have triggered a war of words between the Congress and the BJP leaders. The issue was also raised in Parliament by several members, raising concern about the cyber security preparedness of the country.

Alleging a conspiracy behind the hacking of its website and e-mail and Twitter accounts, the party, in its police complaint, said: "The profanity, abuse and derogatory remarks were then retweeted within seconds and minutes by various individuals carrying the same mal-intent in concert with the said hackers as part of a ring of conspiracy to publish, propagate and spread the highly abusive, obscene ... as posted illegally."

"The e-mail accounts operating through domain inc.in and the Twitter accounts of a large number of party members have been suspended due to the cyber attacks," said a Congress member, requesting anonymity. It comes just a day after Congress vice-president Rahul Gandhi's Twitter account was hacked.

Party chief spokesperson Randeep Surjewala blamed the "fascist" forces, stating that it reflected the extremities of an intolerant culture that resorted to abuse when cornered. Congress president Sonia Gandhi's political secretary Ahmed Patel tweeted: "Those forcing country to adopt online payment overnight, have they taken steps to ensure a/c of ordinary ppl will be immune from hacking?"

Jerusalem Post
Biometric database, fingerprinting to be required for all IDs in Israel
Friday, 02 December 2016
Byline: Yonah Jeremy Bob

Jerusalem - Interior Minister Arye Deri has decided to push to mandate the joining of the national biometric database, including taking finger prints and facial recognition pictures for all identity cards going forward, he announced on Wednesday.
It is still unclear whether Deri will garner a Knesset majority to make the requirement law, but every recent interior minister has supported the initiative, even as the Movement for Digital Rights and some cyber experts have opposed it for fear of rampant hacking threats and invasion of privacy.

The debate has lasted years and included multiple extensions of a pilot program which has taken in a sizable portion, though still a minority, of the country's citizens.

Those objecting would still have their fingerprints and facial recognition picture taken, but it would only be connected to their smart-card, not placed in the database, and as a penalty of sorts, they would need to renew their ID cards every five years instead of every 10 years.

The Movement for Digital Rights has vowed to continue fighting the initiative in the Knesset and even to petition the High Court of Justice to block making fingerprinting and facial recognition required if the Knesset passes the initiative into law.

Arab News
National Center for Electronic Security monitors cyberattacks
Friday, 02 December 2016
Byline: Mohammed Al-Sulami

Jeddah - The National Center for Electronic Security detected destructive electronic strikes against several government agencies and vital establishments inside the Kingdom aimed at disrupting computer servers and electronic appliances to affect the services provided by the establishment.
The hack tries to seize entry information into the system to implant malware or a virus to disrupt users' data. The hack attempt targeted several sectors, including the government sector, transport and other agencies.

The center had sent warnings against organized threats aimed at disabling the services provided by some agencies, on Nov. 19, 2016. Warnings were also sent and shared with many government agencies and vital facilities, and contained important and necessary information on how to avoid any hacking attack, and the means of protecting and safeguarding, along with technical steps to ward off any repercussions as a result of the breach.

The center recommends following the best practices in the protection of electronic systems, in particular with regard to reducing Remote Desktop Protocol (RDP) access via VPN service.

The indicators show that the source of this attack is from outside the Kingdom and has come in several ongoing electronic attacks aimed at government agencies and sectors.

The center stresses the need for various sectors and businesses to follow the best practices and take the necessary preventive measures to safeguard and protect their data and systems from potential electronic intrusion.

During the past few years, a number of Saudi networks and websites witnessed systematic and violent cyberattacks that targeted both the public and private sectors in the Kingdom, the last being in August, while the most severe was in 2012 targeting Saudi Aramco.

Reuters
La Russie dit avoir déjoué une cyberattaque contre ses banques
Friday, 02 December 2016
Byline: Christian Lowe avec Elena Fabrichnaya et Kira Zavialova

Moscou - La Russie a annoncé vendredi avoir mis en échec un complot ourdi par des espions étrangers pour semer le chaos dans le système bancaire russe par des cyberattaques coordonnées et la diffusion de fausses informations sur l'état de ses banques sur les réseaux sociaux.

Le Renseignement intérieur russe (FSB) précise dans un communiqué que les serveurs qui devaient servir à lancer les cyberattaques sont situés aux Pays-Bas et qu'ils sont enregistrés auprès de BlazingFast, une société ukrainienne d'hébergement de sites internet.

Les attaques devaient débuter le 5 décembre et cibler des banques nationales et régionales dans plusieurs villes russes, ajoute le FSB.

"Il était prévu que la cyberattaque s'accompagne de l'envoi massif de SMS et de messages alarmistes sur les réseaux sociaux évoquant une crise du système bancaire russe, des faillites et des retraits de licence", lit-on dans le communiqué.

"Le FSB prend les mesures nécessaires pour neutraliser les menaces contre la sécurité de l'économie et de l'information en Russie", ajoute le service de renseignement sans plus de précision, notamment sur la nationalité des espions étrangers mis en cause.

Le directeur de BlazingFast, Anton Onopritchouk, a déclaré à Reuters que la société basée à Kiev n'avait été contactée ni par le FSB, ni par aucun autre service de renseignements. Il a dit attendre d'en savoir davantage pour mener une enquête interne.

A la question de savoir si ses serveurs pourraient servir à lancer une cyberattaque, il a répondu: "Techniquement, c'est possible. Cela peut arriver à n'importe quelle société d'hébergement où on peut louer un serveur. A partir de là, on peut attaquer ce qu'on veut et dans 99% des cas, on ne s'en rend compte que quand cela a eu lieu."

La Russie est particulièrement vigilante aux cyberattaques depuis qu'elle a été accusée d'avoir été impliquée dans le piratage du système de messagerie électronique du Parti démocrate pendant la campagne présidentielle américaine.

Le vice- président américain, Joe Biden, avait à l'époque menacé le Kremlin d'une réponse "proportionnée".

Plusieurs cyberattaques ont depuis visé des institutions russes sans que l'on sache si elles étaient liées aux tensions entre Moscou et Washington.

ITAR-TASS World Service
Major Russian banks say unaffected by cybersecurity threats
Friday, 02 December 2016

Moscow - Russia's leading financial group VTB and the biggest lender Sberbank said on Friday cyber threats have not affected their activities.
Earlier in the day, Russia's Federal Security Service (FSB) announced that foreign special services were plotting a series of cyber attacks starting from December 5 aimed at destabilizing the country's financial system, including the activity of major Russian banks.

"The security systems of the group's banks meet all the latest requirements and guarantee full protection of our clients' operations," the press service of the VTB Group told TASS.

Sberbank, the third largest bank in Europe, said it is "working in a normal mode."

"Sberbank does not comment on other news within the competence of law enforcement agencies," the bank said.

Russia's Central Bank, the main regulator of the country's banking industry, said it knows about the cyber threats and is constantly cooperating with law enforcers and the banks. "The situation is under control. The necessary recommendations have been given to the banks," the press service said.

The regulator also stressed that it held a meeting with Russia's Ministry of Telecom and Mass Communications and telecom operators. The sides agreed on top priority measures to prevent these attacks.

"Such attempts to destabilize the situation have been already seen, for example in late 2014. Joint steps of credit organizations with the support of the Bank of Russia allowed countering negative trends caused by a targeted information attack," it said.

New York Times
Cyberattacks Disrupt Saudi Aviation Agency
Friday, 02 December 2016
Byline: Sewell Chan

New York - Saudi Arabia's aviation agency was attacked last month by an aggressive computer virus intended to disrupt high-profile government targets, officials and experts said on Thursday.
The attack, which experts say emanated from outside the country, used a version of Shamoon, malware used to target the Saudi energy sector four years ago. Similar kinds of data-clearing software were used in 2014 against the Las Vegas Sands and Sony.

The Saudi government confirmed the latest breaches on Thursday, after several cybersecurity firms noted them. Bloomberg News reported that thousands of computers were damaged at the headquarters of the General Authority of Civil Aviation starting in mid-November, "erasing critical data

and bringing operations there to a halt for several days," although operations at Saudi airports did not appear to be affected.

The state-run Saudi Press Agency, citing a government statement, reported on Thursday that the national cybersecurity department had detected what officials called a systemic attack on crucial government agencies, including in the transportation sector. The attacks were aimed at halting operations, stealing data and planting viruses, the news agency reported.

Saudi Press reported that officials had alerted the government to the attacks last month and had sent vulnerable agencies tips on defending their computers -- suggesting that officials had failed to heed the messages.

The statement acknowledged that the attacks were staged from outside Saudi Arabia, but it did not specify the targets nor say when the breaches began.

If Saudi officials were fazed, they did not show it on Thursday.

"What attack?" Mohsen al-Shahrani, a communications officer for the general security department at the Interior Ministry, said when asked about the assault. "I have not heard anything about this."

Bloomberg, citing anonymous sources, reported that state-sponsored hackers were believed to be responsible for the breaches and suggested that they might have emanated from Iran.

Iran and Saudi Arabia have been in a tit-for-tat cyberwar for more than four years. In April 2012, Iranian engineers working at the Kharg oil terminal, a speck in the Persian Gulf from which a large portion of Iran's oil is exported, noticed that their computers had stopped working. The same happened at the Oil Ministry's headquarters in Tehran, the capital, according to local news accounts.

A computer virus known as a wiper had been interfering with the ministry's internal network, removing files from hard drives and taking over computers. Insiders suspected Saudi hackers of carrying out the attacks, though there was no evidence.

Four months later, Saudi Aramco, the largest company in the Saudi Arabia, was hit by a virus that erased data on three-quarters of the company's computers, replacing everything with an image of a burning American flag. American intelligence officials said the real perpetrator was Iran, although they offered no evidence.

Dmitri Alperovitch, the co-founder and chief technology officer of the security firm CrowdStrike, wrote in a blog post on Thursday that the malware was a variant of Shamoon, which was used in the Aramco attack.

Mr. Alperovitch said the motives for the most recent attacks were not clear. He noted, however, that Iran had targeted Saudi Arabia with cyberattacks before, that the two countries have been locked in a sectarian competition for regional dominance for years, and that they are backing opposing sides of the wars in Syria and Yemen.

Iranian intelligence agents used Shamoon in 2012 in retaliation for international sanctions, Mr. Alperovitch said, adding that the latest attacks came just before a meeting in Vienna of the Organization of the Petroleum Exporting Countries, which agreed on Wednesday to cut oil production for the first time in eight years, prompting an immediate rise in oil prices.

Another security firm, Symantec, reported that the breaches had been timed for the evening of Nov. 17, the end of the workweek, which in much of the Muslim world runs from Sunday to Thursday.

"The attackers appear to have done a significant amount of preparatory work," Symantec reported. "The malware was configured with passwords that appear to have been stolen from the targeted organizations and were likely used to allow the threat to spread across a targeted organization's network. How the attackers obtained the stolen credentials is unknown."

Symantec added, "It would appear that the attack was timed to occur after most staff had gone home for the weekend in the hope of reducing the chance of discovery before maximum damage could be caused."

Another security company, Palo Alto Networks, reported that Shamoon breaches used malware known as Disttrack, "a multipurpose tool that exhibits wormlike behavior by attempting to spread to other systems on a local network using stolen administrator credentials." At least 30,000 computer systems were damaged in the 2012 attacks, Palo Alto Networks reported.

Deutsche Welle
Wikileaks releases 2,420 documents from German government NSA inquiry
Friday, 02 December 2016
Byline: Staff report

Berlin - The documents contained 90 gigabytes of information including many classified documents, according to the statement on the Wikileaks website on Thursday. They are the property of government agencies such as the Federal Intelligence Service (BND, pictured above) and the Federal Office for the Protection of the Constitution (BfV).
The published materials had been submitted last year as part of a German parliamentary inquiry into the surveillance activities of the BND and its cooperation with the NSA.

"The collection contains early agreements between the BND and the NSA and internal processes at the BND, but also more recent details on the close collaboration between the two agencies," Wikileaks

announced, adding: "This substantial new collection of primary source documents provides significant new evidence (of their collaboration)."

The documents, Wikileaks claimed, contain the answers to questions posed by the inquiry committee as well as administrative documents, correspondence, agreements and press reactions. Wikileaks says there are 125 documents from the BND, 33 from the BfV and 72 from the Federal Office for Information Security (BSI).

Wikileaks announced the documents contained "a detailed insight, not just into the agencies themselves, but also into the mechanics of the inquiry." This included information on which private US companies were operating in Germany's security sector.

German ruling on Snowden testimony

The Wikileaks action comes after a German court ruling last week concerning testimony by former NSA employee Edward Snowden to the inquiry. It was in the wake of Snowden's revelations about the activities of the NSA that the inquiry was set up in 2014.

Snowden's travel to Germany was conditional on a guarantee from the government that he "would not be handed over to the US."

Last Monday, the Federal Court of Justice ruled that the committee was obliged to hear Edward Snowden in person. But at the next inquiry hearing on Thursday, the issue of Snowden's invitation was removed from the agenda, according to agency reports. Representatives from Germany's governing coalition say they want to appeal the court's decision.

Founder of Wikileaks, Julian Assange, said: "This substantial body of evidence proves that the inquiry has been using documents from Mr. Snowden and yet it has been too cowardly to permit him to testify. Germany cannot take a leadership role within the EU if its own parliamentary processes are subservient to the wishes of a non-EU state."

Last year, WikiLeaks published documents that suggested the communications of more than 120 top German government officials, including Chancellor Angela Merkel, were being intercepted by the NSA.

ITAR-TASS World Service
FSB reports foreign special services preparing massive cyber attacks
Friday, 02 December 2016
Byline: Staff report

Moscow - Foreign special services are preparing to carry out massive cyber attacks starting from December 5 aimed at destabilizing Russia's financial system, the Federal Security Service said on its website on Friday.
The goal of the cyber attacks is also to destroy the activity of "a range of major Russian banks," according to the FSB.

The servers and command centers for carrying out these cyber attacks are located in the Netherlands and are owned by Ukraine's hosting company BlazingFast.

The cyber attacks are expected to be accompanied by mass SMS and provocative publications in social networks or blogs about "a crisis in the Russian credit and financial system, bankruptcy and withdrawal of licenses of leading federal and regional banks."

"The campaign is directed against several dozen Russian cities," the FSB stressed.

The FSB is carrying out the necessary measures to neutralize the threats to Russia's economic and information security and documenting the forthcoming campaign, it said.

London Times
French poll warning over Russian hacking threat
Friday, 02 December 2016
Byline: Adam Sage

Paris - France's political parties have been summoned to a meeting by the country's top spy agency and told to strengthen their defences against cyberattacks amid fears that Russian hackers could seek to influence the presidential election next year.
French intelligence agencies endorse claims that the Kremlin tried to sway the US presidential race, and believe that similar tactics might be deployed in France. Germany's spy chief expressed concern this week that Russia would use cyberattacks to spread misinformation before the German elections next autumn.

The issue is particularly sensitive in France given President Putin's support for right- wing presidential election candidates. He is an admirer of François Fillon, of the Republican party, and has close ties with Marine Le Pen, leader of the far-right National Front. Both have pledged to build bridges with Moscow if they come to power.

Intelligence agencies have not said specifically that Mr Putin may try to help one or the other win the election but they believe Russian hackers could try to cause chaos by publishing false information on French news sites. They also fear that the Kremlin could seek to infiltrate French political parties, gaining access to membership lists and obtaining information on the country's rulers.

Party leaders were summoned by the General Secretariat for Defence and National Security in October for a briefing on the US cyberattacks and a warning that the Russians could strike in France. They were told to reinforce their computer systems.

A day later, the National Commission for Information Technology and Liberty publicly warned the ruling Socialist party that it was vulnerable. The commission said its inspectors had hacked into a list of all the party's members since 2010, obtaining names, addresses and payment details. The party said it had rectified the flaw, but the incident fuelled fears of a hostile attack.

Media outlets are also thought to be vulnerable to hackers wanting to mislead the public. Guillaume Poupard, director of the National Agency for the Security of Information Systems, said western democracies were facing "the development of a digital threat whose goals were political and to [cause] destabilisation. "In the American case, we cannot dismiss the hypothesis that there was a real plan to influence the election," he said.

Reuters
Russia says foreign spies plan cyber attack on banking system
Friday, 02 December 2016
Byline: Staff report

Moscow - Russia said on Friday it had uncovered a plot by foreign spy agencies to sow chaos in Russia's banking system via a coordinated wave of cyber attacks and fake social media reports about banks going bust.
Russia's domestic intelligence agency, the Federal Security Service (FSB), said in a statement that the servers to be used in the alleged cyber attack were located in the Netherlands, and were registered to a Ukrainian web hosting company called BlazingFast.

The attack was to have started on Dec. 5, and its targets were a number of major national and provincial banks in several Russian cities, the statement said.

"It was planned that the cyber attack would be accompanied by a mass send-out of SMS messages and publications in social media of a provocative nature regarding a crisis in the Russian banking system, bankruptcies and license withdrawals," said the statement.

"The FSB is carrying out the necessary measures to neutralize threats to Russia's economic and information security," it said.

The statement did not say which countries' intelligence agencies were behind the alleged plot.

Anton Onoprichuk, director of Kiev-based BlazingFast, said neither the FSB nor any other intelligence agency had been in touch with his company. He told Reuters he was waiting for more information so the firm could investigate.

Asked if his servers could be used to mount a cyber attack he said: "Technically it is possible. It is possible with any hosting company, where you rent a server. You can attack whatever (you want) from it and in 99 percent of cases it will become known only after the event."

Russia is on high alert for foreign-inspired cyber attacks, especially since U.S. officials accused the Kremlin of being involved in hacks on Democratic Party emails during the U.S. presidential election.

U.S. Vice President Joe Biden said at the time that the United States would mount what he described as a "proportional" response to Russia.

Since then, there have been a number of cyber attacks affecting Russian institutions, though it is unclear if they were linked to the row between Moscow and Washington.

In October, a network of Ukrainian hackers released a cache of emails obtained from the account of an aide to Vladislav Surkov, a Kremlin advisor dubbed "the grey cardinal" because of his behind- the-scenes influence.

On Nov. 11, Russian lenders Sberbank and Alfa Bank said they had been hit by cyber attacks.

Saudi Gazette
Shamoon virus returns in new Gulf attacks after 4-year hiatus
Friday, 02 December 2016

Riyadh - A version of Shamoon, the destructive computer virus that crippled tens of thousands of computers at Middle Eastern energy companies four years ago, was used in mid-November to attack computers in Saudi Arabia and elsewhere in the region.
US security firms CrowdStrike, Palo Alto Networks Inc and Symantec Corp. warned of the new attacks on Wednesday. They did not name any victims of the new version of Shamoon, which cripples computers by wiping their master boot records that they use to start up. They also did not say how much damage had been caused or identify the hackers.

FireEye said in a blogpost that its Mandiant unit "has responded to multiple incidents at other organizations in the region." A spokesman declined to identify the countries or organizations.

Saudi Arabia said on Thursday that a computer virus attack on Nov. 19 targeted Saudi government bodies and vital installations including the Kingdom's transport sector.

"The attack appeared to originate outside the country and was one of "several ongoing cyber attacks targeting government authorities", the Saudi Press Agency quoted the National Cyber Security Center, an arm of the Ministry of Interior, as saying.

It did not give further details of the identity of the attacker or the damage that had been done, beyond saying the virus aimed to disrupt servers and plant malicious software in computer systems.

The reappearance of Shamoon is significant as there have only been a handful of other high-profile attacks involving disk-wiping malware, including ones in 2014 on Sheldon Adelson's Las Vegas Sands Corp. and Sony Corp's Hollywood studio.

Governments and businesses pay close attention to such cases because it can be time-consuming and extremely expensive to restore infected systems.

The original Shamoon hackers left images of a burning US flag on machines at Saudi Aramco and RasGas Co Ltd in 2012. Researchers said the Shamoon 2 hackers also left a calling card: a disturbing image of the body of three year-old Syrian refugee Alan Kurdi, who drowned in the Mediterranean last year.

The FireEye spokesman said the malware contains embedded credentials, which suggests the attackers may have previously conducted intrusions to gather the necessary logins and passwords before later embedding them into the malware for the destructive attack.

The 2012 Shamoon attacks were likely conducted by hackers working on behalf of the Iranian government, said CrowdStrike Chief Technology Office Dmitri Alperovitch. It is too early to say whether the same group was behind Shamoon 2, he said.

The motive of the recent attacks was also not immediately clear. "Why Shamoon has suddenly returned again after four years is unknown," the Symantec Security Response team said on its blog. "However, with its highly destructive payload, it is clear that the attackers want their targets to sit up and take notice."

The malware triggered the disk- wiping to begin at 8:45 p.m. local time on Thursday, Nov. 17, according to the security firms.

The Saudi business week ends on Thursday, so it appears to have been timed to begin after staff left for the weekend to reduce the chance of discovery and allow maximum damage.

"The malware had potentially the entire weekend to spread," Palo Alto researcher Robert Falcone said in a blog post.

CBC News
Privacy watchdogs urge caution with encryption laws
Wednesday, 07 December 2016
Byline: Matthew Braga

Ottawa - Privacy watchdogs from across Canada warned the government on Tuesday to "proceed cautiously" before passing encryption legislation -- a move that would have the potential to undermine the security of everything from financial transactions to online communication.
The warning comes at a time when government and law enforcement agencies have been seeking the ability to access encrypted information, the lack of which they see as a growing investigative problem.

However, both privacy and cryptography experts have long warned that efforts to weaken or defeat encryption for police puts the security of all users at risk.

The government is currently soliciting feedback and holding public consultations on this and other national security issues, as part of its pledge to to repeal the "problematic elements" of Bill C-51.

In a submission to Public Safety Canada, Canada's Privacy Commissioner Daniel Therrien and his colleagues warned against introducing any legislation aimed squarely at encryption, as well as other proposed powers that police do not currently have.

"The government should only propose and Parliament should only approve new state powers if they are demonstrated to be necessary and proportionate -- not merely convenient," Therrien said in a prepared statement to reporters Tuesday morning in Ottawa. The statement was also posted to the commissioner's website.

Existing tools should be examined

A recurring theme of the group's submission is that police have not provided adequate evidence for why they should require additional powers -- such as expanded data retention requirements, or lower thresholds for acquiring basic subscriber information -- nor explained why existing tools are insufficient.

Therrien, along with the country's other provincial and territorial commissioners, are advocating for a closer examination of existing tools, and recommending that some rules should even be tightened.

"This is not the time to further expand state powers and reduce individual rights," Therrien said in his statement.

"This is the time to enhance both legal standards and oversight to ensure we do not repeat past mistakes and achieve real balance between security and respect for basic individual rights."

Legal measures sought

One particularly divisive issue is the matter of encryption -- cryptographic protections that prevent attackers and police alike from eavesdropping on messages as they travel across the internet, or from accessing files on a password-protected device.

"There is currently no legal procedure designed to require a person or an organization to decrypt their material," according to Public Safety Canada's "National Security Green Paper," which was released in September to "prompt discussion and debate about Canada's national security framework."

Both law enforcement and government agencies have increasingly characterized encryption as an impediment to investigations, a problem they refer to as "going dark." Canada's police chiefs, for example, recently called on the government to introduce legal measures that deal with encryption, and the US Senate introduced a draft bill addressing encryption earlier this year.

Yet Therrien argues that powers that came into force with Bill C-31 last year already allow police to seek "assistance" in decrypting information, without compromising the underlying technology behind encryption.

"The crux of the problem springs from the fact there is no known way to give systemic access to government without simultaneously creating an important risk to the security of this data for the population at large," the submission reads. "Laws should not ignore this technological fact."

The country's privacy watchdogs suggest "technical solutions which might support discrete, lawfully authorized access to specific encrypted devices, as opposed to imposing general legislative requirements."

Push for transparency

Encryption isn't the only issue dealt with in the Privacy watchdogs' submission.

Metadata is a perennial concern, and the submissions suggests more stringent legislation under which metadata can be collected and shared with police, as well as international partner agencies.

The commissioners also call on the government to strengthen requirements that private companies and government agencies "be open about the number, frequency and type of lawful access requests they respond to," in regularly issued transparency reports.

They also propose an expanded oversight committee that includes independent expert reviewers, and would oversee all agencies that have a role in national security, calling the government's current proposal "insufficient."

Montreal Gazette
Habib had combat manuals on computers, trial hears
Wednesday, 07 December 2016
Byline: Staff reporter

Montreal - The trial of Ismael Habib, a 29-yearold man accused to trying to leave Canada to commit terrorist acts abroad heard Tuesday what RCMP investigators recovered from the computers seized in the wake of their investigation.
Maxime Embury-Larocque, a member of the RCMP's Integrated National Security Enforcement Team, told the court that two tablet computers seized from a residence in Gatineau last February contained several pictures of the accused, one showing him what appeared to be military fatigues and carrying a knife on his hip while the other depicted him wearing a black T- shirt that Embury-Larocque believed bore the inscription of the Muslim shahada - the acknowledgement of the oneness of God and of Muhammed as his prophet - in Arabic script.

A check of the computers also revealed the name Alexandre Fortin, Embury-Larocque said, the same name on a driver's licence in Habib's possession when he was arrested, although the licence bore Habib's photo.

The court also heard that searches of Habib's computers also yielded PDF files of combat training manuals as well as covers from Inspire, an online magazine perceived as a propaganda and recruitment tool used by al Qaeda terror network.

Embury-Larocque noted that most of the online links found on the computer no longer existed, although investigators were able to extract an apparent record of an online conversation between two persons, one of whom identified himself as "Stéphane Leclair," a false name the correspondent said he used for security reasons.

Reading from an inventory of the information gleaned from the computer, Embury-Larocque said "Leclair" described himself as having a father from Afghanistan,

a Canadian mother and being fluent in English, French, Arabic and Afghani. Embury-Larocque quoted "Leclair" as saying "As for me, I love jihad (holy war) more than anything."

"Leclair" also detailed some of the day-to-day life fighting as a jihadi, noting he fought at the front and saying "There is no place where I feel more at home than here."

Habib is accused of trying to leave the country to commit terrorist acts abroad - specifically with ISIL in Syria - and giving false information to obtain a passport. The 29-year-old was arrested last February and is only the second Canadian to be tried under socalled terrorist travel legislation enacted in 2013, and the first adult.

However a large part of the evidence against Habib was gathered in a "Mr. Big" police operation, during which a police officer pretended to be a high ranking criminal and offered employment to Habib - and in this case help getting a passport and safe passage to Syria - as long as he comes clean about his past and his current intentions.

On Monday, before he heard any new evidence, Quebec Court Judge Serge Delisle announced he would rule on whether the scenario presented to Habib fit the definition of a Mr. Big operation and, if so, whether the statements made by Habib to the undercover police operative are admissible.

Delisle noted, however, that he would first hear all the evidence.

Scoop.co.nz
GCSB wants to give ISPs more power to block cyber threats
Wednesday, 07 December 2016
Byline: Sophie Boot

Wellington - The Government Communications Security Bureau wants to give internet service providers more information and power to block cyber threats which are increasing, its director told the intelligence and security select committee yesterday.
The communications-focussed spy agency has recorded 338 cyber security incidents in the last year, from 109 a year earlier, which director Andrew Hampton said was due to both the number of threats increasing and the improved system picking up more threats.

Cyber threats to New Zealand are "becoming more complex and their sources more diverse" with a "growing range of international threat actors targeting New Zealand organisations for financial gain," Hampton said.

Public and private organisations are targeted for their intellectual property for new technology, customer data, business and pricing strategies, and government positions on sensitive topics, Hampton said.

The agency is also looking to increase the information it gives to ISPs from Cortex, the system which aims to disrupt advanced cyber threats to organisations of national significance in both the public and the private sector.

"We've increased cyber security services to organisations of national significance through Cortex, with the consent of the organisations involved," Hampton said, adding the agency had responded to 69 notifications of network changes within areas of security interest in the year. "More broadly Cortex is a big focus, but our regulatory role under the TICSA Act (the Telecommunications Interception Capability and Security Act 2013) is important because that helps us with telcos to ensure they're not inadvertently introducing vulnerabilities into the system.

"Where we're wanting to evolve Cortex is where we can provide more information to other parties such as ISPs so they can do some of the blocking on our behalf," Hampton said. "An obvious benefit of that is it gets the security agency out of there which deals with any public concern about privacy, but also increases the ability to scale."

Yonhap News Agency
Suspected N.K. attackers hack into S.K. cyber command through main server
Wednesday, 07 December 2016
Byline: Staff reporter

Seoul - Military investigators looking into the first hacking of South Korea's cyber command intranet said Wednesday the suspected North Korean attackers accessed the network through a server at the armed forces' main information center.
The findings raised concerns that confidential information may have been compromised as the affected server is connected with the information systems of the Army, Navy and the Air Force. But the ministry said information saved on the server system was not stolen.

A total of 3,200 computers, including 700 linked with the intranet, were contaminated with malware in the latest cyber attack, which occurred on Aug. 4, the Ministry of National Defense said.

It said some military documents were hacked while refusing to provide details. The computer used by Defense Minister Han Min-koo was also affected, the official said.

On Tuesday, the ministry said the IP addresses linked to the attack were traced to a location in China that has been used by North Korean hackers.

"As one of the military's two integration servers was jointly linked to the internet and the intranet, it allowed the hackers to gain access to the intranet," a ministry official said.

It is one of two servers the military operates. The other server involves information for the defense ministry, the Defense Security Command and the Defense Acquisition Program Administration (DAPA).

"We are still in the process of determining what data were leaked. We found the hackers infiltrated the intranet using the main server but information in the server remains intact," the official said.

The cyber command separated the affected server from the whole network to avoid the spread of viruses in October, two months after the initial hacking attempt was made in August.

It marked the first time that the data of South Korea's cyber command has been compromised. South Korea set up the command in January 2010 as part of its efforts to counter external hacking attempts on the country's military.

North Korea -- which has thousands of cyberwarfare personnel -- has a track record of waging cyberattacks on South Korea and the United States in recent years, though it has flatly denied any involvement.

South Korea's unification ministry said that there is no sign of possible North Korean cyberattacks on its networks and other security- related ministries' system.

"Our ministry and foreign and defense ministries have continued to craft up various measures to boost cybersecurity," Jeong Joon-hee, ministry spokesman, said at a regular press briefing.

Earlier this year, Seoul accused North Korea of stealing information from about 10 South Korean officials by hacking into their smartphones.

Two months ago, Rep. Kim Jin-pyo, a lawmaker of the main opposition Democratic Party, claimed that the cyber command was hacked in September. He told Yonhap that the attack targeted the "vaccine routing server" installed at the cyber command.

Kim, who is a member of the parliament's national defense committee, said that a malicious code was identified and it appears to have taken advantage of the vulnerability of the routing server.

The server is tasked with security on computers that the military has for internet-connection purposes. Around 20,000 military computers are known to have been connected to the server.

Kim said in October that chances are "very low" that the hacking led to a leak of confidential information, given that the military's intranet is not connected to the server.

The defense ministry later announced it has identified the intrusion of the malicious code into the system.

Xinhua News Agency
Beijing shuts down thousands of illegal live streaming accounts
Wednesday, 07 December 2016
Byline: Staff reporter

Beijing - Thousands of illegal accounts have been shut down by Beijing-based live streaming websites since a regulation went into effect on Dec. 1, authorities said Tuesday.

Reports of violent, obscene and vulgar content on live streaming websites abound. In November, the Cyberspace Administration of China published a regulation that bans the use of live streams to undermine national security, destabilize society, disturb social order, infringe upon others' rights and interests, and disseminate inappropriate content, including pornography.

According to the regulation, service providers are obliged to censor content before releasing it and are instructed to establish a system that would allow them to block improper live streams immediately.

So far, more than 4,500 accounts on the Beijing- based websites were closed and more than 3,100 illegal live streaming programs have been removed, according to Beijing's cyberspace administration.

Officials with the administration said they will enhance regulation efforts to "safeguard order in the Internet industry." They also called on the public to join in supervision.

Gulf News
Oman warns against spreading sectarian material online
Wednesday, 07 December 2016
Byline: Fahad Al Mukrashi

Muscat - Oman has warned that it will take serious legal action against anyone who is found disseminating video clips on social media platforms that incite sectarian and religious strife, said Hussain Al Hilali, public prosecutor, in a press statement.
Al Hilali said it is important to criminalise the menace as it destabilises the security of any country and shakes its pillars.

He said sectarian incitement is a criminal offence as per Oman Penal Law since 1974. Al Hilali issued a judicial circular recently to all heads of public prosecution departments in the country to take serious legal action in this regard.

Oman has a unique religious make-up where the dominant sect is the Ibadhi sect of Islam, with a sizeable population of Sunnis and a minority of Shiites, all of which live in relative harmony. It is not clear what triggered the statement from the public prosecutor.

Al Hilali cited Sultan Qaboos' address on the country's 24th national day in which he blasted extremism, fanaticism and partisanship as "poisonous plants which the country's good soil rejects".

The public prosecutor warned Omanis to stay away from such sectarian and religious strife, arguing that it violated the way of life in Oman, warning that the government shows zero tolerance against anyone involved in such matters.

In 2008, Oman introduced a law stipulating that anyone involved in crimes related to terrorism and sectarianism would be jailed for a minimum of 10 years.

It has signed the International Convention for the Suppression of the Financing of Terrorism. Oman also established the anti-money laundering Combating the Financing of Terrorism (CFT) system in 2002, as per a royal decree.

In November, Oman scored zero in the global terrorism index, reflecting on its safety and security against terrorist threats, according to the Global Terrorism Index 2015 released recently by the Economics and Peace Institute.

Jerusalem Post
Israeli experts heading to Japan to provide much needed cybersecurity
Wednesday, 07 December 2016
Byline: Michael Zeff

Jerusalem - Local cybersecurity company Cybereason announced on Tuesday that it is partially relocating to Japan, following a $59 million investment by Japanese Internet giant Soft- Bank. The move is part of a larger trend by Japan, which is seeking international corporations and foreign experts in its fight against an increasing wave of cyber attacks against its institutions.
"Japanese companies and national institutions are constantly under cyber attack, but the public awareness in Japan as to the need for cybersecurity is low compared to Israel or the United States. But now, we've partnered with SoftBank to establish Cybereason Japan Corp to help defend Japan," Lotem Guy, a security research group manager at Cybereason who will be moving his family to Japan in the coming days, told The Jerusalem Post.

Tel Aviv-based Cybereason is a company that locates, isolates and responds to cyber attacks in real-time. Their platform - which relies on the company's tech and human wealth - can find a single component of an attack and connect it to other pieces of information gathered by Cybereason, in order to reveal an entire campaign and shut it down.

"Our product specializes in identifying attacks on large organizations. Our team sits inside an organization and gathers and analyzes data from inside their computers, servers and workstations. That data is then sent to our central server, which runs on our software and studies the organization's behavior, breaking it down into separate units. Then we can identify anything that is out of the ordinary and characterizes a cyber attack, isolate it and respond to it without disrupting the organization's work routine," Guy explained.

According to Japan's National Institute of Information Communications Technology, Japan has experienced more than 50 billion cyber attacks in the last two years. In the past two years, Japanese investment - both private and national - in Israel grew exponentially, especially in the fields of

autonomous drones, recognition and authentication technology, and security- related technology. Now SoftBank and Cybereason are bringing in Israeli experts to upgrade Japan's cyber defenses.

SoftBank is a Japanese multinational corporation with operations in telecommunications, e-commerce, Internet services, technology services, finance, media and other businesses worldwide, and it provides infrastructures for Internet giants like Alibaba and Yahoo.

According to Forbes Magazine, SoftBank is the 62nd largest public company in the world and the third largest in Japan.

SoftBank bought a cybersecurity platform from Cybereason back in 2015, and, after being impressed by the Israeli company's abilities and technology, decided to make a large investment in the company.

"Our deployment of the Cybereason platform internally gave us first-hand knowledge of the value it provides and led to our decision to invest," stated Ken Miyauchi, president and CEO of SoftBank Corp, in a testimonial.

According to Guy, a large portion of the $59m. investment went toward the joint venture of creating the Japanese subsidiary, Cybereason Japan Corp.

"After SoftBank used our platform as a client, it opened their eyes. They realized that now they can do all the things they wanted to do, all the things they knew they needed to do, but never had the tools to do before. They now believe that the Japanese market is in dire need of this tool and that together we can bring it to Japan," said Guy.

"Unlike other more traditional and conservative Japanese businesses, SoftBank is a younger company; it specializes in everything IT and has a younger and more innovative and open spirit," Guy told the Post.

According to Guy, it was that unique spirit that allowed SoftBank to develop an awareness as to the need for cyber defense and led the company to take a more proactive approach, partner up with Cybereason and establish the Japanese subsidiary to cater to the Japanese market.

"The Japanese market is really hard to penetrate for a Western company, it's difficult to sell anything here unless you are Japanese. But this cooperation gives us a very big opportunity to succeed," said Guy.

The partnership between an Israeli cybersecurity pioneer and an established Japanese corporation makes market penetration easier and more likely to succeed, especially in light of Japan's growing need for technologies it doesn't have. The Cybereason Japan team is composed of Cybereason Israel expatriates and Japanese locals, some of whom were originally from SoftBank. The subsidiary already has a number of large Japanese clients who preferred not to make public their use of cybersecurity platforms.

"We didn't think to grow into the Japanese market, at least not this quickly. Our focus was on the US market mostly, but since the beginning of our relationship with SoftBank, this great opportunity has opened up. In my opinion, our ability to sell in the Japanese market will be equal to the US market very soon," Guy said.

Le Monde
Les services américains et britanniques ont espionné les appels passés à bord des vols Air France
Wednesday, 07 December 2016
Byline: Jacques Follorou

Non identifié - La NSA et son homologue anglais peuvent capter toutes les données, y compris les codes secrets, des communications des passagers de la plupart des grandes compagnies aériennes. Dont Air France.
Dans l'immense stock d'archives extraites par Edward Snowden, l'ancien consultant de l'Agence nationale de sécurité américaine (NSA), c'est une pépite. Elle débute par une devinette: «Quel est le point commun entre le président du Pakistan, un trafiquant de cigares ou d'armes, une cible du contre-terrorisme ou le membre d'un réseau de prolifération nucléaire? Ils utilisent tous leur téléphone portable lorsqu'ils sont dans un avion.»

Posée en 2010 dans une des lettres d'information interne de l'une des principales directions de la NSA, «SIDtoday», et classée top secret , elle annonce l'émergence d'un nouveau terrain d'espionnage, qui n'avait pas encore été exploré: l'interception des données de communications à bord des avions de ligne. En2009, la NSA souligne dans un document interne que, en décembre2008, 50000personnes ont déjà utilisé leur téléphone portable en vol, un chiffre qui atteint 100000 en février2009. Pour expliquer cet engouement, la NSA énumère: «De plus en plus d'avions équipés, la crainte recule de voir l'avion s'écraser. Pas aussi cher qu'on le croyait. (...) Le ciel pourrait appartenir à la NSA.»

Fin 2012, le Government Communications Headquarters (GCHQ), l'homologue britannique de la NSA, livre, à son tour, dans une présentation «top secret strap», un des plus hauts niveaux de classification, les dessous du programme Southwinds («vents du sud») , mis en place pour collecter tout le trafic, voix et data, métadonnées et contenu des connexions à bord des avions. La zone est encore limitée aux régions Europe, Moyen-Orient et Afrique, couvertes par les satellites Inmarsat.

La collecte des données se fait «quasiment en temps réel» et un avion peut être suivi toutes les deux minutes. Pour espionner un téléphone, il suffit qu'il soit à une altitude de croisière de 10000 pieds. Le signal transitant par satellite, la technique d'interception se fait par des stations secrètes d'antennes au sol. Le seul fait que le téléphone soit allumé suffit à le localiser, l'interception peut alors être croisée avec le registre des listes de passagers et les numéros des avions, pour mettre un nom sur l'utilisateur du smartphone. Le GCHQ peut même, à distance, perturber le fonctionnement d'un téléphone de sorte que son utilisateur soit contraint de le redémarrer avec ses codes d'accès: les services britanniques interceptent du même coup ses identifiants.

Une fixation qui ne tient pas du hasard

Le GCHQ et la NSA ont baptisé leurs opérations de mise sous surveillance des communications en avion de doux noms d'oiseaux, «Pie voleuse» et «Pigeon voyageur» , comme cela a été rapidement évoqué par Glenn Greenwald, journaliste indépendant américain, dans son ouvrage Nulle part où se cacher (JCLattès, 2014). Mais un examen plus poussé de ces pièces et la lecture de documents inédits extraits par Le Monde , en collaboration avec le site The Intercept, des archives Snowden données à M. Greenwald et Laura Poitras, sur la surveillance entre 2005 et 2013 des avions commerciaux dans le monde entier, prouve que la compagnie Air France a été très tôt au coeur de l'attention de ces deux pays amis, les Etats-Unis et la Grande- Bretagne.

La cible Air France apparaît dès 2005 dans un document de la NSA fixant les grandes lignes du projet de «traque des avions civils dans le monde entier» . Daté du 5juillet et signé par le numéro deux de l'une des principales directions de la NSA, chargée du renseignement d'origine électromagnétique (SID, Signal Intelligence Directorate), ce mémo de 13pages recense sous forme chronologique et détaillée les principales étapes de ce programme pensé pour éviter «un nouveau 11-Septembre» . On peut lire que, dès la fin 2003, «la CIA considère que les vols Air France et Air Mexico sont des cibles potentielles des terroristes» . Le service juridique de la NSA précise alors «qu'il n'y a aucun problème légal pour cibler les avions de ces deux compagnies à l'étranger» et qu' «ils devraient être sous la plus haute surveillance dès qu'ils entrent dans l'espace aérien américain» . Dès février2005, ces mêmes juristes insistent sur la procédure légale à suivre, «en particulier pour la collecte des communications à bord des avions» .

La désignation d'Air France comme risque majeur pour les intérêts et le territoire américains ne relève pas d'une simple hypothèse de quelques techniciens-espions de la NSA. Un cercle impressionnant d'autorités chargées de la sécurité du pays a été informé du «danger» représenté par la compagnie française. Le mémo de la NSA est, en effet, adressé à une vingtaine de destinataires, dont le commandement de la défense aérienne de l'Amérique du Nord, la CIA, le département Homeland Security (la sécurité intérieure), l'Agence de renseignement spatial (NRO), l'Agence de renseignement de la défense (DIA) ou encore l'état-major de l'armée de l'air. Cette fixation sur Air France sera constante au fil des années qui vont suivre et ne tient pas du hasard.

Le premier test de l'utilisation d'un smartphone en plein ciel a été effectué à bord du vol AF1046 d'Air France, le 17décembre 2007, sur une liaison Paris-Varsovie. «On a commencé tôt, confirme au Monde la direction d'Air France, mais, depuis, on n'a pas cessé de faire des tests, aujourd'hui, on s'apprête, comme les autres compagnies, à passer directement au Wi-Fi à bord.» La compagnie française, interrogée sur les pratiques des services secrets anglo-saxons, a d'ailleurs réagi avec mesure: «Nous ne sommes pas les seuls, visiblement, à avoir été visés et nous ne disposons d'aucun élément sur ces pratiques.»

Prises de guerre

En2012, le GCHQ note que 27 compagnies ont déjà permis aux passagers d'utiliser un téléphone portable ou sont sur le point de le faire, surtout pour les premières classes et les classes affaires des vols long-courriers. Parmi elles, British Airways (seulement data et SMS), Hongkong Airways, Aeroflot, Etihad, Emirates, Singapore Airlines, Turkish Airlines, Cathay Pacific ou encore Lufthansa. Air France est, pour sa part, un tel symbole de la surveillance des communications en avion que les services britanniques utilisent un croquis pleine page de l'un de ses avions pour illustrer le fonctionnement de l'interception en vol.

Pour prouver leur savoir-faire, le GCHQ et la NSA fournissent nombre d'exemples d'interceptions passées à bord de vols commerciaux d'autres compagnies. On trouve ainsi les relevés, le 23mars 2012, à 13h56, du vol Etihad ETD8271 des Emirats arabes unis, entre JFK et Denver, du Nice-Moscou du 20mai 2011 (Aeroflot) ou encore, la même année, du Milan-Doha (de Qatar Airways), du Athènes-Doha (toujours de Qatar Airways), du Jeddah-LeCaire (de la Saudi Airlines) ou du Paris-Mascate (d'Oman Air).

La collecte concerne également des Blackberry dont les codes PIN et les adresses e-mails sont identifiés dans un avion, le 2janvier 2012 à 10h23, sans que l'on connaisse sa destination et le nom de la compagnie. Les prises de guerre sont fièrement annoncées: voix, data, SMS, Webmail, Webchat, réseaux sociaux (Facebook, Twitter, etc.), Google Maps, Currency Converters, Media, VOIP, BitTorrent ou Skype. Au cours de leurs exercices d'intrusion, les services secrets britanniques découvrent, un peu surpris, qu'ils ne sont pas les seuls intéressés par ces communications en vol. Ils notent que la compagnie russe Aeroflot a mis en place un système de connexion spécifique pour les GSM à bord de ses appareils, «sans doute pour procéder à des interceptions...», glissent-ils dans une note technique.

Aujourd'hui, près d'une centaine de compagnies permettent de téléphoner en avion. «Les clients estiment désormais normal, voire nécessaire, de rester connecté en vol», assure la direction d'Air France. Les autorités en matière de sécurité aérienne ont toutes validé l'utilisation des GSM à bord des avions et les experts estiment que 2016, 2017 et 2018 seront les années historiques du portable en vol, notamment par l'installation pérenne du Wi-Fi en plein ciel.

De quoi étendre encore l'ampleur de l'espionnage en visant «plusieurs centaines de milliers de personnes» à surveiller, selon les projections de la NSA, soit un périmètre qui dépasse de loin les seules cibles reliées au terrorisme. L'espionnage politique ou économique des passagers en première ou en affaires sur des long-courriers intéresse d'ailleurs bien davantage les services.

La surveillance, elle, n'a aucune limite et chaque nouveauté est un défi technique qui paraît vite relevé. Les services semblent en être même un peu blasés. Les techniciens-espions de la NSA, dans une note interne de 2010, avaient même déjà la tête ailleurs. «Quel sera le prochain terrain d'expérimentation? Les trains? Il faudra qu'on regarde ça...»

New York Times
Europe Presses U.S. Tech Giants to Curb Online Hate Speech
Wednesday, 07 December 2016
Byline: Mark Scott

New York - European officials pushed on Tuesday for American technology giants to do more to tackle online hate speech across the region, adding to the chorus of policy makers worldwide demanding greater action from the likes of Facebook, Google and Twitter.
The rebuke came a day after many of those companies announced that they were joining forces to fight the spread of terrorist content on the internet, agreeing to share technology and information to prevent propaganda and other dangerous materials from being disseminated on their services.

Amid growing security tensions in much of the Western world, governments, intelligence agencies and advocacy groups want Google, Microsoft and other technology companies to take further steps to curb hate speech on digital platforms, as well as to clamp down on how terrorists circulate information online.

But freedom of expression campaigners have warned that such demands may limit people's ability to communicate across the internet, and they have cautioned that the line between hate speech and legitimate political discussion can be blurry.

In a report published on Tuesday, however, the European authorities signaled that only 40 percent of material flagged as possible hate speech online (albeit in a relatively small sample of 600 posts, videos and other online material) had been reviewed by the Silicon Valley companies within 24 hours. Of those 600 postings, just over a quarter was eventually taken down, the report said.

"While I.T. companies are moving in the right direction, the first results show that the I.T. companies will need to do more to make it a success," Vera Jourova, the European commissioner for justice, consumers and gender equality, said in a statement. "It is our duty to protect people in Europe from incitement to hatred and violence online."

Press officers for Google and Microsoft declined to comment. Representatives for Facebook and Twitter were not immediately available to comment.

In a recent interview, Richard Allen, Facebook's head of public policy in Europe, said that the social network was committed to tackling hate speech online, but that there was a fine line between what was legitimate under freedom of speech laws and what was required to protect people online.

"Our policies provide protection from hate speech," Mr. Allen said last month. "We shouldn't apply media regulation to the speech of ordinary citizens."

The report on Tuesday is part of European efforts to coax American technology companies to take more responsibility for what is published through their services. In May, companies including Google, Facebook and Twitter signed a voluntary code of conduct, agreeing to do more to tackle the rise of online hate speech across the 28-member European Union.

Some lawmakers, though, are not satisfied.

In Germany, where Facebook, in particular, has come under scrutiny, a government-backed task force is to report early next year on whether the social network, among other companies, has met national targets for responding to -- and potentially eliminating -- hate speech. Officials want companies to remove at least 70 percent of online hate speech within 24 hours of it being reported.

Heiko Maas, the German justice minister, has said that Facebook could even be held criminally liable for illegal hate speech posts, and he has called for legislation if the company does not meet its legal commitments.

"Facebook has a certain responsibility to uphold the laws," Mr. Maas said.

The social network denies any wrongdoing.

The Guardian (London)
Cable: new hacking scandal is likely without proper regulation
Wednesday, 07 December 2016
Byline: Jasper Jackson

London - Vince Cable is to call on the government to get on with creating a system of press regulation that matches the recommendations of the Leveson inquiry, or risk a repeat of the scandals that led to it. Speaking at an event organised by campaign group Hacked Off, the former business secretary will say that a new ministerial consultation on press regulation is delaying the implementation of Leveson's recommendations, which were made following the phone-hacking scandal.

"The government decision to consult again on the framework for self-regulation has the political effect of stopping progress towards a solution based on the royal charter model," he will tell an audience at the University of Westminster on Tuesday evening. "Suffice to say that the type of scandals which prompted Leveson will happen again in the absence of effective checks and balances."

He is also expected to argue that the government's failure to introduce new regulation exists within the context of a fear among politicians of powerful newspaper owners.

"Nothing better illustrates the deficiency of genuine plurality than the fear which politicians still have of crossing newspaper proprietors or the belief that party advantage will accrue from sucking up to them," he will say.

The speech is the fourth annual Leveson lecture organised by Hacked Off, which supported the creation of a press regulator backed by royal charter and has been heavily critical of industry-backed regulator Ipso.

The government announced the new 10-week consultation at the start of November to consider such issues as whether or not to introduce rules forcing newspapers to pay both sides' costs in libel cases if they do not sign up to a royal charter-backed regulator. The move came just days after Ipso rival Impress gained recognition under the charter, which was meant to trigger the so-called cost-shifting rules.

Newspaper publishers have argued that cost-shifting would have a chilling effect on journalism and is essentially a form of blackmail to force them to sign up to state-backed regulation.

Cable will also suggest that regulation could be used to help tackle the spread of false information, particularly if firms such as Google were brought under a voluntary system.

He is expected to say: "There surely has to be accountability for the algorithms these companies use, with greater disclosure, and named individuals who can be summoned to face democratic scrutiny."

"Bringing them within the framework of voluntary regulation, but with a regulator enjoying independence from the industry itself so it is genuinely faced with responsibility for retraction and redress, is a necessary next step which will also reassure the traditional print press that it is not being singled out for special punishment, as they claim."

Cable's hostility towards some parts of the media is well known. In 2010 he was recorded by two Telegraph journalists saying he had "gone to war with Murdoch" by intervening to block a takeover of Sky by the media mogul's News Corp.

Exposing Cable's views on Murdoch was deemed to be in the public interest by Ipso's predecessor, the Press Complaints Commission. However, the way the sting against Cable and other ministers was carried out breached the organisation's editorial code on subterfuge.

Cable's speech comes just hours after the News Media Association (NMA), which represents the UK's national and regional newspapers, took the first step towards launching a judicial review of the decision by the Press Recognition Panel to give the go-ahead to Impress.

In a pre-action letter, the NMA claims that the PRP decision was not legal because Impress, which is indirectly funded by former F1 tycoon Max Mosley, failed to meet criteria in areas such as its funding, what rules it imposes and how much support it has from the newspaper industry.

The NMA said it had been "advised that it has a powerful case that the Press Recognition Panel made serious and fundamental legal errors in its recognition of Impress".

New York Times
Kremlin Updates Its Plan to Counter Cyber Threats
Wednesday, 07 December 2016
Byline: Andrew E. Kramer

Moscow - The Kremlin published a new plan on Tuesday to defend Russia against what it described as stepped-up cyberattacks and "information-psychological" methods by foreign intelligence agencies bent on influencing its population with online information.
The plan updates a similar information security doctrine put in place by President Vladimir V. Putin in 2000, early in his first term, that staked out a renewed role for post-Soviet government in monitoring information.

The latest iteration of the doctrine comes as American officials have mulled retaliating against Russia for what the Department of Homeland Security said was government- orchestrated hacking before the presidential election, including stealing emails from the Democratic National Committee.

The plan, signed by Mr. Putin on Monday but published on Tuesday, described a threat to Russia of technological malfeasance similar to what the United States has accused the Russians of committing. It did not mention, however, any specific online strikes against Russia indicating that American retaliation could be underway.

Russia, the document says, is at risk of attacks on systems of "information support for democratic institutions" and the spread of harmful, false information.

It notes the "increasing scale of certain countries and organizations using information technologies for military and political goals."

The 16-page document sketches out what the Kremlin sees as the main threats to its security and national interest from foreign information making its way into the country, and sets priorities for countering them. It identifies terrorist recruiting and financial crime as dangers.

Under Mr. Putin, the Kremlin has staked out a role as a defender of conservative values, notably pushing back against gay rights, and the new doctrine is no exception, with a clause raising concern about risks to "traditional Russian spiritual and moral values" of Russian young people.

It also notes the risk to Russia of "a tendency toward an increase of materials containing biased assessments of the state policies of the Russian Federation in foreign media."

The doctrine supports a plan, in the works for some time, to gain control over the Russian segment of the web by basing more servers inside the country. The plan envisions operating the Russian internet autonomously, if needed in time of war, by switching it off from the rest of the world.

And it directs Russian diplomats to pursue the Kremlin's policy goals on information security at international organizations like the United Nations.

Russia has advocated, without much success so far, replacing the nonprofit group that now controls top-level domains with a global agency, the International Telecommunication Union.

The document calls attention to "information-psychological actions" from abroad undermining Russian "patriotic traditions of defending the Fatherland."

Russia has already passed laws aimed at regulating internet content and forcing foreign companies to base data servers in Russia. Last month, a Moscow court ordered internet service providers to block LinkedIn, the professional social networking site, for failing to comply.

Under a separate law governing news aggregators, sites with daily traffic exceeding 1 million users would bear responsibility as publishers, including a requirement to verify the truthfulness of the articles reposted on their websites. The law would apply to Google, among other aggregators.

A spokesman for the regulator, Roskomnadzor, on Tuesday denied a report in the Izvestiya newspaper saying Russian officials had already instructed Google to comply.

Bloomberg View
Russia Expects a Taste of Its Own Cyber Medicine
Tuesday, 06 December 2016
Byline: Leonid Bershidsky
Section: column

Column - Russia, demonized as the biggest cyber-villain in the world in the wake of the U.S. election campaign, must now take special care of its own information security. Its adversaries don't just possess powerful cyber spying and offensive capabilities -- they suspect Russian involvement in every incident, and that makes Russia vulnerable to all kinds of retaliation.
After it was accused of trying to influence the U.S. presidential race, Russia faces the same charges in Germany. Given Chancellor Angela Merkel's support of anti-Russian sanctions and her deep- seated support of a close partnership with the U.S., Russian President Vladimir Putin has strong motives to undermine her. Last week, Wikileaks, which appeared to closely coordinate its U.S. election-related publications with Russian propaganda outlets such as the RT channel and Sputnik network of websites, published material from a German parliamentary inquiry into the cooperation between Germany's BND

intelligence service and the U.S. National Security Agency. The issue is politically sensitive to privacy-minded Germans, who do not appreciate their country's collaboration with the intrusive U.S. service. The Russian propaganda organizations were on it immediately.

Merkel's government anticipates more than leaks. Late last month, about 900,000 customers of Germany's biggest internet provider, Deutsche Telekom, experienced outages after what appeared to be an attack on a particular type of router. The company said the problems were caused by "deliberate hacking," and German politicians wasted no time in hinting at Russian involvement. Merkel said she didn't have any specific information about the Deutsche Telekom attack, but added, "Let me just say that such cyberattacks, or 'hybrid attacks' as they're known in Russian doctrine, are part of everyday life today, and we need to learn to deal with them."

In a recent interview with the daily Sueddeutsche Zeitung, Bruno Kahl, the head of the BND, said he had evidence Russian was undertaking cyberattacks "which have no other purpose but to cause political uncertainty." Add the powerful, well-funded BND to the U.S. intelligence services plotting to prevent Russian attacks, and the Kremlin has a serious problem.

Putin clearly understands that and feels the need to shift the narrative or at least signal his preparedness. On Monday, he approved a new Russian information security doctrine which mentions "a number of foreign countries increasing their technological capacity to impact" Russian infrastructure "to attain military goals." It also talks about foreign intelligence services attempting to "exert psychological influence by information means in order to destabilize the domestic political situation in various regions of the world and undermine the sovereignty and territorial integrity of states."

According to the document, the Russian stance against such practices is defensive. But it is more likely an attempt to justify cyberattacks and the spreading of propaganda in the Kremlin's favorite way - - by saying everybody else does it too.

The new doctrine was published on the day the FSB, Russia's domestic intelligence service, said it expected the start of a major cyberattack by "foreign special services" against the Russian banking sector. On Dec. 2, the FSB said in a brief statement that Russian banks would be attacked from servers in the Netherlands owned by the Ukraine-based hosting company BlazingFast. At the same time, the FSB said, social networks would fill with panic-inducing messages about the collapse of certain banks and the central bank's plans to strip them of licenses.

The threat apparently was taken seriously. The communications ministry held meetings with bankers and internet providers, and the central bank offered extra liquidity in case there's a bank run. Monday came and went, though, and nothing happened to Russian banks; no panic spread through social networks, either. A BlazingFast representative suggested that the publicity scared off any hackers that might have planned the attack, but the FSB announcement also may have been part of a Kremlin campaign to present Russia as a victim rather than an instigator of hybrid warfare in cyberspace.

Though the Ukrainian firm -- a legitimate infrastructure provider with a branch in Amsterdam -- wasn't directly accused of involvement in the cyberattack, Russia has plenty to fear from Ukrainians. Unlike the U.S. and German spy agencies, careful not to start an all-out war with Russia, Ukraine is already involved in a proxy war with its eastern neighbor. It is also a lawless place full of excellent information technology specialists. The recent global operation to roll up Avalanche, a giant botnet used by cybercriminals for various malware attacks that have caused hundreds of millions of dollars in damage, culminated in the arrest of Hennady Kapkanov, a Ukrainian citizen, in Poltava. Avalanche was just the type of criminal network that could be used for an attack on a country's banking system, and it was far from the only one or even the biggest.

It was a Ukrainian hacktivist group that breached the email of Putin adviser Vladislav Surkov in October. They didn't find anything particularly sensational, but they did demonstrate their ability to hack Kremlin servers.

Moscow has long been worried about the dominance of Western software and the wide reach of U.S. internet companies. Last week, Natalya Kasperskaya, head of the InfoWatch information security company suggested that the Russian government stake a claim to all the data collected from Russian citizens on the internet before foreign companies get their hands on it. Russia has introduced stringent rules for internet firms, obliging them to store Russians' personal data within the country. Now, though, it's no longer a matter of protectionism or even securing Russians' personal data: Russia has every reason to expect attacks on its critical systems perpetrated in retaliation for Russian meddling in foreign elections.

Making sure these attacks don't come is a matter of constant vigilance. The FSB warning may even have been a drill. It also helps if elections in Western countries are won by people who won't be interested in retaliating. Donald Trump probably isn't. If indeed Putin has authorized election meddling and Western intelligence agencies have proof of that, we can expect that he will double down on the activity and step up the cyberwar.

La Presse (site web)
Surveillance: les commissaires à la vie privée demandent un meilleur encadrement de la police
Tuesday, 06 December 2016
Byline: Vincent Brousseau-Pouliot

Ottawa - Citant les révélations d'Edward Snowden et les cas de journalistes surveillés au Québec, les commissaires à la protection de la vie privée du pays mettent le gouvernement Trudeau en garde: au lieu de donner de nouveaux pouvoirs aux corps policiers, Ottawa doit plutôt mieux encadrer les pouvoirs policiers existants en matière de surveillance.
Dans le cadre de la consultation du gouvernement Trudeau pour moderniser le cadre de sécurité nationale, le commissaire à la protection de la vie privée du Canada Daniel Therrien ainsi que tous ses

homologues provinciaux demandent à Ottawa de ne pas hausser les pouvoirs policiers en matière de surveillance.

«Ces agences ont vu leurs pouvoirs augmentés de façon très considérable ces dernières années, particulièrement en vertu des projets de loi C-51 et C-13. En même temps, dans la foulée du 11 septembre 2001, nous avons été témoins trop souvent d'activités inappropriées ou même illégales de la part d'agents de l'État qui portaient atteinte aux droits des citoyens ordinaires qui n'étaient pas soupçonnés d'aucun crime ou activité terroriste. À mon avis, ces écarts s'expliquent par l'absence de normes claires qui encadrent suffisamment l'action de l'État», a dit le commissaire à la protection de la vie privée du Canada Daniel Therrien, en conférence de presse ce matin à Ottawa.

Le commissaire Daniel Therrien estime que «des garanties juridiques claires sont nécessaires pour protéger les droits et les abus, que les organismes de sécurité nationale doivent faire l'objet d'un contrôle efficace, et que l'octroi de nouveaux pouvoirs à l'État doit être justifié par des faits réels.»

«Sans vouloir faire comparaison» avec les services de renseignement des ex-républiques de l'Europe de l'est, le commissaire Daniel Therrien rappelle toutefois une décision récente de la Cour fédérale dénonçant le fait que le Service canadien du renseignement de sécurité (SCRS) a conservé de façon illégale pendant plusieurs années des métadonnées de citoyens canadiens (le SCRS interprétait la loi différemment et s'est plié à la décision de la Cour fédérale). «Nous parlons ici de retenir des données de citoyens ordinaires. Je ne crois pas que c'est le type de société dans laquelle [les Canadiens] veulent vivre», dit le commissaire Daniel Therrien.

Métadonnées

Les commissaires de protection de la vie privée s'inquiètent particulièrement de la collecte de métadonnées des citoyens (ex: leurs numéros de téléphone et non le contenu de leurs conversations). À ceux qui demandent de baisser le seuil juridique pour obtenir un mandat pour accéder à des métadonnées auprès d'un juge, le commissaire Daniel Therrien rappelle que le projet de loi C-13 a abaissé l'an dernier le seuil «à un motif raisonnable d'avoir un soupçon». «Je ne peux pas concevoir un test moins exigeant», dit le commissaire Daniel Therrien, qui s'oppose à la suggestion de certains intervenants que des métadonnées pourraient être obtenues par les forces policières en vertu d'une autorisation administrative.

Les commissaires de protection de la vie privée aimeraient aussi que les conditions d'obtention des métadonnées soient mieux encadrées, «de sorte que les juges aient en tête le caractère sensible des données» selon le commissaire Daniel Therrien. «Les métadonnées peuvent révéler davantage que le contenu des enregistrements», dit-il.

Les métadonnées devraient ainsi être aussi difficiles au plan juridique à obtenir que le contenu des enregistrements, selon les commissaires à la vie privée. Les forces policières devraient ainsi démontrer qu'il s'agit d'une mesure de dernier ressort et que d'autres méthodes d'enquête ont été utilisées. «On

pourrait limiter [l'accès aux métadonnées] aux crimes les plus graves», suggère aussi le commissaire Daniel Therrien.

Encryptage

Les commissaires à la protection de la vie privée «exhorte» le gouvernement fédéral «à faire preuve de prudence» avant de songer à légiférer sur l'encryptage, un «outil essentiel pour la protection des renseignements personnels». «Il n'existe aucun moyen connu de donner un accès systémique au gouvernement sans exposer parle fait même la population générale à un risque importante à la sécurité de leurs données», écrit le Commissariat à la protection de la vie privée du Canada.

Les commissaires à la protection de la vie privée accueillent favorablement l'idée de créer un comité de députés sur la sécurité nationale et le renseignement, mais suggère de leur adjoindre des experts «afin d'assurer une protection efficace des droits».

En conférence de presse, le commissaire à la protection de la vie privée du Canada Daniel Therrien était accompagné de ses homologues de l'Ontario Brian Beamish et du Québec Jean Chartier. «Nous pensons que même le processus judiciaire reste à parfaire et mérite d'être mieux encadré. [...] Les pouvoirs policiers qui recherchent davantage de pouvoirs n'ont jamais fait la preuve [...] que le système actuel ne fonctionnait pas», dit Me Jean Chartier, président de la Commission d'accès à l'information du Québec.

Le gouvernement Trudeau a lancé a lancé cette année une consultation sur la modernisation du cadre de sécurité nationale. Les commissaires à la protection de la vie privée ont déposé aujourd'hui un mémoire commun.

Korea Herald
Military intranet hacked by North Korea
Wednesday, 07 December 2016
Byline: Yoon Min-sik

Seoul - South Korea's Defense Ministry said Tuesday the military's intranet had been hacked for the first time ever, presumably by North Korea, resulting in a number of military secrets being leaked.
The military found that malicious code had been spread on its computers via its servers used to relay updates on Sept. 23.

"The military formed a cyber investigative team to look into this matter and found that some military data -- including confidential information -- has been leaked. It appears to be a North Korean act," the ministry said.

Code used in the attack has certain similarities with that previously used by North Korean hackers, a ministry official explained.

He added that the attack originated from Shenyang, China, where many North Korean hackers are believed to be based and which was the believed origin of a 2014 attack on Korea Hydro & Nuclear Power Co.

But the official refused to specify what data had been stolen.

"We cannot give out details on what information was leaked, because it might give (North Korea) an advantage in the ongoing cyber warfare," he said. He also refused to confirm how many computers were hit by the cyberattack, but added that multiple servers in the intranet was infected.

The military said that none of the data from other countries that has signed intelligence sharing agreements with South Korea has been stolen.

The incident raised questions about the security of what the military had basically described as "unreachable."

The military's manual states that no classified information can be saved on computers connected to the internet, and that the line must be cut off during the operation and any activity must be erased afterwards.

But some of the computers -- located in one of the bases -- linked to the intranet was connected to the internet due to "administrative carelessness and violation of regulation," the ministry said.

The connection opened a path to infection of malicious code, allowing hackers to remotely control the computers and steal the data.

While the first large- scale activity took place on Sept. 23, some of the code that allowed the attack had already been planted on Aug. 8.

During the hacking attack on the Korea Hydro & Nuclear Power Co. in 2014, officials had also claimed that a hacker could not infiltrate its intranet because it was cut off from outside.

As follow-up measures for the attack, the military outlined 14 tasks to step up cyber security. This includes procuring a measure to monitor the section where the internet and the military intranet could be interlinked and replacing the current computer vaccine system.

Reuters
China shuts thousands of illegal live streaming accounts - Xinhua
Wednesday, 07 December 2016
Byline: Staff reporter

Shanghai - Beijing-based live streaming websites have shut down thousands of illegal accounts after new regulations by Chinese internet authorities guarding against violent and obscene content came into effect, the official Xinhua news agency said on Wednesday.
The Cyber Administration of China (CAC) formalised controversial rules regulating the country's fast-growing live-streaming video industry in November, in a move that stripped out smaller competitors and placed hard-line surveillance measures on leading firms.

More than 4,500 accounts on Beijing-based websites had been closed and more than 3,100 live streaming programmes had been shut, Xinhua reported the CAC as saying.

"Reports of violent, obscene and vulgar content on live- streaming websites abound," Xinhua said.

The new rules, which came into effect on Thursday, require streaming services to provide information on users who stream content the government deems a threat to national security or social order.

CAC officials said they would enhance regulations further and called on the public to engage in supervising the internet.

The National (UAE)
UAE's digital security has room for improvement
Wednesday, 07 December 2016
Byline: Caline Malek

Dubai - Building a layered security network that has the trust of the local population and shares data among governments departments is just one of the ways the UAE can protect itself from digital threats, experts have said.
Although the UAE has been working on its e-government services for the past two and a half years, there is room for improvement.

"The GCC will cross the UK and Europe in the next few years in smart automation," said Dr Usman Zafar, chief executive at Duc International Consulting in the UAE. "But as citizens, we want information at the right time so pushing information has become crucial."

He said large investments in data centres had not achieved any return. "There is no unified integration," he said at the second day of Biometrics Middle East Conference on Tuesday.

"Government departments work in silos and don't communicate so you can't get a smart service. We need interoperability and we need to find a mechanism to enable scattered government systems to talk to each other."

Dr Zafar said a national framework was needed to share data as it removes barriers and allows for better collaboration among ministries.

Gaining more trust from the community in e-government services is another crucial factor for success.

"Innovation has no geographic boundaries," said Daniel Hughes, managing director at Forge Training and Management Consulting in the UAE and former head of navigation at the UAE Navy Forces Institute. "It's been a core part of every region and it's leading to a lot of the new developments."

He said a lot more innovation in biometrics could happen but consumers lacked trust in technology.

"We're moving down the path of biometrics," he said. "From cardiac rythm to vein patterns in our fingers and eyes, it is what we are. The technology is there and it's easy to use but it's the individuals that use that data to spread it that cause problems."

For Richard Castillo, master trainer and consultant at the firm, a layered security is vital as it is one of the most effective tools for enforcement.

"One of the key elements of layered security is criminals never know what to expect," he said. "They have very strong intelligence but technology and biometrics has had such an impact on enforcement operations. There is no single security solution, to me it's a combination and every layer of security is crucial, from the officers, to the training, technology, biometrics verification and private sector assistance."

Mr Castillo, who has worked in airports, land borders and alongside customs and security enforcement, said the Gulf has been targeted.

"There are threats here like everywhere," he added. "We're talking about money laundering because it's a passageway for commerce so every business should have a layered security in place."

Although he said the UAE had very good security features, but there was room for improvement. "There is no one country that has a 100 per cent fault proof system," he said. "But it requires an educational effort."

Canadian Press
RCMP fabricated response to access-to-info request 'unacceptable:' Goodale
Thursday, 08 December 2016

OTTAWA _ Public Safety Minister Ralph Goodale says it's "unacceptable" that an RCMP employee fabricated a response to an access-to- information request.
Goodale says the individual involved was "at a very junior level" and has been disciplined.

The fabrication was revealed last week in a letter from RCMP Supt. David Vautour to Bruce Cheadle, a reporter for The Canadian Press who in May 2015 had requested information regarding the now-defunct long-gun registry.

Cheadle did not receive a response to his access request until March 1, 2016, but that letter was backdated almost five months.

Vautour said a note included with the tardy response claimed that the letter had originally been sent to Cheadle in October 2015, but was returned to the RCMP by Canada Post due to an incorrect postal code.

He said the Mounties have since determined that the backdated letter and the explanatory note were fabricated to avoid a possible complaint about the delay in responding to the request.

"Our office does not condone actions that are contrary to the RCMP core values of honesty, integrity and professionalism," Vautour wrote Cheadle.

"We want to advise you that we have addressed this matter through a formal disciplinary process and made the Office of the Information Commissioner aware of this matter."

Goodale noted that it was the RCMP itself that discovered the fabrication and informed both Cheadle and the access-to-information watchdog.

"This behaviour is not tolerated and discipline has been delivered," Goodale said Wednesday.

Ironically, Cheadle's original access request involved the issue of backdated legislation which retroactively absolved the RCMP of any wrongdoing when it illegally destroyed long-gun registry records even as Legault was conducting an investigation into a complaint about access to those records.

Stephen Harper's previous Conservative government passed the Ending the Long-gun Registry Act in April 2012 and then pushed the Mounties to quickly destroy the data, despite assuring Legault that the records would be preserved until her investigation was completed, as legally required.

When Legault subsequently informed the government that the RCMP had committed an alleged offence, the Conservatives re-wrote the law, retroactively stripping Legault of her jurisdiction over the

registry records, absolving the Mounties of any wrongdoing and shutting down an active investigation into the matter which had been started by the Ontario Provincial Police.

As part of his coverage of that story, Cheadle had submitted an access request for copies of electronically scanned long-gun registration application forms and transfer applications. The backdated response he received informed him that the Access to Information Act no longer applied to the requested records.

Despite the fabricated date and explanation for the delay in responding, Vautour said the substance of the response "was accurate."

Cheadle has lodged a formal complaint with Legault's office about the fabrication.

In June 2015, Legault filed a court challenge to the constitutionality of the retroactive law, arguing that it undermines the rule of law and government access-to-information systems across the country.

However, the court case has been on hold for months as Prime Minister Justin Trudeau's year-old Liberal government attempts to negotiate a settlement.

Xinhua News Agency
Third China-U.S. cyber security ministerial dialogue convenes in Washington
Thursday, 08 December 2016
Byline: Staff reporter

Washington - The third China-U.S. ministerial dialogue on fighting cyber crimes was held here Wednesday.
The dialogue was co-chaired by China's State Councilor and Minister of Public Security Guo Shengkun with U.S. Attorney General Loretta Lynch and Secretary of Homeland Security Jeh Johnson.

In his remarks to the meeting, Guo noted that under the auspices of Chinese President Xi Jinping and his U.S. counterpart Barack Obama, China-U.S. cooperation in safeguarding cyber security is booming and has yielded positive outcomes in cracking down on cyber crimes and related matters.

Calling the current China-U.S. cooperation in cyber security a link between past and future, Guo proposed that the two sides press on in using the dialogue mechanism as the main channel for communication in tackling cyber security issues, give prompt and effective response to the requests from the other side, and constructively manage their differences.

The U.S. side said that China and the United States share common interests in fighting cyber crimes and protecting cyber security, and the high-level dialogue mechanism also serves as a crucial platform for

candid communication and enhancing mutual understanding and trust between law enforcement officials of the two countries.

U.S. officials also called for continuing and developing the current dialogue mechanism to jointly fighting cyber crimes, including cyber terrorism and e-mail fraud.

The two sides agreed to convene the next cyber security ministerial dialogue in China in 2017.

ABC (Australia)
Cyber security war game set in 2022 hopes to prepare governments, businesses for the worst
Thursday, 08 December 2016
Byline: Matthew Clayfield

Australia's first simulated cyber security "game" kicks off at the National Security College of the Australian National University.
Australia's first simulated cyber security "game" was set in 2022 and explored two equally unpalatable cyber attack scenarios in the hopes to prepare governments and businesses for the inevitable.

The game was co-hosted by the National Security College at the Australian National University and the RAND Corporation, bringing together 90 participants from government, business and academia.

Michelle Price, senior adviser in cyber security at the National Security College who helped to co-ordinate the game, said Australians "human behaviour" in cyber space needed to improve.

"It's in large part why we're such a significant target for malicious activity," she said.

Australia is currently losing up to $17 billion each year through malicious cyber activity.

And the attacks on this year's Census website remain an equally stark reminder of what can happen when organisations are unprepared.

Professor Rory Medcalf, head of the National Security College, said the game was a full-scale simulation of the "kind of complex cyber security attacks Australia could face in years to come".

"The whole point is to bring together senior levels of the private sector, the government, the bureaucracy, to make very quick complex decisions against uncertain challenges," he said.

Game designed to work out what needs to change now

Participants included ministers and shadow ministers, state and federal agencies, and representatives of the Australian Securities Exchange.

They were presented with two strategic scenarios set six years from today and forced to develop solutions to problems while taking into account their various interest and concerns.

Ms Price said each person in the room took on a role across the six different groups, to ensure the questions that the facilitator asked everyone to focus on were approached "from different points of view".

"To try and work out if we did find ourselves in different circumstances in 2022, which of course we will, how would we respond at that time," she said.

"What are the kinds of things that we need to do over the next couple of years to either course correct on our policy setting, or which parts of the current policy settings we need to keep working on embedding."

Cyber security 'needs to be an automatic behaviour'

She said that while the game was designed to be challenging, it's real purpose was to generate conversations and ideas.

"Most Australians don't understand why cyber security is important to them as individuals," she said.

"That's not just adults, that's also children.

"We need to make sure that across the board cyber security is something that becomes an automatic human behaviour.

"So that we not only understand it, but we appreciate why it's so important that we make sure we're secure when were online."

Dan Tehan, the federal minister assisting the Prime Minister for cyber security, was among the game participants and said the Government had put in place a cyber security strategy in April this year and were implementing it.

"That strategy clearly defines the need for government, for business, for academia and for the community to work hand in hand," he said.

"It's going to be a whole of community approach and what we're going to do today is map how we can get all sectors of the economy working together to deal with the cyber threat."

Press Trust of India
More attacks on cloud, IoT devices likely in 2017: Symantec
Thursday, 08 December 2016

New Delhi - Higher instances of attacks on cloud and Internet- connected devices are likely in the coming year as cybercriminals evolve their approach towards accessing enterprise and consumer data, security software maker Symantec today said.
"Given the significant shift towards cloud-based storage and services, the cloud is becoming a very lucrative target for attacks. The cloud is not protected by firewalls or more traditional security measures, so there will be a shift in where enterprises need to defend their data," Symantec Director Solutions Product Management APJ Tarun Kaura said. He added that attacks on cloud could result in multi- million dollar damages and loss of critical data.

"Given the consistently changing security landscape, it's important to take a moment and determine where the security industry needs to focus their attention as we move into the next year," Kaura said unveiling Symantec's security predictions for 2017.

Highlighting the proliferation of devices connected to the cloud and Internet, he said the shift toward "modern workplace" where businesses allow employees to introduce new technologies like wearables and virtual reality will continue.

"Enterprises will need to shift their focus from safeguarding end-point devices toward protecting users and information across all applications and services. They will have to look beyond computers and mobile devices for vulnerabilities," he said.

Kaura added that nearly everything in an enterprise is now connected to the internet and will need to be protected.

Another security challenge that may gain traction is 'fileless malware'. Fileless infections are those written directly onto a computer's RAM without using files of any kind. These are difficult to detect and often elude intrusion prevention and antivirus programs. "This type of attack increased throughout 2016 and will continue to gain prominence in 2017, most likely through PowerShell attacks," he said.

Kaura also highlighted the issue of rogue nation states financing themselves by stealing money. "There is a dangerous possibility that rogue nation states could align with organised crime for their personal gain, such as what we saw in the SWIFT attacks. This could result in down time for countries' political, military or financial systems," he said.

In February this year, a group of cybercriminals stole USD 81 million from the Bangladesh central bank. The attack triggered an alert by payments network SWIFT after it was found the attackers had used malware to cover up evidence of fraudulent transfers.

In October, the Indian banking sector saw the biggest-ever security breach with 32 lakh debit cards of various public and private sector banks being feared to have been 'compromised' by cyber malware attack in some ATM systems.

Times of India
Hackers operated Twitter handles of Rahul, Congress from 5 countries (Canada).
Thursday, 08 December 2016
Byline: Somreet Bhattacharya

New Delhi - The Twitter handles of Rahul Gandhi and the Congress which were recently hacked were operated from five countries including the US, Delhi Police on Wednesday said.
The Economic Offences Wing (EOW), which is probing the matter, received a reply around three-four days ago from Twitter headquarters on the Internet Protocol (IP) addresses used by the hackers to send derogatory tweets from these accounts, a senior police officer said.

"We have got to know that the IP addresses from where the accounts were accessed don't fall under our jurisdiction. The Twitter handle logs show both the accounts were operated from five countries - Sweden, Romania, the US, Canada and Thailand. We will write to the Internet service providers of these countries to share details of users with us and that is how the investigation will proceed," the officer said.

Analysis of the data shows that the accounts were accessed from these countries on November 30 from 9.15am to 9.30am and from 10:30am on December 1, the officer added.

In case, police do not get the necessary details, they might have to initiate the process of sending Letters Rogatory to competent courts in these countries for assistance, sources said. According to the officer, police are yet to get log details of the Congress website from the party's server.

Police had lodged two FIRs in connection with the hacking of the two Twitter accounts, the party website and the email accounts of Congress and Rahul on December 1 following two complaints from Congress chief spokesperson Randeep Surjewala to the EOW.

Rahul's Twitter account was hacked on November 30 and some remarks full of expletives were posted. On December 1, his email account was also hacked, the party had claimed. Two cases under section 66 of IT Act were registered, police had said.

Haaretz
U.K. Intelligence Called Israel 'True Threat' to Middle East
Thursday, 08 December 2016

Jerusalem - British intelligence spied on Israeli diplomats and firms in addition to its military, the French daily Le Monde reported on Wednesday, based on leaked documents that came into the possession of whistleblower Edward Snowden. In one of the files, Britain's GCHQ intelligence-gathering apparatus defined Israel as "a true threat" to the Middle East.
"The Israelis constitute a true threat to regional security, notably because of the country's position on the Iran issue," a leaked top- secret document from 2009 said.

According to Le Monde, the GCHQ collected information on Israeli diplomats, including a person described by the newspaper as the second-highest ranking official in the Israeli foreign ministry. That person was not named. The British also spied on the Palestinian Authority, the report said.

Email correspondence belonging to the Israeli ambassadors to Nigeria and Kenya was also the subject of British intelligence-gathering efforts as was Ophir Optronics, a firm deemed to be tied to the Israeli defense establishment that specializes in fiber optics, and the Hebrew University of Jerusalem's Racah Institute of Physics.

According to Le Monde, the GCHQ kept track of the phones of Palestinian Authority President Mahmoud Abbas as well as that of his two sons, Yasser and Tarek Abbas, on December 9, 2008. Noting that these interceptions occurred three weeks before Israel's military offensive in Gaza in January 2009, the newspaper suggests they may have served to aid Israel to prepare for the operation.

From the end of 2008 through 2009 the British agency monitored communications among the PLO secretary general and numerous Palestinian delegations, in particular those in France, Belgium, Portugal, Pakistan, South Africa and Malaysia. It also spied on Israeli Arab lawmaker, Dr. Ahmad Tibi, and former Palestinian Prime Minister Ahmed Qurei.

A 2008 note from the American security agency, the NSA, revealed in the Snowden archives, and cited on the American site The Intercept, described the Palestinian Authority's security forces as "no threat to the United States or its allies...and these forces are frequently the best informed on violence in the region."

Another NSA document from April 18, 2013 cited "the great closeness of the NSA dating back to the 1980s with the Electronic Warfare Directorate, Jordan's technical secret services. The two cooperate on priority targets and the Jordanians provide a large portion of the names of individuals targeted by the NSA in the region."

The Le Monde report followed a previous publication based on documents stolen by Snowden dealing with spying by U.S. and British intelligence on Israeli military aircraft.

For 18 years, GCHQ and its American counterpart, the NSA, had collected drone transmissions after cracking the Israeli army's encryption for communication among fighter jets, drones and army bases. The information was reported in January by The Intercept and the German newspaper, Der Spiegel.

Britain and the United States reportedly have used this access to monitor Israel Defense Forces operations in the Gaza Strip, watch for a potential strike on Iran and keep tabs on drone technology that Israel exports. Snowden worked for U.S. intelligence before publishing classified material in 2013 and fleeing to Russia.

Reuters
Germany sees increase in Russian propaganda, cyber attacks
Thursday, 08 December 2016
Byline: Staff report

Berlin - Germany's domestic intelligence agency on Thursday said it had seen a striking increase in Russian propaganda and disinformation campaigns aimed at destabilizing German society, and targeted cyber attacks against political parties.
"We see aggressive and increased cyber spying and cyber operations that could potentially endanger German government officials, members of parliament and employees of democratic parties," Hans-Georg Maassen, head of the domestic BfV intelligence agency, said in statement.

Maassen, who raised similar concerns about Russian efforts to interfere in German elections in an interview with Reuters last month, cited what he called increasing evidence about such efforts and said further cyber attacks were expected.

The agency said it had seen a wide variety of Russian propaganda tools and "enormous use of financial resources" to carry out "disinformation" campaigns aimed at the Russian-speaking community in Germany, political movements, parties and other decision makers.

The goal of the effort was to spread uncertainty in society,"to weaken or destabilize the Federal Republic of Germany," and to strengthen extremist groups and parties, complicate the work of the federal government and influence political dialogue.

The agency said it had seen a "striking increase" in spea-phishing attacks attributed to a Russian hacking group APT 28, also known as "Fancy Bear" or Strontrium, the same group blamed for the hack of the U.S. Democratic National Committee this year and a cyber attack on the German parliament in 2015.

The attacks were directed against German parties and members of parliament, the agency said, adding they were carried out by government bodies posing as "hacktivists".

"Propaganda and disinformation, cyber attacks, cyber espionage and cyber sabotage are part of the hybrid threat facing western democracies," Maassen said.

German officials have accused Moscow of trying to manipulate German media to fan popular angst over issues like the migrant crisis, weaken voter trust and breed dissent within the European Union so that it drops sanctions against Moscow.

But intelligence officials have stepped up their warnings in recent weeks, alarmed about the number of attacks.

Last month, German Chancellor Angela Merkel said she could not rule out Russia interfering in Germany's 2017 election through Internet attacks and misinformation campaigns.

Russian officials have denied all accusations of manipulation and interference intended to weaken the European Union or to affect the U.S. presidential election.

U.S. intelligence officials had warned in the run-up to the Nov. 8 presidential election of efforts to undermine the credibility of the vote that they believed were backed by the Russian government.

The Intercept
Drowning in Information: NSA Revelations From 262 Spy Documents
Thursday, 08 December 2016
Byline: Micah Lee, Margot Williams

Washington - By the first half of 2004, the National Security Agency was drowning in information. It had amassed 85 billion phone and online records and cut the ribbon on a new hacking center in Hawaii -- but it was woefully short on linguists who could make sense of captured communications and lacked enough network analysts to effectively monitor all the systems it had hacked.
The signals intelligence collected by the agency was being used for critically important decisions even as NSA struggled to understand it. Some bombs in Iraq were being targeted based entirely on signals intelligence, a senior NSA official told staff at the time -- with decisions being made in a matter of "minutes" with "less and less review."

Information overload is just one of several themes running through 262 articles from the NSA's internal news site, SIDtoday, which The Intercept is now releasing after careful review. The documents also detailed an incident in which the Reagan administration appears to have leaked classified intelligence to the press for political purposes, described in an accompanying article by reporter Jon Schwarz.

SIDtoday articles published today also describe how the NSA trained FBI agents, enabled U.S. intervention in Latin America, and, with the help of a gifted analyst at the Defense Intelligence Agency, learned the value of simply reading information that was already public. One document even suggests that NSA personnel routinely got dangerously chatty at restaurants near headquarters. These stories and more are described in the highlights reel below. The NSA declined to comment.

Dropping Bombs in Iraq "With Less and Less Review"

A top NSA official disclosed in a January 2004 SIDtoday column that U.S. forces were "dropping bombs" based entirely on signals intelligence, the type of intelligence collected by the agency. He then implied that the American officers involved risked prosecution for war crimes.

Charles Berlin, chief of staff in the Signals Intelligence Directorate, recounted an anecdote about a former commander of his who, in one session in the winter of 1995-96, personally reviewed more than 100 possible airstrike targets in the Balkans. The commander's motivation, Berlin said, was to protect his underlings from being prosecuted for war crimes, and his actions "really brought home the concepts of responsibility and accountability."

"For us today this lesson is especially important," he added. "The planning cycle for dropping a bomb has compressed from a day to minutes and the criterion for the aiming point has less and less review."

"As many of you know, our forces in Iraq are dropping bombs on the strength of SIGINT alone. We are proud of their confidence in us, but have you ever considered the enormous risk the commanders are assuming in this regard? Are you ready to share that risk?"

Inside the NSA's Call-Logging Machine

Among the ways the NSA identified potential terrorists was through a practice known as "information chaining," which uses communications metadata to draw a social graph. And there's no question the agency had lots of metadata: As of 2004, the NSA had amassed a database of more than 85 billion metadata records related to phone calls, billing, and online calls -- and was adding 125 million records a day, according to a January 2004 SIDtoday article titled "The Rewards of Metadata."

The database, known as FASCIA II, would at some unspecified point in the future begin processing 205 million records a day and storing 10 years of data, the article added. One of the world's largest Oracle databases at the time, FASCIA II held metadata records from telephone calls, wireless calls, billing, the use of media over the internet, and high- powered cordless phones, with plans to add email metadata in the future.

The article explained that metadata is used by the agency in the process of "information chaining," in which analysts spy on relationships between people. It further claimed that two senior al Qaeda operatives had been captured with the help of such techniques. A March 2004 SIDtoday article said a chaining tool called MAINWAY helped a counterterrorism analyst uncover six new "terrorist-related numbers."

Short on Linguists, NSA Struggled to Understand Targets

It's one thing to collect phone calls, email messages, and other signals intelligence. It's quite another to make sense of it. Several SIDtoday articles from the first half of 2004 made clear that the NSA was falling far short in its attempts to process communications conducted in languages other than English.

Only half of the agency's more than 2,300 "language missions" worldwide had qualified personnel, according to a June 2004 SIDtoday article by an NSA "senior language authority." The author declared that "this shortcoming must be rectified." An NSA report to an oversight council, quoted in the article, said that the lack of qualified language analysts was particularly acute in the "Global War on Terrorism."

Exacerbating the situation was the fact that captured communications require a high level of linguistic proficiency to understand. "The cryptologic language analyst must be able to read and listen 'between the lines' to unformatted, unpredictable discourse," as the article put it. Only a quarter of military cryptologic linguists, who formed the vast majority of the workforce, could work at this level, known as "level 3" proficiency, while barely half of the civilian cryptologic linguists could, according to a follow-up SIDtoday article. The military's language training institute offered "virtually no existing curriculum" above level 2.

NSA's plan to address the problem included reforms to the training institute and on-site instruction to bring existing linguists up to higher levels. The agency planned to invest about $80 million per year in training over five years. Other efforts included an internal online language training tool, an evaluation of redundant Arabic machine translation projects underway in various government agencies, and the formation of a language technology team within the NSA.

How the NSA Over-Hacked

Sometimes metadata isn't enough and the NSA decides it needs to compromise targets' computers to collect much more data. The first half of 2004 saw a ramp-up of NSA's hacking capabilities. In March, SIDtoday reported, the agency's elite hacking team Tailored Access Operations approved Kunia Regional Security Operations Center in Hawaii -- the same facility where Edward Snowden later worked -- as the first NSA field office to conduct "advanced" Computer Network Exploitation. Other facilities conduct the first stage of hacking, "target mapping," but the Kunia facility began doing "vulnerability scanning" all the way through to "sustained SIGINT collection."

Another March SIDtoday article said that an advanced network analysis division used to help "exploit targets of interest" had "played an instrumental part" in capturing alleged al Qaeda operative Husam al-Yemeni, had developed a "more complete understanding of the Pakistani Army Defense Network (ADN) infrastructure," and had assisted with the hacking of "an important digital network associated" with the leader of Venezuela at the time, referred to erroneously as "Victor Chavez."

The NSA was so successful at hacking networks that the agency was overwhelmed with information. "We simply do not have enough network analysts to effectively monitor these targeted networks," an

NSA division chief wrote in an April 2004 SIDtoday article. To solve the problem, the agency began prototyping an automated monitoring system.

"Outstanding" Bookworm Spy Doesn't Need to Really Spy

Even as the NSA made enormous efforts to collect vast quantities of private communications, a lone SIDtoday article extolled the value of publicly available data. The piece, from May 2004, gushed about a Defense Intelligence Agency analyst who dug up leads by poring over Russian material that was "open source." The DIA bookworm searched in newspapers, government documents, and "obscure websites" for information that aided the NSA in collecting intelligence, including names, telephone numbers, and addresses. The article, co-authored by an NSA director with responsibility for Russia, praised the analyst's "outstanding language and research skills." It turned out that "critical lead information" on Russian underground facilities, including a mysterious and widely discussed site at Yamantau Mountain in the Urals, was "often only available in open source literature, such as the Internet."

How the NSA Secures -- and Routinely Puts at Risk -- Sensitive Information

Knowing how much intelligence value could be reaped from openly circulated information, the NSA worked to encourage discretion among members of its workforce. NSA employees practiced poor operational security on a "monthly" basis by disclosing too much information in restaurants and other public settings near the agency's Fort Meade headquarters, an agency security manager indicated in a tutorial on operational security that ran in SIDtoday in April 2004.

The article used a hypothetical scenario to explain why operational security, or OPSEC, was important for everyone. The author, OPSEC manager for the NSA's Signals Intelligence Directorate, wrote: "You're at a luncheon at a local restaurant to bid farewell to Sue, a co-worker who is moving on to a new office." Your boss makes a toast to Sue, describing her contributions against organized crime and offering various details of her work. Sue then gives a toast thanking some of the gathered individuals.

"Sound familiar?" the OPSEC manager asked. "Then you've witnessed (or perhaps participated in) a demonstration of poor OPSEC. ... Have you ever stopped to consider what your unclassified public discussions might be giving away? Take the scenario, for instance. This is a scene that is played out monthly in the Fort Meade area." The article went on to list the pieces of information that an adversary, who could have been listening in from a nearby table, would have learned.

OPSEC turned out to be a recurring theme for SIDtoday -- OPSEC training is, after all, mandatory for all NSA personnel. A January 2004 article, written by the author of the April 2004 piece, listed some tips to help personnel to apply OPSEC to their day-to-day activities: Identify your critical information, analyze the threat, identify vulnerabilities, assess risk, and apply countermeasures.

NSA employees aren't the only ones trained to practice good OPSEC. A March 2005 article reported that the leaders of Venezuela and Cuba practiced OPSEC successfully. President Bush considered Venezuelan

President Hugo Chavez a "threat to democracy in the region and a threat to U.S. interests in particular." But "from a SIGINT perspective, Venezuela poses a particularly difficult challenge. With Castro as his mentor, Chavez has learned the importance of communications security and has made sure that his subordinates understand this as well."

Law & Order & the NSA

Various 2004 SIDtoday articles highlight the NSA's behind-the-scenes work on behalf of federal law enforcement.

One detailed a two-week training course on "intelligence reporting" given by NSA staff to FBI officers working on terrorism cases. The course, which had a component dubbed "SIGINT Reporting 101," aimed to provide "insight into the complexity and difficulty of our business" and to dispel "Hollywood myths about the NSA."

Another SIDtoday article showed how the U.S. Coast Guard was able to interdict a boat carrying 3.2 metric tons of cocaine thanks to the NSA's monitoring of VHF radio signals, which carried voice communications of narcotraffickers. An official Coast Guard history of the incident elides the NSA's role. The same SIDtoday article also disclosed that the Colombian air force carried out a strike against a suspected trafficker aircraft after a tip-off from the NSA.

NSA vs. FARC

Colombian guerrillas holding American hostages evaded massive NSA surveillance, according to a February 2004 SIDtoday article.

One year after three American contractors, who had been on a surveillance mission for the U.S. military, were captured by the Revolutionary Armed Forces of Colombia, a Marxist guerilla group, the U.S. "has not been able to determine with high confidence the exact location and status of the hostages," wrote an NSA account manager for the military's Southern Command. This despite "hundreds" of U.S. government personnel having worked to gain their release. U.S. efforts were stymied when FARC's leadership ordered that personnel cease mentioning hostage operations directly in their communications; the best the NSA could achieve at the time of the SIDtoday article was to monitor calls between two radio operators, "Paula and Adriana," who in turn were connected to the FARC leaders "we strongly suspect are linked to the hostages."

The author of the SIDtoday article added that the agency continued to try and get a fix on the location of the hostages. Yet their captors eluded the Americans for another four years. The three Americans were freed by Colombian commandos in July 2008.

A March 2004 SIDtoday article noted a success against FARC, bragging that the arrest of FARC financial leader Anayibe Rojas Valderrama, known as "Sonya," and a number of her associates a month earlier

"resulted from years of monitoring. ... Accurate geolocational data as to where she was and when, allowed a vetted Colombian team to capture them by surprise and without any loss of life." Valderrama was extradited to the United States where she was tried and convicted on drug trafficking charges in 2007.

Internal NSA Criticism of Political Groups and the News Media

A national intelligence officer gave a top-secret "issue seminar" to NSA staff on the question of "where political action fades into terrorism," according to a seminar announcement published in June 2004. The announcement suggested that the line between "legitimate political activity" and "activity that is the precursor to, or supportive of, terrorism" is fuzzy. The course used the Vienna-based organization Anti-Imperialist Camp as a case study, describing it as "ostensibly a political organization" but noting that "its many ties to terrorist organizations -- and its attempts to collaborate with Muslim extremists -- raise questions about where political action fades into terrorism." No further details were given to substantiate the alleged ties; the group's website remains online. A spokesperson for the group, Wilhelm Langthaler, told The Intercept that the group was targeted for such accusations for political reasons, including its opposition to the war in Iraq and "our public support for the resistance against occupation which we have compared with the antifascist resistance against German occupation."

Another seminar announcement said the news media helped stymie U.S. intelligence collection. "A day hasn't gone by that our adversaries haven't picked up a newspaper or gone on the Internet to learn something new about how the US intelligence gathering system operates and what its capabilities or limitations are," the course overview explained. "And in response, a day hasn't gone by that our adversaries haven't modified their operations and activities to avoid being detected and collected against by the US intelligence gathering system."

NSA's Role in the Failed Iran Hostage Rescue Attempt

In an anecdote about signals intelligence during the 1980 Iranian hostage rescue mission, a SIGINT staffer recalled the night of April 24 of that year, when he was told he was monitoring the ongoing "Operation Ricebowl." In a May 2004 SIDtoday article, the staffer wrote: "We knew the parameters of the Iranian Air Defense system because it was U.S. equipment and installed by U.S. contractors while the Shah of Iran was still in power. We knew exactly where the gaps in coverage were and we exploited it during the rescue attempt." The author went on to describe his shock the next morning when he saw on TV news at home that the mission had ended with a disastrous helicopter crash.

The Hill
Former NSA chief: Trump lacks 'deep knowledge' of cybersecurity
Thursday, 08 December 2016
Byline: Joe Uchill

Washington - Gen. Michael Hayden, a former head of the NSA and CIA, says he's worried about Donald Trump's understanding of cybersecurity.
"When he was asked in the second or third debate about his views on cyber, I think it's fair to say he displayed -- he did not have a deep knowledge of the subject," said Hayden Wednesday at the Wall Street Journal Future of Cybersecurity breakfast.

Hayden was one of a bevy of former military and intelligence officials who served under Republican presidents but declined to support Trump's presidential bid.

"If he governs in any way consistent with the language he used as a candidate, I would be very, very concerned," Hayden said at Wednesday's event.

He expressed hope that Trump would eventually pivot and learn more about cybersecurity but said he had not seen any signs that was happening.

Asked by moderator John Bussey of the Journal why he was skeptical, Hayden rattled off a list of reasons he did not trust Trump's judgment on cybersecurity.

"Number one, an absolute refusal to admit to a high confidence judgment of the American intelligence community that the Russians had an aggressive, covert influence campaign on the American political process," said Hayden.

In an article released Tuesday that proclaimed the president-elect Time magazine's "Person of the Year," Trump continued to deny Russia's involvement in the hacks on Democratic party organizations and personnel.

Hayden also expressed concerns about Trump's announced intention to have the Department of Defense develop a plan to protect critical infrastructure.

"Statutorily, that job belongs to Homeland Security," said Hayden.

Hayden was also concerned by what he characterized as Trump's rush to judgment in the encryption debate, noting Trump's call to boycott Apple.

Hayden, like former Homeland Security Director Michael Chertoff, is a firm believer that civilian use of encryption provides stronger national security.

Trump, like FBI Director James Comey, believes that encryption provides terrorists and criminals with a way to hide from law enforcement.

"I think that is a reflexive national security position, not a thoughtful one," Hayden said.

Le Monde

Vols au-dessus d'un nid d'espions

Thursday, 08 December 2016

Byline: Jacques Follorou

Non identifié - La NSA américaine et son homologue britannique peuvent capter toutes les données, y compris les codes secrets, des communications des passagers de la plupart des compagnies aériennes. Dont Air France.

Dans l'immense stock d'archives extraites par Edward Snowden, l'ancien contractuel de l'Agence nationale de sécurité américaine (NSA), c'est une pépite. Elle débute par une devinette : " Quel est le point commun entre le président du Pakistan, un trafiquant de cigares ou d'armes, une cible du contre-terrorisme ou le membre d'un réseau de prolifération nucléaire? Ils utilisent tous leur téléphone portable lorsqu'ils sont dans un avion. "

Posée en 2010 dans une des lettres d'information interne de l'une des principales directions de la NSA, " SIDtoday ", et classée top secret, elle annonce l'émergence d'un nouveau terrain d'espionnage, qui n'avait pas encore été exploré : l'interception des données de communications à bord des avions de ligne. En 2009, la NSA souligne dans un document interne que, en décembre 2008, 50 000 personnes ont déjà utilisé leur téléphone portable en vol, un chiffre qui atteint 100 000 en février 2009. Pour expliquer cet engouement, la NSA énumère : " De plus en plus d'avions équipés, la crainte recule de voir l'avion s'écraser. Pas aussi cher qu'on le croyait. (...) Le ciel pourrait appartenir à la NSA. "

Fin 2012, le Government Communications Headquarters (GCHQ), l'homologue britannique de la NSA, livre, à son tour, dans une présentation " top secret strap ", un des plus hauts niveaux de classification, les dessous du programme Southwinds (" vents du sud "), mis en place pour collecter tout le trafic, voix et data, métadonnées et -contenu des connexions à bord des avions. La zone est encore limitée aux régions -Europe, Moyen-Orient et Afrique, couvertes par les satellites Inmarsat.

La collecte des données se fait " quasiment en temps réel " et un avion peut être suivi toutes les deux minutes. Pour espionner un téléphone, il suffit qu'il soit à une altitude de croisière de 10 000 pieds. Le signal transitant par satellite, la technique d'interception se fait par des stations secrètes d'antennes au sol. Le seul fait que le téléphone soit allumé suffit à le localiser, l'interception peut alors être croisée avec le registre des listes de passagers et les numéros des avions, pour mettre un nom sur l'utilisateur du smartphone.

Le GCHQ peut même, à distance, perturber le fonctionnement d'un téléphone de sorte que son utilisateur soit -contraint de le redémarrer avec ses codes d'accès : les services britanniques interceptent du même coup ses identifiants.

UNE FIXATION CONSTANTELe GCHQ et la NSA ont baptisé leurs opérations de mise sous surveillance des communications en avion de doux noms d'oiseaux, " Pie voleuse " et " Pigeon voyageur ", comme cela a

été évoqué par Glenn Greenwald, journaliste américain, dans son ouvrage Nulle part où se cacher (JC Lattès, 2014). Ce dernier a été le dépositaire avec Laura Poitras des documents Snowden. Ils sont tous deux cofondateurs du site d'information The Intercept .

La lecture attentive de la présentation de ces opérations ainsi que celle d'autres pièces inédites des archives Snowden, -consultées par Le Monde en collaboration avec The -Intercept, sur la surveillance entre 2005 et 2013 des avions et de leurs passagers dans le monde entier, prouvent que la compagnie Air France a été très tôt au coeur de l'attention de ces deux pays amis, les Etats-Unis et la Grande-Bretagne.

La cible Air France apparaît dès 2005 dans un document de la NSA fixant les grandes lignes du projet de " traque des avions civils dans le monde entier " . Daté du 5 juillet et signé par le numéro deux de l'une des principales directions de la NSA, chargée du renseignement d'origine électromagnétique (Signal Intelligence Directorate, SID), ce mémo de 13 pages recense sous forme chronologique et détaillée les principales étapes de ce programme pensé pour éviter " un nouveau 11-Septembre " . On peut lire que, dès la fin 2003, " la CIA considère que les vols Air France et Air Mexico sont des cibles potentiellesdes terroristes " . Le service juridique de la NSA précise alors " qu'il n'y a aucun problème légal pour cibler les avions de ces deux compagnies à l'étranger " et qu' " ils devraient être sous la plus haute surveillance dès qu'ils entrent dans l'espace aérien américain " . Dès février 2005, ces mêmes juristes insistent sur la procédure légale à suivre, " en particulier pour la collecte des communications à bord des avions " .

La désignation d'Air France comme risque majeur pour les intérêts et le territoire américains ne relève pas d'une simple hypothèse de quelques techniciens-espions de la NSA. Un cercle impressionnant d'autorités chargées de la sécurité du pays a été informé du " danger " représenté par la compagnie française. Le mémo de la NSA est, en effet, adressé à une vingtaine de destinataires, dont le commandement de la défense aérienne de l'Amérique du Nord, la CIA, le département Homeland Security (la sécurité intérieure), l'Agence de renseignement spatial, l'Agence de renseignement de la défense ou encore l'état-major de l'armée de l'air. Cette fixation sur Air France sera constante au fil des années qui vont suivre et ne tient pas du hasard.

PRISES DE GUERRELe premier test de l'utilisation d'un smartphone en plein ciel a été effectué à bord du vol AF 1046 d'Air France, le 17 décembre 2007, sur une liaison Paris-Varsovie. " On a commencé tôt, confirme au Monde la direction d'Air France, mais, depuis, on n'a pas cessé de faire des tests, aujourd'hui, on s'apprête, comme les autres compagnies, à passer directement au Wi-Fi à bord. " La compagnie française, interrogée sur les pratiques des services secrets anglo-saxons, a d'ailleurs réagi avec mesure : " Nous ne sommes pas les seuls, visiblement, à avoir été visés et nous ne disposons d'aucun élément sur ces pratiques. "

En 2012, le GCHQ note que 27 compagnies ont déjà permis aux passagers d'utiliser un téléphone portable ou sont sur le point de le faire, surtout pour les premières classes et les classes affaires des vols long-courriers. Parmi elles, British Airways (seulement data et SMS), Hongkong Airways, Aero-flot, Etihad, Emirates, Singapore Air-lines, Turkish Airlines, Cathay Pacific ou encore Lufthansa. Air France est,

pour sa part, un tel symbole de la surveillance des communications en avion que les services britanniques utilisent un croquis pleine page de l'un de ses avions pour illustrer le fonctionnement de l'interception en vol.

Pour prouver leur savoir-faire, le GCHQ et la NSA fournissent nombre d'exemples d'interceptions passées à bord de vols commerciaux d'autres compagnies. On trouve ainsi les relevés, le 23 mars 2012, à 13 h 56, du vol Etihad ETD 8271 des Emirats arabes unis, entre JFK et Denver, du Nice-Moscou du 20 mai 2011 (Aeroflot) ou encore, la même année, du Milan-Doha (de Qatar Airways), du Athènes-Doha (toujours de Qatar Airways), du Jeddah-Le Caire (de la Saudi Airlines) ou du Paris-Mascate (d'Oman Air). La collecte concerne également des Blackberry dont les codes PIN et les adresses e-mails sont identifiés dans un avion, le 2 janvier 2012 à 10 h 23, sans que l'on connaisse sa destination et le nom de la compagnie. Les prises de guerre sont fièrement annoncées : voix, data, SMS, Webmail, Webchat, réseaux sociaux (Facebook, Twitter, etc.), Travel Apps, Google Maps, Currency Converters, Media, VOIP, BitTorrent ou Skype.

Au cours de leurs exercices d'intrusion, les services secrets britanniques découvrent, un peu surpris, qu'ils ne sont pas les seuls intéressés par ces communications en vol. Ils notent que la compagnie russe Aeroflot a mis en place un système de connexion spécifique pour les GSM à bord de ses appareils, " sans doute pour procéder à des interceptions... ", glissent-ils dans une note technique.

AUCUNE LIMITE À LA SURVEILLANCEAujourd'hui, près d'une centaine de compagnies permettent de téléphoner en avion. " Les clients estiment désormais normal, voire nécessaire, de rester connecté en vol ", assure la direction d'Air France. Les autorités en matière de sécurité aérienne ont toutes validé l'utilisation des GSM à bord des avions et les experts estiment que 2016, 2017 et 2018 seront les années historiques du portable en vol, notamment par l'installation pérenne du Wi-Fi en plein ciel. De quoi étendre encore l'ampleur de l'espionnage en visant " plusieurs centaines de milliers de personnes " à surveiller, selon les projections de la NSA, soit un périmètre qui dépasse de loin les seules cibles reliées au terrorisme. L'espionnage politique ou économique des passagers en première classe ou en classe affaires sur des long-courriers intéresse d'ailleurs bien davantage les services.

La surveillance, elle, n'a aucune limite et chaque nouveauté est un défi technique qui paraît vite relevé. Les services semblent en être même un peu blasés. Les techniciens-espions de la NSA, dans une note - interne de 2010, avaient même déjà la tête ailleurs : " Quel sera le prochain terrain d'expéri-mentation? Les trains? Il faudra qu'on regarde ça... "

Atlantico (site web)
Les dernières révélations Snowden atomisent la théorie d'une mondialisation heureuse
Thursday, 08 December 2016
Byline: Franck Decloquement

Non identifié - Les dernières révélations Snowden atomisent la théorie d'une mondialisation heureuse (et ça, c'est nettement plus gênant que les arguments des populistes sur le libre-échange)
Les guerres économiques que se livrent les pays du monde entier représentent une menace bien plus sérieuse pour le libre-échange que les théories économiques de Donald Trump.

Atlantico : Les révélations d'Edward Snowden mettent chaque jour en avant de nouvelles informations sur les pratiques de la NSA. Parmi ces révélations, certaines soulignent le risque que font courir les agences de renseignement au libre-échange et à la libre-concurrence. Quel est-il exactement ? Les missions poursuivies par les organes de renseignements vont-elles à l'encontre des principes du libre-échange ?

Franck Decloquement : Selon de très nombreux observateurs ayant pu enquêter en profondeur sur le sujet, la NSA est une « arme d'espionnage économique massive » , et un « fer de lance sous l'égide de Washington » , évidemment prête à tout - dans le cadre de ses prérogatives propres - pour défendre les intérêts commerciaux américains. A l'image du dernier livre de Claude Delesse « NSA - National Security Agency » , édité chez Tallandier, qui est une très bonne introduction en la matière, à destination d'un lectorat grand public. Ceci est indéniable et ressort très clairement de toutes les analyses sérieuses de documents connus et de témoignages crédibles qui ont pu être considérés pour comprendre ce qui se passe à l'intérieur de cette immense « black box » . Pour autant, il reste de très nombreuses zones d'ombre, et ceci est bien compréhensible. Contrairement à la CIA, fondée de manière très officielle, l'existence de la NSA est restée très secrète et ne fut officiellement reconnue qu'en 1957. En outre, ceci lui fit gagner son premier sobriquet, inventé par les gens de presse, de « No Such Agency » . Expression malicieuse que l'on pourrait aussi traduire par : « une telle agence n'existe pas ! » . Compte tenu de sa suprématie planétaire quant à la captation des données en transit dans l'ensemble du spectre électromagnétique, son appui opérationnel à la captation d'actifs immatériels, industriels ou technologiques pour les ravir à la concurrence internationale - au bénéfice des intérêts américains - est notable. À l'image de certains fleurons industriels comme le Brésilien Petrobras ou le Français Alcatel. Certains documents NSA ayant parfois même fuité, malgré l'étroite surveillance et l'exigence d'une stricte confidentialité imposée aux parties prenantes. L'affaire Snowden démontre aussi que « l'ennemi de l'intérieur » peut à tout moment surgir, agir et divulguer opportunément d'énormes quantités de données « ravies » , même dans les enceintes secrètes les plus sanctuarisées du monde. Pour autant, les différentes attributions secrètes qui incombent à la NSA ne sauraient se réduire aux seules divulgations qui ont pu être rendue possible. Ce continent noir ne se laisse évidemment par percer à jour aussi facilement.

Mais les sous-traitants partenaires de la NSA ne sont pas en reste non plus, à l'image de Palantir Technologies, la très secrète entreprise fondée par Nathan Gettings, Alex Karp, Joe Lonsdale, Stephen Cohen et l'emblématique Peter Thiel. Palantir Technologies est une start-up de services et d'édition de logiciels spécialisés dans l'analyse et la science des données, communément appelé « Big data » ou « méga données » , qui a révolutionné le monde du renseignement. L'entreprise basée à Palo Alto en Californie ; et fondée il y a 12 ans ; travaille pour la communauté du renseignement des États-Unis, et notamment pour la NSA. Mais aussi pour la CIA et le FBI. Ainsi que pour différents autres acteurs du

système de défense des Etats-Unis, à l'image des US Marines, de l'US Air force et des opérations spéciales. Elle s'est également diversifiée dans les secteurs de la santé, de la finance, de l'assurance mais aussi des biens de consommation courante. Elle met par ailleurs sa technologie à disposition d'ONG comme « Community solutions » . Cette entreprise atypique en raison de la jeunesse de ses collaborateurs était valorisée en 2014 à 15 milliards de dollars. Son patronyme provient en droite ligne de l'oeuvre de Tolkien, « Le Seigneur des Anneaux » , et plus spécifiquement de ces pierres mystérieuses qui permettent de voir l'avenir... Aussi appelé « pierre de vision » ou « pierre clairvoyante » . « Un palantír a l'apparence d'un globe sombre de matière transparente (une sorte de boule de cristal), permettant à son utilisateur d'observer des lieux distants dans l'espace et le temps, ou bien de dialoguer avec une autre personne qui utilise elle aussi un palantír » . Le décor est planté quant aux fins poursuivies ! On le voit ici, le mythe de la concurrence « pure et parfaite » est très largement entamé par les pratiques obscures de l'agence, et renvois pour beaucoup d'observateurs avisés et de spécialistes, aux contes enfantins pour adultes... La concurrence et les actions déloyales sont légion. Et elles n'ont que très peu d'acteurs à craindre sur le plan mondial, compte tenu de la puissance du dispositif, de l'ampleur des moyens techniques et humains alloués pour y parvenir, des impératifs stratégiques toujours clairement énoncés par le pouvoir politique, et l'obligation de garantir à tout prix les conditions de la sécurité nationale.

Philippe Crevel : Si les écoutes des passagers d'Air France par les services de renseignements américains et britanniques apparaissent en l'état peu réalistes du fait que la connectivité des avions d'Air France n'est pas l'une de leur qualité, elles posent néanmoins une réelle question, celle des moyens mis en oeuvre par les agences gouvernementales pour obtenir des informations qui concernent tant la sécurité que les activités économiques.

Dans un contexte de concurrence exacerbée, les Etats et les entreprises essaient d'obtenir des renseignements stratégiques. Si nous évoluons dans un système de libre-échange encadré par l'Organisation mondiale des échanges, de plus en plus de comportements peu coopératifs se développent. Cela ne peut que conduire à une montée du protectionnisme, montée réclamée par les populistes. Or, à partir du moment où les Etats commencent à intervenir dans le commerce et dans l'économie, le déclin n'est pas loin. De la Chine du 16ème à la France de Méline en passant par celle de Colbert, le protectionnisme étatique a toujours mené à la catastrophe. Aujourd'hui, ce sont les tentatives des nationalistes en tout genre de vouloir contrecarrer le libre-échange qui pourraient peser sur la croissance. Il ne faut pas oublier que depuis 1945 nous tirons une grande partie de la croissance du commerce international. De même, si la pauvreté a reculé ces vingt dernières années, au niveau mondial, c'est avant tout la conséquence de l'ouverture de la Chine et des pays d'Europe centrale au commerce extérieur. L'OMC devrait, pour faire face aux tentatives des Etats d'utiliser des techniques militaires à des fins commerciales, disposer de pouvoirs de sanctions, afin d'assurer la liberté des échanges et de la circulation des biens, des services et de l'innovation. En effet, le renouveau du populisme pourrait aboutir à une protection accrue des innovations qui aurait pour conséquence leur moindre diffusion au sein de la population.

Dans quelle mesure l'objectif de la NSA et de ses homologues est-il prioritairement économique ? De quand date réellement cette transformation ?

Franck Decloquement : Depuis sa création le 4 novembre 1952, la fonction première de la NSA est connue rétrospectivement des spécialistes. Ses missions sont définies par la « National Security Council Intelligence » - Directive numéro 6 - selon les besoins et ordres du Directeur du renseignement national. Bien qu'elle appartienne au département de la Défense, la NSA agit pour l'ensemble de la communauté du renseignement américain. De nos jours, la centrale est plus spécifiquement en charge du « renseignement d'origine électromagnétique » , de la « sécurité des systèmes d'information » et du « traitement des données » à l'échelle planétaire pour le compte du gouvernement américain. Et ceci pour des raisons historiques assez claires : le renseignement d'origine électromagnétique - « COMINT » (ou « Communications Intelligence ») - joua un rôle primordial dans la conduite de la deuxième guerre mondiale par les États-Unis, et son issue victorieuse. Les éléments des forces armées des États-Unis chargés de l'écoute et du décryptage des communications ennemies pour le compte de l'US Navy et de l'US Army, remportèrent de très nombreux succès contre les communications allemandes et japonaises dans les opérations connues sous le référentiel « Ultra » et « Magic » . Combinés avec la radiogoniométrie, l'analyse de trafic et l'exploitation du texte diffusé en clair, le « COMINT » pu fournir énormément de renseignements d'importance vitale. Des affres de la Deuxième Guerre mondiale dérivèrent alors une certaine « culture du renseignement » marquée par le besoin de concentrer d'importantes ressources humaines et de matériels techniques, afin d'attaquer des systèmes d'informations et de cryptages / chiffrages, toujours plus puissants et toujours plus complexes de l'ennemi.

L'entrée de plain-pied dans la guerre froide ne put que renforcer encore cette inclinaison initiale dans la captation et le décryptage des signaux d'origine électromagnétique émanent de la Russie. De même que dans le cadre de l'intensification croissante de la guerre économique, à travers le globe, compte tenu du processus de mondialisation des échanges commerciaux en cours. Une fois l'Union Soviétique vaincu, il fallu très vite réorienter l'appareil de guerre conventionnel américain et son dispositif humain très lourd, vers le secteur marchand. Ce que fit Bill Clinton sous sa mandature. Accélérant ainsi la reconversion de plus de 10 000 agents américains du renseignement, vers la sphère économique. Président à la naissance d'un « Advocacy Center » , sorte de « War Room » en charge d'orienter les agences du renseignement américain vers l'aide opérationnelle à leurs entreprises nationales parties à la conquête des marchés internationaux. Dans ce cadre hyperconcurrentiel, les services spécialisés de la NSA ne pouvant qu'être d'une aide précieuse, on l'imagine aisément avec le recul. Aux Etats Unis, les partenariats publics- privés ne sont pas un vain mot, puisqu'ils se déclinent en action très concrètes. A la différence de la France et des ses conservatismes idéologiques et administratifs.

De très nombreuses personnalités politiques françaises ont eu des mots parfois très durs concernant l'ingérence américaine dans les affaires hexagonales. A l'image des allemands aujourd'hui, suite aux actions d'espionnage dont ils firent l'objet. Et beaucoup n'auraient pas été surpris d'apprendre qu'il était mis sur écoute par la National Security Agency (NSA) américaine, à l'image d'un François Mitterrand au crépuscule de sa vie, qui confia au journaliste Georges-Marc Benhamou sa perception géopolitique de la

situation que le confident s'empressa vite de retranscrire dans son livre « le dernier Mitterrand » : « La France ne le sait pas, mais nous sommes en guerre avec l'Amérique. Oui, une guerre permanente, une guerre vitale, une guerre économique, une guerre sans mort apparemment. Oui, ils sont très durs les Américains, ils sont voraces, ils veulent un pouvoir sans partage sur le monde. C'est une guerre inconnue, une guerre permanente, sans mort apparemment et pourtant une guerre à mort » . Délire d'un vieille homme agonisant ou extrême lucidité d'un ancien président de la République au fait des réalités géoéconomiques ? Chacun pourra arbitrer en conscience.

Quels sont les procédés traditionnellement mis en place à des fins de guerre économique par les agences de renseignement et d'intelligence économique ? Peut-on vraiment croire à l'infiltration d'entreprises stratégiques ou aux guerres des normes ?

Franck Decloquement : : Il ne faut pas confondre les pratiques tout à fait légales de l'intelligence économique et stratégiques (IES), qui ne travaillent qu'à partir de sources ouvertes - « blanches » ou « grises » - avec les pratiques de l'espionnage économique ; régalien en ce qui concerne la NSA ; qui représentent la partie congrue du renseignement que l'on peut qualifier de « clandestin » , puisque celui-ci ne vise prioritairement que le recueil frauduleux de documents et de données de sources « noires » , d'accès confidentiel, ultra restreint ou très secret. Considérant les écoutes illégales, la surveillance globale des télécommunications, l'empiégeage des matériels ou des composants informatiques, des applications pouvant aisément moucharder sur les données de leurs utilisateurs, des malwares en circulation sur l'internet et plus généralement la captation du « signal » à l'échelle de la planète, nul ne doute aujourd'hui que nous sommes en face d'une réalité - celle des actions coercitives, illégales, déloyales et clandestines - qu'il nous est bien difficile aujourd'hui de ne plus voir, mais aussi de contrecarrer compte tenu de nos liens politiques, diplomatiques, stratégiques et de notre subordination économique manifeste à nos alliés.

Le « confidentiel entreprise » n'ayant pas véritablement pu percer et s'imposer, nos firmes, nos multinationales et nos PME - à l'identique du monde économique dans sont ensemble - sont plongés dans les affres de « la guerre du tous contre tous » et du « chacun pour soi » , face aux velléités d'une puissance sans équivalences dans le monde, et qui accompagne la croissance et le succès de ses entreprises le cas échéant, via ses outils de guerre technologique. La projection du droit et des normes, sont en effet des armes également redoutables contre lesquelles nous n'avons pas su réagir, ou su imposer collectivement notre véto. Et ceci, en intelligence avec d'autres pays européens soumis aux mêmes formes de contrôle. L'union dans ce cas faisant toujours la force. Il s'agit d'une véritable guerre de mouvement, d'agilité intellectuelle, de supériorité technologique et stratégique, agissant dans un registre d'action spéciale, aux confins de la sphère économique et de la souveraineté des Etats. Nul ne peut l'ignorer désormais.

L'Humanité
WikiLeaks accuse le régime de collusion avec Daech
Thursday, 08 December 2016

Byline: S.A.

Ankara - Le site a publié 57 934 mails de Berat Albayrak montrant des relations troubles entre l'« État islamique » et la compagnie pétrolière Powertrans.
Le ministre turc de l'Énergie, Berat Albayrak, pourrait bien se faire tirer les oreilles par son beau-père pour manque de prudence. Lundi et mardi, le site d'information WikiLeaks a publié 57 934 mails du gendre de Recep Tayyip Erdogan qui prouveraient les liens troubles entretenus par la Turquie et l'organisation de l'« État islamique » (EI). La compagnie pétrolière turque Powertrans aurait en effet bénéficié d'une dérogation à l'embargo imposé par le gouvernement sur les importations et exportations de pétrole en provenance ou en direction des régions sous contrôle de Daech. Ankara aurait donc sciemment acheté du pétrole syrien à l'EI, finançant indirectement le groupe djihadiste en hommes et en matériel militaire.

Ces mails - qui courent de juillet 2000 à septembre 2016 (putsch avorté compris) - corroborent ce que le quotidien d'opposition Cumhuriyet a tenté de faire savoir le 29 mai 2015.

Sur son site Web, le journal avait diffusé des images tournées par les forces de sécurité turques en janvier 2014 près de la frontière syrienne montrant des gendarmes en train d'intercepter deux convois de camions chargés d'armes dirigés par les services secrets turcs (MIT). Pour avoir osé montrer ces images, le rédacteur en chef, Can Dündar, et Erdem Gül, son chef de bureau à Ankara, ont été accusés d'« espionnage » et « divulgation de secrets d'État », déclenchant l'ire de Recep Tayyip Erdogan, qui menaça publiquement le journaliste : « Je ne le laisserai pas, je le suivrai et il devra payer la facture. »

Cette nouvelle affaire prouve également l'état de corruption généralisé qui règne dans l'entourage proche du président turc. En 2013, Bilal Erdogan, son propre fils, avait déjà été pris la main dans le sac pour une sombre affaire de trafic illicite d'or avec l'Iran : c'est un certain Can Dündar qui avait révélé l'affaire.

La Tribune (France)
L'Europe au défi de la souveraineté dans le cyberespace
Thursday, 08 December 2016
Byline: Les Arvernes

Paris - Les pays européens ne font que suivre Washington. Or la France pourrait être à l'avant-garde d'une politique européenne dans ce domaine.
L'échéance présidentielle française, dans un peu plus de 6 mois maintenant, concerne bien évidemment les destinées de la France, mais avec elle, une part de celles de l'Europe. En tant qu'acteur majeur de la construction communautaire, aussi bien que par son rang de grande puissance économique et militaire, la France a un rôle spécial à jouer en Europe. Parmi les chantiers qui attendent le prochain président français et son gouvernement, celui de la place de notre pays et, par ricochet, de l'Europe dans le cyberespace, est l'un des plus importants.

Vassalisation des pays européens

Depuis Wikileaks et les révélations d'E.Snowden sur l'espionnage pratiqué par les Etats-Unis, on aurait pu s'attendre à ce que les Européens se saisissent enfin du dossier de la place du continent dans le cyberespace. Or rien n'a changé. Pis encore, la vassalisation des pays européens à l'égard des Etats-Unis s'est encore accrue. Aucune grande capitale n'a pipé mot sur l'extension jusqu'en 2017 du Foreign Intelligence Surveillance Act (FISA) Amendements Act of 2008 qui autorise les services américains à intercepter toute communication où que ce soit sur la planète, dès que la « sécurité nationale » apparaît menacée.

Cette loi est, en somme, un blanc- seing pour l'espionnage généralisé des communications électroniques mondiales. De la même manière, les parlementaires européens ont accepté en avril 2016 le transfert des données des passagers des compagnies aériennes (Passenger Name Record) aux autorités américaines, alors même que le G29, organisme européen regroupant les entités nationales chargées de la protection des données, avait rendu un avis dans lequel il pointait les dérives potentielles d'un tel système. A l'heure où les autorités européennes se saisissent des questions de droit à l'oubli, il est quelque peu étonnant de constater que les instances politiques de l'Union acceptent sans ciller de confier ces mêmes données personnelles des citoyens européens à une puissance extérieure. En même temps il suffit de compiler les chiffres du lobbying européen pour se rendre compte que dans le top 10 apparaissent Microsoft (3e), Google (6e), mais aussi le chinois Huawei (9e) qui a lui aussi bien compris que l'Europe était tout sauf un acteur animé d'une volonté souveraine en ce domaine.

Au bon vouloir de Washington

En réalité, depuis les débuts de l'ouverture d'Internet aux particuliers, l'Europe est calée dans la roue des Etats-Unis et, si elle bénéficie de quelques miettes, n'en est pas moins soumise au bon vouloir de Washington pour ce qui touche au cyberespace. La faiblesse chronique des acteurs économiques européens dans le domaine des matériels et des logiciels, ne doit pas servir d'excuse facile à ceux qui refusent de penser une certaine forme de cybersouveraineté. Alors que la Chine a depuis longtemps pris son cyber- destin en mains et que d'autres pays comme la Russie, imposent la localisation des serveurs abritant les données des citoyens sur le sol national les pays européens demeurent passifs. Ceux-ci entraînés par le Royaume-Uni, allié privilégié des Etats-Unis, y compris sur la partie cyber- espionnage, avaient eu tendance à suivre béatement les positions de Washington, y compris lors des tentatives de régulation de l'Internet, comme la conférence de Dubaï de l'Union internationale des télécoms de 2012. Le Brexit étant maintenant consommé, les Européens ont tout loisir de reprendre leur destin en mains; pour autant qu'ils le veuillent.

La France, seule cyberpuissance de rang mondial du Vieux continent

La France, en tant que seule cyberpuissance de rang mondial du Vieux continent, est la mieux à même d'être à l'avant-garde de la politique communautaire en ce domaine. L'excellence des entreprises

françaises dans plusieurs domaines, à commencer par la pose et l'entretien des câbles sous-marins, secteur-clé du Net, ou la cybersécurité, issue des technologies militaires (Thalès, Airbus, Safran, etc.), doit être valorisée pour permettre à la France et à l'Europe de retrouver une marge de manoeuvre dans les politiques liées au cyberespace. Les questions de stockage des données des citoyens, de gouvernance internationale, d'indépendance des entreprises sur les questions normatives, sont autant de grandes problématiques que le futur président français sera le mieux à même de porter à Bruxelles. Si la France est trop petite pour devenir un acteur majeur du Net, elle peut, en entraînant l'Europe, faire que le continent ne soit plus dans le cyberespace qu'une simple banlieue de Washington.

Les Arvernes sont un groupe de hauts fonctionnaires, chefs d'entreprises, essayistes, professeurs d'Université

China Daily
China, US to do more on cyber crime
Thursday, 08 December 2016
Byline: Chen Weihua

Washington - Chinese and US officials meeting in Washington on Wednesday for a bilateral cybersecurity dialogue have agreed to expand cooperation, according to Chinese officials.
Chinese State Councilor and Minister of Public Security Guo Shengkun joined US Attorney General Loretta Lynch and Secretary of Homeland Security Jeh Johnson in co-chairing the third China-US High-Level Joint Dialogue on Cybercrime and Related Issues.

The two sides reached a new consensus in deepening cooperation in cybersecurity. Achievements made in the meeting cover areas such as cracking down on cybercrimes, cooperation in cybersecurity, improving the hotline mechanism, cyber counterterrorism cooperation and information sharing, according to a press release from the Chinese delegation.

The two sides recalled the achievements made since the first dialogue and spoke positively of the importance and necessity of the mechanism, the press release said.

Guo was quoted as saying in the meeting that China and the US established the high-level dialogue mechanism based on the important consensus reached between President Xi Jinping and US President Barack Obama in September 2015.

He said the two leaders gave important input to the dialogue when they met in Lima, Peru, last month on the sidelines of the APEC Leaders Summit.

"With the high attention and promotion by the two heads of state, the cooperation in cybersecurity between China and the US has advanced rapidly to become a new highlight in bilateral relations," Guo said at the meeting.

The two-day meeting from Dec 7-8 is attended by top officials from multiple government departments in both countries, including China's Ministry of Public Security, Cyberspace Administration, Ministry of Foreign Affairs, Ministry of Industry and Information Technology, Ministry of State Security and Ministry of Justice and the US' Department of Justice, Department of Homeland Security, Department of State and Federal Bureau of Investigation.

Guo said the two sides have achieved notable progress in areas such as cracking down on cybercrimes, protecting cybersecurity and sharing information. "(It) has made a positive contribution to ensuring the national security and the safety of the people in both countries," he said.

He noted that it has been an important period for the two countries in carrying out their law enforcement cooperation focusing on cybersecurity. He expressed that the dialogue mechanism should be the main channel for the two countries in communicating cyber-related issues.

Guo also emphasized the importance of focusing on cooperation, managing and controlling differences,

and timely and effective responses to each other's concerns as well as the need of achieving no-conflict, no-confrontation, mutual respect and win-win cooperation.

"The Chinese side is willing to make continued efforts with the current US government team and the next government team to take the bilateral cooperation in cybersecurity to a new high and to make a contribution to the building of a new type of major country relationship," Guo said.

An official from the Chinese delegation, who prefers not to be identified, said US officials also agree that without such a dialogue mechanism, China and the US could still face confrontation and conflict in cybersecurity, as the situation appeared more than a year ago.

In the past year, China has requested the US for assistance in investigating 10 cybercrime cases while the US has made request for nine cases.

The official also praised the hotline mechanism for helping reduce miscalculation when serious cases emerge.

Both Lynch and Johnson expressed that two countries have shared interest in cracking down on cybercrimes and protecting cybersecurity, according to the Chinese press release.

They described the high-level dialogue mechanism as "a new highlight of China-US cooperation" and "playing an important role in protecting cybersecurity and cracking down cybercrimes" as well as "providing an important platform for the law enforcement departments in both countries to conduct candid exchanges and enhance mutual understanding and trust".

Both Lynch and Johnson hoped that the mechanism could be further developed and more practical cooperation will be carried out in cracking down on criminal activities such as cyber terrorism and email scams. Both sides proposed to hold the fourth round of dialogue in China in 2017.

The Daily Beast
Everyone's a Target to the NSA. Here's How the Courts Can Stop It.
Thursday, 08 December 2016
Byline: Ashley Gorski

Comment - Next month, President-elect Donald Trump will be handed the keys to the NSA's vast spying apparatus. As a candidate, he supported mass surveillance of Americans' phone calls, called for expanded spying on American Muslims, and even invited Russia to hack the emails of his political opponent. With these threats to privacy and liberty on the horizon, our courts will likely be more important than ever as a bulwark against unlawful spying.
One of the courtroom battles that will shape Trump's spying powers is already under way.

On Thursday, the Fourth Circuit Court of Appeals will hear oral arguments in Wikimedia v. NSA, our case challenging "Upstream" surveillance. First revealed by whistleblower Edward Snowden in June 2013, Upstream surveillance involves the NSA's bulk searching of Americans' international internet communications with the assistance of companies like AT&T and Verizon. If you email friends abroad, chat with family members overseas, or browse websites hosted outside the United States, the NSA almost certainly has searched through the contents of your communications--and it has done so without a warrant.

Upstream surveillance takes place in the internet "backbone"--the network of high- capacity cables, switches, and routers that carries Americans' domestic and international internet communications. The NSA has installed surveillance equipment at dozens of points along the internet backbone, allowing the government to copy and then search the contents of vast quantities of internet traffic as it flows past.

The government claims that Upstream surveillance is authorized by Section 702 of the Foreign Intelligence Surveillance Act. That law allows the NSA to engage in warrantless surveillance of Americans when they are communicating with so-called targets abroad. But these targets can be virtually any foreigner overseas--including people who are not accused of any wrongdoing whatsoever, like journalists, lawyers, and human rights researchers. No judge signs off on the government's individual targets. Instead, the NSA secretly vacuums up millions of communications under a single court order each year.

One of the most glaring problems with Upstream surveillance is that it is not targeted at all--at least not in any ordinary sense of the word. Instead, the government is systematically examining online communications in bulk, scanning their full contents to see which ones merely mention its targets.

Because of how it operates, Upstream surveillance represents a new surveillance paradigm, one in which computers constantly scan our communications for information of interest to the government. To use a non- digital analogy: It's as if the NSA sent agents to the U.S. Postal Service's major processing centers to conduct continuous searches of everyone's international mail. The agents would open, copy, and read each letter, and would keep a copy of any letter that mentioned specific items of interest--despite the fact that the government had no reason to suspect the letter's sender or recipient beforehand.

The ACLU brought this lawsuit on behalf of a coalition of legal, media, educational, and human rights organizations, including the Wikimedia Foundation (which runs Wikipedia), Amnesty International USA, The Nation magazine, PEN American Center, Human Rights Watch, the Rutherford Institute, the National Association of Criminal Defense Lawyers, Global Fund for Women, and the Washington Office on Latin America.

Each of these nine plaintiffs has been deeply affected by U.S. government spying. The confidentiality of plaintiffs' international communications is essential to their work, and Upstream surveillance undermines their ability to ensure that these communications--with colleagues, journalists, witnesses, foreign government officials, victims of human rights abuses, and the tens of millions of people who read and edit Wikipedia--are indeed private. This spying violates our clients' constitutional rights to privacy, freedom of expression, and freedom of association.

Last year, a federal district court in Maryland dismissed our suit (PDF), wrongly concluding that our clients lack standing to challenge Upstream surveillance because they had not "plausibly" alleged that their communications are intercepted. Without standing, our plaintiffs can't have their day in court to challenge this spying on the merits.

However, as we explained in our appeal briefs (PDF, PDF), it's more than plausible that our clients' communications are intercepted: The government's own disclosures about Upstream surveillance, along with media reports, show that the NSA is vacuuming up and reviewing almost all text-based communications that enter and leave the country.

Wikimedia alone engages in over a trillion internet communications each year, with individuals located in virtually every country on earth. Given the volume and geographic distribution of these communications, it's indisputable that plaintiffs' communications are ensnared by the NSA.

We hope that the Fourth Circuit agrees. With Trump about to take over, there's simply too much at stake for the judiciary to close the courthouse doors on those harmed by mass surveillance.

Ashley Gorski is a staff attorney in the ACLU's National Security Project.

National Post
Ottawa denies using data from vote reform website
Friday, 09 December 2016
Byline: Marie-Danielle Smith

Ottawa - The government says information collected by an online electoral reform consultation isn't accessible to the Liberal Party, after an Ontario man alleged he started getting fundraising emails soon after completing the survey.
Sean Fullerton, a database analyst in Kitchener, Ont., told the National Post he unsubscribed from Liberal emails more than a year ago, but started receiving them again almost immediately after entering his email address on MyDemocracy.ca, a website being used to gather opinion on democratic values.

But both the government and Vox Pop Labs, the company that designed the site, deny email addresses are even being collected.

"Protecting personal information is something we take very seriously. Political parties have no access whatsoever to any information shared with MyDemocracy. ca. That is just not happening," said John O'Leary, the director of communications for Democratic Institutions Minister Maryam Monsef.

"Emails are not retained in the system when results are emailed to users. They are not stored and cannot be retrieved by anyone, Vox Pop Labs included," said Clifton van der Linden, the CEO and founder of the public opinion company, in an email. "The implication that these email addresses are stored or shared with third parties is utterly baseless."

He added, "our organization would of course investigate any reports about the security of our system and integrity of our database, but we have not received such reports thus far."

Fullerton, who works at an insurance company, explained Thursday he found it "really, really odd" when Liberal fundraising emails started pouring into his email account within a few hours of completing the electoral reform consultation Monday.

He said he rescinded his party membership in May 2015 - in protest after the Liberals voted in favour of a controversial anti-terror law, Bill C-51 - and stopped receiving fundraising asks after unsubscribing from email lists. "They just stopped," he said. "As soon as I did that survey, I started getting them again."

Based on his experience with managing databases, his best guess, he said, was that the system automatically linked the email he inputted to another database containing past party affiliates.

Fullerton insisted he didn't engage in any other activity, or fill out any other forms, that could've caused him to start receiving emails again. That's why he found it "suspicious."

He plans to make a formal complaint against the Liberal Party for going against anti- spam legislation by sending him emails he doesn't want to receive.

NDP MP Nathan Cullen wonders why email addresses are being asked for at all, along with other details such as age, income, level of education and postal codes. Originally, the fine print on MyDemocracy.ca said survey entries that did not include those details would not be counted in results. But that text changed Thursday to say purely anonymous entries would be included in the overall, aggregate results - just not the results weighted to be more representative. "They know a lot about you, with that much information," Cullen said. "And there's worries that this eventually turns into a Liberal fundraising list." If the government was collecting data for partisan use, he said, "that would be one of the most unethical and cynical things imaginable." A spokesman for the Treasury Board Secretariat, which is responsible for government web policy, said Thursday government institutions are responsible for making sure contracts with third parties meet Privacy Act requirements. That includes not sharing personal information publicly or with other organizations, including political parties.

Personal information "is not generally collected in the course of a survey," said Alain Belle- Isle, but when it is, "respondents would be informed of the protection of their personal information prior to collection." In the case of MyDemocracy.ca, that information is available but participants must click into the "privacy policy" section of the site to find it.

The website itself is not registered to the government but to a domain name company called Go Daddy. Canada's privacy czar is looking into the electoral reform survey, but hasn't said if and when a formal investigation will be conducted.

Canadian Press
Door open to CSIS use of metadata from innocent people
Friday, 09 December 2016
Byline: Jim Bronskill

Ottawa -The federal public safety minister is keeping the door open to the idea of Canada's spy agency crunching potentially sensitive data about innocent people.
Ralph Goodale told MPs at a House of Commons committee Thursday he is weighing views on whether the Canadian Security Intelligence Service should be allowed to retain and use such information.

Last month Federal Court Justice Simon Noel said CSIS violated the law by keeping electronic data about people who were not actually under investigation.

CSIS processed the metadata beginning in 2006 through its Operational Data Analysis Centre to produce intelligence that can disclose intimate details about individuals.

Metadata is information associated with a communication, such as a telephone number or email address, but not the message itself.

The court ruling means metadata can be kept and used by CSIS only if it relates to a specific threat to Canadian security or if it is of use to an investigation, prosecution, national defence or foreign affairs.

Privacy watchdogs from across the country said this week that Canada's spy agencies should destroy the data trails of innocent people they collect incidentally during terrorism investigations, once the actual targets have been cleared of suspicion.

The office of federal privacy commissioner Daniel Therrien says metadata must be handled with care because it can reveal medical conditions, religious beliefs and sexual orientation, among other personal traits.

Goodale told MPs on the public safety committee the government would "consider all of the factors that are relevant in these circumstances" as it completes a review of national security policy.

NDP public safety critic Matthew Dube expressed concern about future problems.

"So you're not closing the door, then, to the possibility of this happening again?" Dube said. "Because to me it seems that if the Federal Court has deemed this illegal, then the answers should be clear."

CSIS director Michel Coulombe told the committee he hoped the spy service would be in a position within about six months to decide what to do with the associated metadata collected over the 10-year period.

Conservative public safety critic Tony Clement wondered why CSIS was keeping the data in question at all.

Coulombe said the law dictates that CSIS must hang on to any data used in criminal or administrative proceedings. As a result, the agency is going through the material to see what it needs to keep.

"So before we rush and destroy that information, we have to make sure that by destroying it we're not going to be contravening another court decision," Coulombe said.

"We have to take the time to do that analysis."

Globe and Mail Online
Canadian spywatcher's Snowden remark 'highly inappropriate,' Goodale says
Friday, 09 December 2016
Byline: Colin Freeze and Daniel Leblanc

Toronto and Ottawa - Public Safety Minister Ralph Goodale has rebuked a Canadian spywatcher for publicly suggesting Edward Snowden "should be shot."
"That remark strikes me as highly inappropriate," the minister told reporters in Ottawa on Thursday.

He was not the only person offended. From Russia, the famous fugitive American at the centre of the comment also found it disturbing.

"Canadian spy, charged with keeping spies from breaking the law, wants man dead for showing spies broke law," read a Tweet from Mr. Snowden on his verified account. He then added wryly, "Bonus: he's mad he was recorded."

On Wednesday, The Globe that Michael Doucet, a former Canadian intelligence analyst, gave a 90-minute talk to a small audience at Toronto's Ryerson University in which he made several off-the-cuff remarks. He later said he did not think his talk was being recorded.

When a member of the audience asked Mr. Doucet what Mr. Snowden's fate would have been had he been Canadian and leaked intelligence secrets, he replied: "Do you want my opinion on that? Do you really want it? I'll give it to you. If Edward Snowden had worked for CSIS and did what he did, he should be shot."

This comment was surprising because Mr. Doucet is executive director of a government watchdog agency, the Security Intelligence Review Committee. SIRC reviews the highly classified operations of the Canadian Security Intelligence Service, and its officials rarely make unscripted remarks in public.

Mr. Doucet quickly added that he was merely being provocative, and would like Mr. Snowden to face trial.

In 2013, Mr. Snowden was a security- cleared contractor who fled the United States with volumes of U.S. government documents. He leaked them to select journalists who wrote articles about their contents, including secret spy programs of questionable legality.

Mr. Snowden has lived in Russia for the past 3 1/2 years and would face charges under the Espionage Act should he return to the United States. Supporters consider him a principled whistle-blower, and have been pushing (https://pardonsnowden.org/supporters) for outgoing President Barack Obama to pardon him.

The Snowden leaks have woken the world up to the fact that the U.S. National Security Agency and its allies in a partnership known as the Five Eyes - Canada, Britain, Australia and New Zealand - have been collecting, pooling and analyzing global telecommunications traffic on a massive, constant and indiscriminate basis.

As a result of the Snowden revelations, the U.S. government gave up some potentially unlawful surveillance. For example, U.S. federal agents had been secretly requisitioning Americans' phone records in bulk from phone companies.

Over the years, The Globe has written about several Snowden documents pertaining to Canada.

A leaked presentation about the capabilities of powerful analytical software known as Olympia showed that, in 2012, Canadian analysts dissected telecommunications traffic related to Brazil's Ministry of Mines and Energy. They winnowed flows of global data down to specific Brazilian devices that were earmarked to be hacked at a later point.

After that leak, many Canadians expressed surprise that the federal government would apparently engage in economically driven espionage against a friendly nation.

The Snowden leaks also showed that an allied agency did similar topographical data analysis against Canadian corporations.

NSA documents suggested U.S. spies had mapped out traffic flows associated with a major Canadian bank and a telecommunications company. The reasons were never made explicit, but the mapping raised questions about whether the Five Eyes countries actually make good on their supposed gentlemen's agreement to refrain from spying on each other.

Les Echos Business (site web)
Visite sur le dark web
Friday, 09 December 2016
Byline: Journaliste maison

Non identifié - Observer ce qui se dit sur la partie « ?cachée? » d'Internet permet aux entreprises d'anticiper une attaque informatique. Mais infiltrer les réseaux cybercriminels nécessite de prendre des précautions.
Internet tient son oiseau de malheur. Cette semaine, Dailymotion n'a pas pu faire autrement que de reconnaître ses faiblesses quand le site Leaked Source a annoncé que des mots de passe et des identifiants de ses membres inscrits étaient tombés aux mains de cybercriminels. Heureusement, la plate-forme française de vidéos en ligne avait chiffré une partie de ces informations, les rendant difficilement exploitable pour un informaticien mal intentionné. Ces derniers mois, LinkedIn, Foursquare, MySpace et d'autres ont vécu l'amère expérience d'être brocardé par le site hébergé en Russie. A chaque fois, ses administrateurs invitaient gratuitement les internautes à vérifier s'ils sont concernés. Contre paiement, il propose aussi de consulter les bases de données volées. Leaked Source affirme les repérer en scannant le Web officiel et le dark web. Mais les entreprises pourraient très bien s'infiltrer elles-aussi sur la partie « cachée » d'Internet, celle où les moteurs de recherche traditionnels ne fonctionnent plus. « Je ne conseille pas aux entreprises de le faire seul mais repérer ce qui se passe

sur le dark web leur permettra de limiter les dégâts », pointe Alexeï Chachourine, analyste pour Orange Cyberdéfense. Ainsi, Dropbox a anticipé le pire l'été dernier.

Auprès des marchands d'armes informatiques

Attention, surfer sur le dark web n'est pas une promenade en bord de mer par temps calme. Certes, tout n'y est pas noir, malgré ce que laisse penser l'appellation de ce coin du cyber-espace. De simples citoyens soucieux de leur vie privée y communiquent entre eux. Mais, c'est aussi là qu'on y trouve des espions peu recommandables, des trafiquants de drogue et des marchands d'armes informatiques.

Daniel Smith, responsable de la recherche en sécurité chez Radware, guide ses interlocuteurs sur les réseaux Tor et Invisible Internet Project (I2P). Sur le moteur de recherche spécialisé Torch, il lance en anglais la requête « louer un botnet » . Pour 25 dollars, il peut souscrire au détournement de la puissance informatique d'un ordinateur vers la cible de son choix. A très grande échelle, cette technique a paralysé une partie du Web mondial en octobre dernier. Sur le darknet, des places de marché-façon eBay de la cybercriminalité- proposent des logiciels rançonneurs pour moins de 400 dollars. Pas étonnant que ce fléau fasse de plus en plus de victimes. Pour davantage de discrétion, la facture peut être réglée en bitcoins, la monnaie électronique anonyme. Sur les forums de hackers, Daniel Smith fait lire les discussions entre vendeurs et acheteurs de logiciels malveillants. Certaines communautés lui sont fermées : « pour s'inscrire, il faut commettre un crime », explique-t-il. Lui-même se dit ancien hacker mais assure n'avoir jamais franchi la limite de la loi. Certains de ses anciens camarades comptent eux sur leurs réputations d'experts techniques prêts à tout pour décrocher les meilleures missions sur des sites de petites annonces spécialisées.

Infiltration sous pseudonyme

L'environnement est effrayant mais entrer en contact avec ce monde-là permet aux responsables de la sécurité informatique de mieux comprendre leurs adversaires. « Sur le dark web, les entreprises peuvent apprendre comment sont monétisées les données volées, notamment les données bancaires, ou entendre parler d'une faille concernant leurs propres système de paiement en ligne ou leurs objets connectés », explique Alexeï Chachourine. C'est aussi là que les sites Internet peuvent savoir s'ils ont été ou sont encore dans le viseur de cybercriminels. Par exemple, des listes de sites où le vol d'identifiant de cartes bancaires paraît facile sont mises à jour quotidiennement.

Pour s'y infiltrer, les spécialistes préconisent d'utiliser un ordinateur entièrement déconnecté du réseau de l'entreprise et qui ne servira qu'à ça. « Naviguer dans le dark web est dangereux , prévient Daniel Smith, on peut cliquer sur un lien qui lance une attaque informatique sans s'en rendre compte et devenir complice d'un crime » . Lorsqu'il discute en ligne avec des hackers, il utilise une liste de pseudonymes à rallonge pour ne pas se faire repérer. Alexeï Chachourine utilise le même stratagème. « Les cybercriminels réputés se protègent des curieux. Si votre profil n'est pas sérieux, ils ne vous répondront pas », remarque-t-il. Pire, ils attaqueront. Malheureusement, c'est aussi auprès d'eux que les analystes peuvent apprendre les informations les plus intéressantes. Pour contourner le problème,

des start- up comme Cybelangel scanne le dark web pour ses clients. Mais la tâche est plus ardue que la recherche de fichiers de données menée par Leaked Source. « Lancer une surveillance automatique du dark web est impossible car les sites changent souvent de noms , réfute Alexeï Chachourine, de plus, les cybercriminels utilisent des jargons et des expressions codées inspirés par plusieurs langues » . Pour ne rien arranger, il s'agit souvent des langues rares : russe, chinois ou roumain. Sur le dark web plus qu'ailleurs, le crime n'a pas de nationalité.

Yonhap News Agency
N. Korea denies involvement in cyberattack on S.Korean military
Friday, 09 December 2016
Byline: Staff reporter

Seoul - North Korea on Friday denied its involvement in a hacking attack against South Korea's military, saying Seoul is pulling off "a childish plot" to divert public attention from its political crisis.
South Korea accused North Korea this week of being behind the first infiltration of the intranet of its cyberwarfare command in August, noting that the Internet Protocol address linked to the attack was traced to a location in China that was previously used by North Korean hackers.

North Korea's main propaganda website, Uriminzokkiri, rebuffed the claim, saying hackers never make the mistake of exposing their IP addresses or methods, which could risk revealing their identities.

"If we are behind the hacking, why do we use the IP address that the South takes issue with," Uriminzokkiri said in a report. "This a total nonsense."

It claimed South Korea is trying to provoke a confrontation with the North in a desperate attempt to survive the current political conundrum.

The National Assembly is set to vote on an impeachment motion against President Park Geun-hye over a corruption scandal on Friday afternoon.

North Korea is known to have thousands of cyberwarfare personnel. It has a track record of waging cyberattacks on South Korea and the U.S. in recent years, though it has denied involvement.

Meanwhile, the ministry neither confirmed nor denied media reports that military documents involving key operation plans were also compromised.

"We cannot confirm whether the reports are true or not as it could be useful information for North Korea," a ministry official said.

Given the hacked intranet is linked to some 700 personal computers in the Army, Navy and Air Force, chances are high that some military operation plans leaked to the rogue state.

South China Morning Post
Beijing puts out peace feeler to US on cybersecurity
Friday, 09 December 2016
Byline: Nectar Gan

Beijing - The nation's top security official told Washington yesterday that Beijing was ready to work with the administration of president-elect Donald Trump on cybersecurity, a thorny issue in Sino-US ties, state media reported.
The olive branch was extended in Washington by Public Security Minister Guo Shengkun as he met US officials for a third round of cybercrime talks, a dialogue set up by Xi Jinping and US President Barack Obama in September of last year.

Beijing and Washington have been squabbling over cybersecurity for years, with each side accusing the other of hacking and stealing trade secrets.

Beijing suspended the two nations' only cybersecurity working group in 2014 after Washington indicted five PLA officers on theft of trade secrets.

It is still unclear whether Trump will raise concerns over cybersecurity with China once he assumes office.

Trump wrote on Twitter four years ago that "the Chinese are now hacking White House computers. Why not? They already own the place".

In a debate with Hillary Clinton on the campaign trail, Trump dismissed her claims of Russian hacking, saying: "She's saying Russia, Russia, Russia. Maybe it was. It could be Russia but it could be China ... it could be somebody that sits on their bed that weighs 400 pounds."

Guo said cybersecurity cooperation had become "a new highlight in bilateral relations" between the US and China since Xi and Obama created a mechanism for the two nations to discuss cybercrimes.

"Both sides should treat this dialogue mechanism as the chief channel for communication over cyber issues to focus on cooperation, manage disputes and respond to each other's concerns in a timely and effective way," Guo was quoted as saying by Xinhua.

Allegations of hacking, however, persist.

In the latest case, the US magazine Fortune reported on Wednesday that a series of security breaches that struck prestigious law firms last year was carried out by people with ties to the Chinese government.

Beijing has repeatedly said that China is a victim of hacking and that Chinese authorities always opposed "cyber attacks in any form".

Le Temps (Suisse)
« Tous les dirigeants des organisations internationales sont espionnés »
Friday, 09 December 2016
Byline: Simon Petite

Genève - Pascal Lamy, ancien directeur de l'OMC, a été écouté par les services secrets britanniques. C'est l'une des révélations du « Monde » basées sur des documents d'Edward Snowden
Les grandes oreilles américaines et britanniques s'étendent jusqu'à Genève. L'ancien directeur de l'Organisation mondiale du commerce (OMC), le Français Pascal Lamy, a été espionné à la fin de son premier mandat en 2009. C'est l'une des révélations du Monde de jeudi, qui a eu accès à des documents de l'ancien contractant de la NSA américaine Edward Snowden. « Tous les dirigeants d'organisations internationales savent qu'ils ont le privilège d'être espionnés par tout le monde sans pouvoir espionner quiconque, ironise Pascal Lamy. Cela évite les cas de conscience, et cela permet de se croire important. »

Pays africains sur écoute

Le journal a travaillé sur des relevés d'interceptions datant du début de l'année 2009. Des recherches menées en collaboration avec le site américain The Intercept, auquel Edward Snowden, réfugié en Russie, a transmis tous ses documents. Ce travail d'enquête montre que l'Afrique et les intérêts français sur le continent ont été l'objet d'une attention particulière de la part des services de renseignement britannique et américain. En analysant ces relevés, il est apparu que les e-mails et les conversations de téléphoniques de Pascal Lamy étaient interceptés par le service de renseignements électronique du Royaume-Uni (GCHQ).

Toujours selon Le Monde, les agents britanniques cherchaient à connaître les positions du directeur de l'OMC, afin de mieux préparer une réunion du G20 en avril 2009, alors présidé par le premier ministre britannique Gordon Brown. D'autres Français occupant des positions stratégiques au sein des organisations internationales auraient été visés. Ce qui pose la question d'autres cibles à Genève, qui concentre un nombre inégalé d'institutions internationales.

Au bout du lac, ces informations ne surprennent pas. Depuis les premières révélations d'Edward Snowden sur l'espionnage de masse américain, les organisations internationales disent avoir pris des mesures pour tenter de garder leurs données sensibles à l'abri des oreilles indiscrètes. « Nous mettons régulièrement à jour nos systèmes de protection », explique Ewan Watson, chef des relations publiques du Comité international de la Croix-Rouge (CICR). Les délégués font remonter des informations sensibles, comme des rapports de visites de prison ou des témoignages de victimes de guerre avec

toutes leurs données personnelles. Des informations, qui, si elles tombaient dans les mains des gouvernements concernés, mettraient immédiatement en danger ces personnes. Le Haut- Commissariat aux droits de l'homme recourt, lui, à des systèmes cryptés, notamment pour son travail sur la Corée du Nord ou la Syrie.

Le Monde
Une vingtaine de pays africains sur écoute
Friday, 09 December 2016
Byline: Journaliste maison

Londres - Une vingtaine de pays africains ont été espionnés par les satellites du GCHQ, les services secrets britanniques, au moins entre 2008 et 2011. L'identité des cibles figure parmi des listes de milliers d'interceptions, au premier rang desquelles apparaissent les chefs d'Etats et les premiers ministres. Le GCHQ intercepte les échanges du président kényan Mwai Kibaki et de ses conseillers les plus stratégiques, mais aussi de son premier ministre, Raila Odinga, en mars 2009. Il en va de même de l'Angola, premier producteur de pétrole d'Afrique, dirigé depuis 1979 par le président José Eduardo Dos Santos - le palais présidentiel a été ciblé.
Les autorités de Kinshasa sont également étroitement surveillées. Joseph Kabila, à la tête de la République démocratique du Congo, intrigue les Britanniques, qui visent toutes ses communications et celles de ses conseillers. Le GCHQ a aussi mené des interceptions massives au Nigeria, où il suit les conversations du président Umaru Yar'Adua et de ses proches. Le chef d'Etat nigérian est mort en mai 2010 - son successeur, Goodluck Jonathan, figure aussi parmi les lignes à -intercepter.

Au Ghana, le président John Kufuor et ses collaborateurs sont écoutés; en Sierra Leone, le président Ernest Koroma; au Togo, Faure Gnassingbé; en Guinée-Conakry, Kabiné Komara, premier ministre de la junte dirigée par le président putschiste Moussa Dadis Camara, dont les proches conseillers figurent aussi dans les bases de données britanniques.

Dans les relevés de 2009 apparaissent également d'anciens chefs d'Etat : Olusegun Obasanjo au Nigeria (1999-2007) et son homologue de Sierra Leone, Ahmad Tejan Kabbah (1998-2007).

A Conakry, il s'agit de Cellou Dalein Diallo et Lansana Kouyaté, anciens premiers ministres, aujourd'hui chefs de file de l'opposition. Au Congo-Brazaville, Pascal Lissouba (1992-1997), en exil en France, a été au coeur de la surveillance en 2009.

Les ministres des affaires étrangères du Nigeria, du Kenya, du Zimbabwe, du Soudan et de Libye et nombre d'ambassadeurs sont écoutés, leurs courriels interceptés, ainsi que les élites militaires, économiques ou financières.

Le Monde
Les millions de clés de chiffrement volées de Gemalto
Friday, 09 December 2016
Byline: Damien Leloup

Londres - Ce ciblage massif et systématique de techniciens et d'employés figurant à des échelons intermédiaires de la hiérarchie d'opérateurs techniques a déjà prouvé son utilité, par le passé, pour le GCHQ. En février 2015, The Intercept révélait, sur la base de documents Snowden, que c'est par ce biais que les services britanniques étaient parvenus à voler des millions de clés de chiffrement de cartes SIM à l'entreprise franco-néerlandaise Gemalto. Peu connue du grand public, Gemalto est l'un des principaux fabricants mondiaux de puces sécurisées : ses produits équipent passeports électroniques, cartes de paiement, ou encore téléphones portables.
C'est notamment ce dernier point qui intéressait le GCHQ: une fois les clés de chiffrement des cartes SIM en sa possession, l'agence pouvait aisément mettre sur écoute des lignes téléphoniques dans un certain nombre de pays. L'agence s'est donc penchée sur toute une série de salariés de l'entreprise, dont les noms ou adresses mail ont été ajoutés à sa base de données de cibles potentielles. Plusieurs responsables techniques ou commerciaux ont ainsi été surveillés électroniquement - un document interne du GCHQ évoque ainsi comme cible prioritaire un employé de l'entreprise qui communique occasionnellement par courriels chiffrés : «Nous avons vu qu'il envoyait des fichiers chiffrés grâce à XKey score [le principal outil de surveillance de la NSA et du GCHQ]. Si nous nous intéressons de nouveau à ce dossier, c'est probablement un très bon endroit par où commencer. »

Méthodologie constante

A l'époque, Gemalto utilisait occasionnellement des fichiers chiffrés transmis par email pour fournir des clés de chiffrement à ses clients - une pratique qui n'a plus cours dans l'entreprise. La méthodologie du GCHQ, elle, semble être restée constante au fil des ans, et sur tous les continents: identifier des «cibles» intéressantes, puis tenter de prendre le contrôle de leur boîte e- mail ou de leur ordinateur grâce à des logiciels-espions envoyés par courriel.

Comment les services secrets britanniques choisissaient-ils ces cibles ? D'autres documents Snowden, publiés par The

Intercept, montrent que le GCHQ avait mis au point un système de classement élaboré, qui leur permettait de « noter » les cibles potentielles. Un script automatisé récoltait toutes les conversations électroniques des cibles potentielles, et «notait» ces dernières en fonction de la fréquence à laquelle elles utilisaient certains termes techniques. Au début des années 2010, le GCHQ avait ainsi sur sa liste prioritaire des employés de Gemalto, du constructeur chinois Huawei, du finlandais Nokia, du fournisseur d'accès Belgacom ou encore de Yahoo! et de Google.

Le Monde

Les techniciens télécoms, cibles de choix
Friday, 09 December 2016
Byline: Damien Leloup, et Martin Untersinger

Londres - La surveillance des employés permet d'accéder au réseau interne des opérateurs téléphoniques
Parmi les cibles du -Government Communications Headquarters (GCHQ), l'agence de -renseignement technique britannique, ils côtoient trafiquants d'armes, leaders politiques du Moyen- Orient et chefs de groupuscules terroristes.

Leur tort? Travailler pour un opérateur de téléphonie. Plusieurs documents extraits par Le Monde, en collaboration avec le site The Intercept, des archives de l'ex-consultant de l'Agence nationale de sécurité (NSA) américaine, Edward Snowden, confiées à Glenn Greenwald et Laura Poitras, prouvent en effet que les employés des télécoms constituent une part significative des cibles du GCHQ. Ils permettent aussi d'éclairer d'un jour nouveau les -piratages de Belgacom et de -Gemalto, deux opérations d'ampleur menées notamment par les services britanniques et révélées ces trois dernières années.

Le Monde a pu éplucher des -dizaines de documents internes de l'agence britannique de renseignement, des comptes rendus de tests sur des liaisons par satellite acheminant trafic Internet et téléphonique. Les employés d'opérateurs téléphoniques, à tous les niveaux de la hiérarchie, apparaissent très fréquemment dans les cibles du GCHQ. Deux pièces, datées du printemps 2009, relatent même les efforts de l'agence pour intercepter les communications internes de deux opérateurs très présents au Moyen-Orient et en Afrique.

Un document du 10 juin 2009, intitulé " Réseau intranet Zain ", décrit les tests menés par le GCHQ sur un flux satellitaire -faisant transiter des communications internes à l'opérateur -téléphonique Zain. Basé au Koweït, il est présent dans huit pays, essentiellement au Moyen-Orient. En 2010, Zain a vendu ses activités dans ces pays à l'indien Bharti Airtel, troisième opérateur mobile mondial. Mais, à l'époque des documents, il est très présent en Afrique et opère encore dans quinze pays, du -Burkina Faso au Niger en passant par l'Ouganda et le Tchad.

Négociation commercialeCet opérateur n'est pas le seul à intéresser les Britanniques : un document du 16 avril 2009 montre que le GCHQ a repéré une liaison satellite acheminant des communications internes à l'opérateur, " entre ingénieurs ", de MTN. MTN, groupe sud-africain fondé en 1994, est présent dans une vingtaine de pays d'Afrique et fait partie des poids lourds du secteur, avec plus de 200 millions de clients.

Dans nombre de ces documents apparaissent des employés d'opérateurs télécoms. Il y a bien sûr des cadres de haut -niveau comme le directeur des opérations de Zain en Arabie saoudite, le directeur logistique du groupe, le directeur technique de Touch, filiale de Zain au Liban, et même Chris Gabriel, le -directeur Afrique du groupe à l'époque.

Mais la plupart des cibles ne sont pas des cadres importants de ces entreprises télécoms. Il s'agit des responsables " roaming " dans au moins quinze pays - africains. Ils représentent à eux seuls environ la moitié des cibles au sein des opérateurs télécoms - aucun d'entre eux n'a donné suite à nos sollicitations. La -minutie avec laquelle le GCHQ s'intéresse à eux ne fait aucun doute sur le caractère stratégique, pour l'agence, de leurs échanges électroniques.

Le " roaming ", ou " itinérance ", permet aux abonnés mobiles d'un opérateur téléphonique d'utiliser leur téléphone dans un autre pays. Pour que cela fonctionne, les opérateurs téléphoniques doivent nouer des partenariats, soit directement l'un avec l'autre, soit en passant par un intermédiaire qui centralise les accords.

Cette négociation commerciale a un pendant technique : il faut pouvoir configurer les réseaux pour que le téléphone soit reconnu où qu'il se trouve, et -pouvoir également décompter pré-cisément l'activité du téléphone pour la facturation. Les personnels des opérateurs téléphoniques ont donc un double profil, à la fois technique et - commercial. Ils peuvent donc être amenés à disposer du Graal pour les agences de renseignement : un accès au réseau interne de leur opérateur.

Une attaque visant des responsables itinérance est rare, mais pas inédite. Des documents Snowden publiés par The Intercept avaient révélé que l'entreprise Belgacom avait été victime d'un piratage massif organisé par le GCHQ, touchant aussi bien ses ordinateurs que son réseau de télécommunications, au début des années 2010. Ce piratage, particulièrement bien conçu et discret, visait en priorité une -filiale peu connue de l'opérateur : BICS, Belgacom International Carrier Services, la branche de l'opérateur qui gère les accords d'itinérance avec d'autres opé-rateurs. C'est cette filiale qui -négocie avec des opérateurs dans le monde entier pour établir des partenariats d'itinérance, permettant d'interconnecter leurs réseaux.

Ce piratage accrédite l'hypothèse selon laquelle ces responsables itinérance ne sont pas la cible finale du GCHQ, mais plutôt la porte d'entrée au réseau -interne des opérateurs télécoms. Les documents n'indiquent pas si une attaque a bien eu lieu : ils indiquent simplement que les agents du GCHQ se sont intéressés de très près aux e-mails de ces responsables. Les informations recueillies dans ces courriels peuvent être cruciales pour une reconnaissance préalable à une véritable attaque des réseaux des opérateurs.

" Ticket d'entrée "Espionner les courriels est en effet un bon moyen pour comprendre leurs responsabilités, leurs relations hiérarchiques, les processus de décision interne, mais aussi comprendre la partie du réseau informatique à laquelle ils ont accès, sa configuration, les matériels qui y sont - installés, les différentes autorisations... Autant d'informations nécessaires pour cibler une attaque, par exemple en effectuant une opération d'hameçonnage, qui consiste à l'envoi de courriels apparemment anodins ou habituels pour subtiliser des mots de passe ou installer un logiciel malveillant. Une fois dans l'ordinateur, il est facile d'installer un dispositif d'espionnage dans le réseau de l'opérateur.

Ce mode opératoire est même décrit dans un document interne à la NSA et lui aussi publié, dès 2014, par The Intercept . Un ingénieur de l'agence y décrit sa " chasse " aux gestionnaires des réseaux. Il explique : " On ne peut pas collecter tout, tout le temps. Si une cible commence à utiliser un réseau que nous n'interceptons pas, il y a un peu de travail à faire pour diriger notre système d'écoutes dans sa direction. (...) Imaginons qu'une de vos cibles utilise son mobile sur un réseau à l'étranger. (...) Ce serait vraiment sympa si nous avions accès aux infrastructures locales - qu'il utilise - , où nous pourrions suivre sa position et l'intégralité de ses appels. "

Pour cela, écrit cet analyste, il faut d'abord surveiller et compromettre ceux qui détiennent " les clés du royaume ", soit les techniciens gérant ce réseau. Il mentionne, dans ce même document - une lettre d'information interne -, les adresses e-mail comme un mot-clé très intéressant pour repérer et compromettre ces techniciens. Les pirater, " c'est généralement le ticket d'entrée au réseau ", conclut-il.

Les documents consultés par Le Monde n'indiquent pas la cible finale du GCHQ, ni même si la surveillance des communications de la liste des cibles a bien eu lieu. En revanche, est-il légitime de surveiller des gens qui n'ont rien de suspect, ou de pouvoir accéder aux communications de centaines de milliers de clients d'un opérateur téléphonique?

Le Monde
Les satellites, des espions venus du ciel
Friday, 09 December 2016
Byline: Jacques Follorou et Martin Untersinger

Yorkshire, Royaume-Uni - Les services captent les données qui arrosent la planète et y cherchent des mots-clés pour évaluer leur intérêt
Les révélations de l'ex-consultant de la NSA Edward Snowden, qui ont essentiellement porté sur l'espionnage d'Internet par les câbles sous- marins, ont eu tendance à le faire oublier, mais l'espionnage par satellite a fait figure, pendant des décennies, de joyau du renseignement technique. Voici comment les grandes puissances écoutent encore des communications du monde entier.

Le fonctionnement des satellites géostationnaires qui encerclent la planète est relativement simple, et leur surveillance l'est tout autant. Lorsqu'un satellite renvoie les données vers la surface de la Terre, il arrose une vaste zone où les flux de communication (Internet, téléphone...) sont récupérés par des antennes de réception. Et où ils peuvent aussi être interceptés. Il suffit par exemple aux stations d'écoute des services de -renseignement britanniques du -Government Communications Headquarters (GCHQ), l'équivalent de la NSA américaine, de pointer leurs antennes vers ces satellites et de se " brancher " sur les fréquences utilisées pour récupérer ce flux de communication.

Parmi ses sites d'interceptions satellitaires, le GCHQ dresse ses grands radômes blancs au bord d'une falaise, à Bude, bourgade de Cornouailles. Deux sites sont installés sur des bases militaires à l'étranger, l'une à Chypre, l'autre à Oman, assurant une couverture idéale du Proche et du Moyen-Orient. Le

Royaume-Uni abrite une autre station d'écoute satellite, dans le Yorkshire, à Menwith Hill, administrée par des personnels de son grand allié, la NSA.

Méticuleux travailLorsqu'un satellite est reconfiguré ou un nouveau flux de communication inauguré, les techniciens du GCHQ sont d'abord - chargés de déterminer si l'interception est techniquement possible. Les documents obtenus par Le Monde sont le résultat de ce travail de test. Dans l'écrasante majorité des cas, à la question : " Est-ce que cet opérateur - "carrier" - peut être chargé - "tasked", surveillé - dans le système de collecte? ", la réponse est positive.

Ensuite, les techniciens doivent déterminer si des informations pertinentes peuvent en être extraites. Pour ce faire, ils soumettent à ce flux de communication une liste de " sélecteurs ", des mots-clés qu'ils estiment être -intéressants correspondant à des numéros de téléphone ou à des adresses électroniques. Les documents font donc apparaître une liste des communications : il ne s'agit pas de la retranscription du contenu de l'appel ou de l'échange de courriels, mais simplement de l'énumération de toutes les conversations impliquant ce numéro ou cette adresse surveillée. Parfois des échanges SMS.

Ces documents ne fournissent pas de renseignement, ils sont simplement destinés à déterminer si l'écoute d'un flux satel-litaire est susceptible, à l'avenir, d'en fournir, en listant toutes les fois où une adresse ou un numéro de téléphone intéressant les services s'est manifesté.

Le résultat de ce méticuleux travail figure dans la centaine de documents techniques du GCHQ que Le Monde a pu consulter. Ils donnent un aperçu de la manière dont les services de renseignement techniques travaillent pour s'assurer d'un accès toujours plus complet aux communications. Même si les documents ne détaillent ni la durée, ni l'ampleur, ni le contexte de la surveillance des cibles du GCHQ, ils permettent de mieux comprendre qui les services britanniques et leurs alliés veulent surveiller, et donc de discerner leur stratégie et leurs objectifs - qui vont souvent bien au-delà de la lutte contre le terrorisme ou la prolifération nucléaire.

La place conservée par les satellites pour les communications entre l'Afrique et le reste du monde tient à trois facteurs. L'architecture des télécommunications de ce continent est encore marquée par l'histoire coloniale et une des épines dorsales de ce réseau relie encore l'Europe, dont la France ou la Belgique, à ses anciennes colonies. Le deuxième réside dans des considérations purement pécuniaires : il n'est pas financièrement intéressant de construire des infrastructures qui relient directement l'Afrique au Moyen-Orient ou à d'autres régions du monde. Mieux vaut -emprunter des routes déjà tracées par l'Europe.

Enfin, si l'ouest de l'Afrique est plutôt bien -connecté à Internet grâce à plusieurs câbles sous-marins qui le relient à l'Europe, le reste du -continent et notamment l'Afrique centrale manquent encore d'infrastructures terrestres.

Un document de synthèse à diffusion restreinte du ministère britannique de la défense, daté de 2010 et fourni par Edward Snowden, résume l'intérêt des satellites pour les espions de la surveillance. Dans les

vingt principaux marchés d'Afrique subsaharienne, 45,6 % des communications internationales empruntaient la voie satellitaire, note le document, qui constate aussi que " de nombreux fournisseurs d'accès à Internet africains reçoivent de la bande passante de l'étranger par satellite " . L'explosion d'Internet n'a pas été complètement absorbée par la pose de nouveaux câbles : la demande satellitaire en Afrique a, depuis, continué à progresser L'interception est devenue massive.

New York Times
After Cyberattacks, Germany Fears Russia May Disrupt Vote
Friday, 09 December 2016
Byline: Melissa Eddy

Berlin - After hackers infiltrated the German Parliament's computer network in May 2015, it took nearly a year before the country's intelligence agency concluded that the attack was most likely the work of their Russian counterparts.
Last week, when 900,000 Germans lost access to internet and telephone services, it took a matter of hours before politicians began pointing fingers at Moscow.

Berlin is now concerned that Germany will become the next focus of Moscow's campaign to destabilize Western democracies as national elections approach next year.

Those fears intensified after the Obama administration accused the Russian government of attacking Democratic Party emails during the American presidential campaign.

The increasing dissemination of false news, disinformation and propaganda during the American campaign and before Italy's referendum last weekend has added a related layer of worry about the potential to corrupt public debate and democratic processes.

Hans-Georg Maassen, the head of Germany's domestic intelligence agency, warned in an interview on Thursday of "growing evidence for attempts to influence the federal election next year."

His agency has seen an increase in "aggressive cyberespionage" targeting German politicians, he said.

If the advent of the personal computer helped undermine a closed Soviet system that could not compete in an information age, then exploiting the vulnerabilities of the internet and social media may be Russia's revenge.

Intelligence and other officials can now point to a growing string of campaigns of disinformation, hacked computer networks and leaked emails fitting a pattern that traces a murky route back to Moscow.

The aim, they say, is to undercut liberal opponents of Moscow, destabilize political systems and undermine democratic processes across the European Union and in NATO member countries, while supporting anti-European forces.

"Based on the prevailing Russian strategy of hybrid influence and destabilization, which we have observed over time and for which we have facts, the government, officials and some political parties have become sensitized to this form of conflict," said Wilfried Jilge, an expert on Ukraine and Eastern Europe with the German Council on Foreign Relations.

"Such suspicions are the result of observation and experience over the past year and a half," Mr. Jilge said.

Many of the efforts seem intended to tilt elections in a direction preferred by Moscow or to undercut certain leaders.

That was presumably the motivation for hacking the Democratic National Committee and leaking emails that embarrassed Hillary Clinton, who long had an antagonistic relationship with the Russian president, Vladimir V. Putin.

On the other hand, her challenger, the eventual winner, Donald J. Trump, was effusive in his praise for the Russian leader.

False news, also linked to Russia, was widely disseminated in Italy by opponents of the push by Prime Minister Matteo Renzi for constitutional changes. Many of those opponents are much closer to Moscow than to Mr. Renzi, who lost and has now resigned.

Germans have not been immune to such disinformation, either.

In January, a news article that said a 13-year-old Russian-German girl had been kidnapped and raped by migrants in Germany spread quickly on Russian-language news channels.

Outrage over a supposed cover-up of the abuse drew members of Germany's Russian-speaking minority into the streets across the country, shocking German politicians.

German police officials later proved that the events never took place. But the damage was already done, and the false report fed opposition to Chancellor Angela Merkel's decision to open the doors to nearly a million refugees.

As for Moscow's motivations in Germany, Eberhard Schneider, a professor of political science at the University of Siegen, has observed Russia's propaganda tactics since the days of the Cold War.

Ms. Merkel, he noted, was one of the strongest supporters of the sanctions against Russia for its annexation of Crimea and the war in eastern Ukraine. Mr. Putin has a strong incentive to undermine her.

"Germany is the most important power in the European Union," he said. "If you can harm Germany and prevent that Merkel has a good outcome in the next election, that is in his interest."

The disruption at Deutsche Telekom, which began on Nov. 27, set off a fresh round of alarm over potential Russian meddling and the vulnerability of Germany's computer networks, which could be disrupted or hacked during an election.

A day after the breach, Bruno Kahl, head of the Germany's foreign intelligence service, raised the prospect of evidence linking Russia to interference in the United States election campaign and warned that Germany could be next.

"It is known that cyberattacks take place which have no other purpose than to provoke political uncertainty," he told the newspaper Süddeutsche Zeitung.

"These attempts to interfere focus on Europe, and on Germany especially," Mr. Kahl said. "A kind of pressure is being exercised on public discourse and democracy here, which is unacceptable."

Investigations into the incident later blamed links to "criminal organizations," though neither Deutsche Telekom nor the government disclosed any concrete link to Moscow.

Observers like Mr. Jilge of the Council on Foreign Relations say that caution is prudent in assigning blame, but that suspicion of Moscow is warranted given the accumulating pattern.

"The fact that hackers appeared to have carried out this attack does not automatically mean that they are linked to Russia," he said of the Deutsche Telekom attack.

"But if we look at the target and the timing, and know that such influence and disinformation is part of the Russian approach, then it is not surprising that some would seek to address this issue," he said.

Asked about the Deutsche Telekom disruption, Ms. Merkel said she did not know who was responsible, but she also mentioned Russia.

"I will simply say, such cyberattacks, or hybrid conflicts as they are known in Russian doctrine, are now part of daily life and we must learn to cope with them. We must inform people a lot on this point," the chancellor told reporters last week.

"We cannot allow ourselves to be unsettled by this," Ms. Merkel said. "We must simply know that this exists and learn to live with it."

Both Deutsche Telekom and the government's Office of Information Security said a strain of the Mirai malware, which seeks to embed itself in devices connected to the internet, appeared to have caused the disruption.

Mirai was the same malware used in an attack in the United States in October that brought down websites for Twitter, Netflix, Spotify, Airbnb, SoundCloud and The New York Times, among others.

In Germany, the malware apparently succeeded only in knocking out the routers and disrupting internet connections.

"According to our analysis, the objective of the attack is to install malware on the routers to add them to a botnet -- meaning they could be used as the remote-controlled infrastructure for future attacks," Deutsche Telekom later said in a statement.

The company pledged to focus on improving its network security to render it better able to resist any form of attack.

The speed with which officials began to suspect Russia was a stark contrast to 2015, when hackers used a phishing tactic, using a fake email, to penetrate computers in Germany's lower house of Parliament.

Only this past May did Mr. Maassen's domestic intelligence agency confirm suspicions that Russian intelligence was behind the attack. Finally, in October, it issued a broad warning.

"German parties or politicians," it cautioned, "could fall into the focus of Russian cyberespionage campaigns and operations."

Wall Street Journal
Georgia Says Someone in U.S. Government Tried to Hack State's Computers Housing Voter Data
Friday, 09 December 2016
Byline: Brian Tau

New York - The secretary of state of Georgia is asking the Department of Homeland Security to explain what appears to be an attempted breach of the state's computer systems that house its voter registration database by someone in the federal government.
In a letter to Department of Homeland Security Secretary Jeh Johnson dated Thursday, Georgia's Secretary of State Brian Kemp said the state had discovered an unsuccessful attempt to breach the firewall of state computer systems. The attempt occurred on Nov. 15 and was linked to an IP address associated with DHS, he said.

"We are looking into the matter. DHS takes the trust of our public and private sector partners seriously, and we will respond to Secretary Kemp directly," a spokeswoman for DHS said.

"At no time has my office agreed to or permitted DHS to conduct penetration testing or security scans of our network," wrote Mr. Kemp, a Republican. "Moreover, your department has not contacted my office since this unsuccessful incident to alert us of any security event that would require testing or scanning of our network."

The alleged attempted intrusion by the federal government on a state computer system responsible for election security was detected by a third-party security firm working for the state of Georgia. The attempt was unsuccessful, according to the state. The computers also house information about company incorporations.

In his letter, Mr. Kemp asked the department to confirm whether a scan attempt was made, who authorized the scan and whether the department was scanning other state systems without authorization.

The Department of Homeland Security made a major push in advance of November's elections to help states secure election systems against possible hacking, as fears of foreign interference in the U.S. election process reached a fever pitch in the months leading up to Election Day.

The department also considered declaring election systems "critical infrastructure," which would have given the federal government additional authority to protect the systems. DHS didn't take that step, however, as many states expressed concern about additional federal authority over their election systems and said the constitution provided states the right to run their own elections.

As a result of some of the concerns, the department clarified that assistance on election-related security matters was voluntary and encouraged states to take advantage of DHS resources and expertise to help secure state election systems.

"DHS assistance is strictly voluntary and does not entail regulation, binding directives, and is not offered to supersede state and local control over the process," Mr. Johnson, the DHS chief, said in September.

Georgia was one of the states that had declined the federal government's assistance for election security, citing state sovereignty. "Right now, we're just demanding answers," said David Dove, a top aide to the Georgia secretary of state. "My boss, Secretary Kemp, has been a very vocal critic of the Department of Homeland Security declaring election systems critical infrastructure."

Jerusalem Post
Ministers welcome social media sites tackling terrorism
Friday, 09 December 2016
Byline: Gil Hoffman

Jerusalem - Justice Minister Ayelet Shaked and Strategic Affairs Minister Gilad Erdan welcomed on Thursday a move by social media giants Facebook, Twitter and YouTube aimed at curbing the spread of terrorist content online.
According to the companies, they will create a shared industry database of "hashes," unique digital "fingerprints," for violent terrorist imagery, terrorist recruitment videos or images that have been removed from their services that they will then share with one another.

The database will be open to all of the companies. Each individual company will then be able to review a "hash" according to their own content policies and decide whether or not to remove something that another company has already removed.

The move came after Israel and other countries complained that social media companies had not been doing enough to reduce the amount of terrorist-related content. Erdan and Shaked met in September with top executives from Facebook who visited Israel.

Shaked said that while the initiative was a positive step, there was still plenty more that companies like Facebook, Youtube, and Twitter could be doing.

"Terrorism is a common enemy for the entire free world, so there should be no difference between sovereign countries and massive suppliers of content that have been used by terrorists in order to murder men, women, children, and elderly people," Shaked told The Jerusalem Post. "I am glad that the meetings with Facebook executives that I conducted together with Minister Erdan brought positive results."

Erdan posted the announcement by the social media companies on his official Twitter account in English, along with an explanation in Hebrew. He added that the social media companies still need to take more responsibility to clean themselves of incitement and "not wait for our overtures to do the work for them." "This is important in order to clean the Internet of content identified as inciting," Erdan wrote.

Shaked also credited a bill she and Erdan publicized in July that would require removing terrorism-promoting content from the Internet and various social media platforms. The Ministerial Committee for Legislation advanced the bill, which was officially sponsored among others by Zionist Union MK Revital Swid, who heads a Knesset caucus on fighting violent discourse and incitement on the Internet.

The bill would empower courts to order social media providers to remove content that is in criminal and constitutes a danger to personal, public or state security. It would also give the state vast powers that it does not possess in standard proceedings. The state could seek a court order for removal without giving notice to the social media platform, introduce classified evidence and introduce evidence that would not normally be admissible.

The legislation would give social media companies 48 hours from the time the incitement is posted to remove it or be fined NIS 300,000 per post. If there is proof the site knew about the content encouraging terrorism and still did not remove it, the fine will be increased to NIS 400,000.

Swid said the social media companies realized, albeit too late that they play a key role in the struggle against terrorism. "Forming the database is a welcome first step in the worldwide struggle against terrorism," she said. "I expect the companies to take more steps like including a link to report incitement to terrorism that would be dealt with immediately. This is necessary and can save lives."

Gulf News
Public-private partnerships in cyber security
Friday, 09 December 2016
Byline: Faisal Al Bannai

Dubai - The model of government as regulator and companies as regulated is not sustainable in the realm of cyber security. Instead, what's required is the fostering of public-private partnerships (PPP). PPPs have been effective in addressing problems associated with large physical infrastructure projects and have been extremely useful in overcoming barriers to project execution related to all types of risks, access to capital, and efficient project delivery.

These partnerships also provide a powerful means of addressing social and economic problems -- education, public health, road safety and pollution -- that are difficult or next to impossible for a single entity or government agency to tackle on its own. Through PPP, all parties involved -- government, the private sector, academia, etc -- bring their different resources to the problem.

This is the kind of public-private partnership approach we need for cyber security. Neither government nor the private sector by itself can be singularly effective enough. Bringing all parties' resources together is the key.

In the digital world, cyber threats move faster than regulations and legislation can be implemented. This can mean laws are constantly playing catch up.

What's more, for us to address cyber threats, it's essential that information be shared in a timely fashion, and often in unconventional directions -- such as between government and industry, between law enforcement and industry, among nations, and across both industry and government department silos.

Making this information flow and keeping it flowing is one of the most important roles that government can play in boosting cyber security. Government also must work with industry and educators to build a larger pipeline of young people into the cyber security industry.

As a coordinator, government can set up the systems and organisations to enable rapid information sharing across stakeholders, including reticent corporates. Government can also encourage other types of knowledge sharing, including best practice, and help formalise this with standards and regulations that at least provide a baseline level of security.

Public-private partnership is no panacea. But in a world where traditional lines are blurred; information is held by countless parties; and attackers and targets are a mishmash of strategic government agencies, individual consumers and lone wolf hackers, PPP is a compelling way to respond effectively.

We are already seeing evidence of this with the establishment of entities such as the Smart Dubai Office, the government entity charged with overseeing Dubai's citywide smart transformation, engaging with leadership in the public and private sector to make Dubai a global benchmark smart city.

The passage of Dubai's Open Data Law last year, also highlights the efforts in the public sector to organise the operation and security of digital information. The law regulates the use and sharing of "Dubai Data", which is defined as any data related to the Emirate of Dubai and which is available to data providers. This makes this legislation a fundamental component of Dubai's smart city ambitions with respect to the exchange of actionable information between critical entities.

We've built everything from power plants to hospitals with PPP. Now it's time to use it to build perhaps our most important edifice yet, a secure cyber future.

Xinhua News Agency
Third China-U.S. cybersecurity ministerial dialogue yields positive outcomes
Friday, 09 December 2016
Byline: Staff reporter

Washington - The third China-U.S. ministerial dialogue on fighting cyber crimes and other related affairs issued Thursday a list of positive fruits as the two sides worked hard to strengthen cooperation in cybersecurity.
The dialogue was co-chaired by China's State Councilor and Minister of Public Security Guo Shengkun with U.S. Attorney General Loretta Lynch and Secretary of Homeland Security Jeh Johnson.

During this round of dialogue, both sides endorsed the establishment of the dialogue mechanism as beneficial to bilateral communication and enhanced cooperation, and both regarded further solidifying, developing, and maintaining the dialogue mechanism as beneficial to mutual interests.

Both sides recommitted to cooperate on investigating cyber crimes and related matters emanating from China or the United States and to refrain from cyber-enabled theft of intellectual property with the intent of offering competitive advantages to companies or commercial sectors, said the document.

China and the United States identified a number of areas for future cooperation on enhancing cybersecurity, including enhancing network hygiene by cleaning and patching malware infections in respective networks, engaging in regular reciprocal sharing of malicious IP addresses, malware samples and other network protection information.

The two countries pledged to continue discussion on future cooperation in cybersecurity of critical infrastructure, and to hold as early as possible in 2017 a China-U.S.government and technology company roundtable to discuss cybersecurity issues of mutual concern.

As to the fight against cyber terrorism, both sides acknowledged the seminar on misuse of technology and communications to facilitate violent acts of terrorism held in November this year in China. Both sides will consider holding another seminar in 2017.

The two countries agreed that the dialogue should continue to be held each year.

In his remarks to the meeting, Guo noted that under the auspices of Chinese President Xi Jinping and his U.S. counterpart Barack Obama, China-U.S. cooperation in safeguarding cybersecurity is booming and has yielded positive outcomes in cracking down on cyber crimes and related matters.

Calling the current China-U.S. cooperation in cybersecurity a link between past and future, Guo proposed that the two sides press on in using the dialogue mechanism as the main channel for communication in tackling cybersecurity issues, give prompt and effective response to the requests from the other side, and constructively manage their differences.

The U.S. side said that China and the United States share common interests in fighting cyber crimes and protecting cybersecurity, and the high-level dialogue mechanism also serves as a crucial platform for candid communication and enhancing mutual understanding and trust between law enforcement officials of the two countries.

According to 2014 data from the Cyberspace Administration of China, China has been a victim of cyber-attacks. More than 10,000 websites are tampered with every month, and about 80 percent of government websites suffered attacks, mainly originating in the United States.

Also, the Internet Society of China reported that 84 percent of Internet users in the country have been affected by personal information leaks. The number of Internet users in China hit 710 million in June this year.

China's top legislature in November adopted a cybersecurity law to safeguard sovereignty on cyberspace, national security and the rights of citizens.

Haaretz

German Maker of Israeli Submarines Says Secrets Stolen in 'Massive' Cyberattack
Friday, 09 December 2016
Byline: Gili Cohen

Jerusalem - ThyssenKrupp, the German maker of Israel's new fleet of submarines, has been the victim of a "massive" cyberattack, the company said Thursday.
In response to a question from Haaretz, ThyssenKrupp said that the cyberattack did not affect any of its naval projects, including those linked to Israel.

The company, which owns the shipyards now building new warships for Israel, has been in the center of a scandal in recent weeks involving Netanyahu's personal lawyer and the role he might have played in Israel's deal to buy the submarines.

Technical trade secrets were stolen earlier this year in the hack, the steelmaker said on Thursday. "ThyssenKrupp has become the target of a massive cyberattack," the German company said in a statement.

In attacks discovered in April and traced back to February, hackers stole project data from ThyssenKrupp's plant engineering division and from other areas yet to be determined, the company said.

Israel has bought submarines from ThyssenKrupp for billions of dollars. Iran, which indirectly owns stock in the group, has received the equivalent of tens of millions of euros in dividends from ThyssenKrupp, a Haaretz investigation of the company's financial reports revealed.

ThyssenKrupp, one of the world's largest steel makers, attributed the breaches to unnamed attackers located in Southeast Asia. It did not identify which documents were stolen and said it could not estimate the scale of the intellectual property losses. A criminal complaint was filed with police in the state of North Rhine-Westphalia, it said.

Secured systems operating steel blast furnaces and power plants in Duisburg, in Germany's industrial heartland in the Ruhr Valley, were unaffected, the company said.

No breaches have been found at other businesses ranging from elevators to its marine systems unit, which produces military submarines and warships. ThyssenKrupp is a major supplier of steel to Germany's automotive sector and other manufacturers.

It said the attack was uncovered by ThyssenKrupp's in house computer emergency response team. State and federal cyber security and data protection authorities were informed. The management board was made aware of the attacks at an early stage, it said.

Ottawa Citizen
Cheaper alternative for Canada.ca project ignored, sources say
Saturday, 17 December 2016
Byline: Vito Pilieci

Ottawa - The federal government could have employed a simple framework for its massive Canada.ca web renewal project, making it much cheaper than the large corporate Adobe contract it signed, several sources familiar with the project say.
The web renewal initiative, which aims to move all of the government's disparate department websites into a single Canada.ca domain, has been plagued with budget overruns and delays. Today, fewer than 10 federal departments are in the process of moving to the new website. The project intended to see as many as 90 departments move to Canada.ca by 2017.

The government awarded Adobe a $1.95-million contract in March 2015 to provide services that would allow it to merge its various departmental websites under the Canada. ca banner. The value of that contract has since ballooned to more than $9.2 million.

Another solution that was passed over, according to insiders, could have resulted in a more cost-effective approach.

DrupalWXT, a website technology already used by departments such as Statistics Canada, as well as the technology powering Whitehouse.gov in the United States, was proposed by government employees during the consultation process, several people familiar with the talks confirm. DrupalWXT would have allowed staff to manage the conversion to Canada.ca, and its open-source software would have made the project far cheaper than turning to a commercial solution.

Government employees even created a demonstration website that mimics the look, colour scheme and layout of the Canada. ca webpage to prove the technology could work.

However, according to sources, the open-source option wasn't even considered by Services Canada when it was tasked with revamping the federal government's presence online. Only commercial offerings were looked at.

The Request for Proposals document, released on Oct. 16, 2014, notified businesses of the government's intentions so they could bid on the project and stated: "Canada has a requirement for a commercially available fully hosted Managed Web Service."

The document later said the government is specifically looking for "100 authenticated user licences" for the new web platform.

Open-source software isn't commercially available: it's open by nature, and users don't need to pay for a licence.

The request attracted interest from three companies: Adobe, Dell and the Hewlett-Packard Company (HP). The bids by Dell and HP were deemed "non-compliant" by Service Canada, and Adobe won the contract.

Government officials would not say why the open-source, in-house solution was passed over. Instead, officials asserted a competitive bidding process took place and the best bid was awarded the contract.

"The RFP was to procure a Managed Web Service that would support the Government of Canada's objective to transform its web presence to better serve Canadians by taking advantage of new technology and make it easier for the public to search and find information online using any device," said Amélie Maisonneuve, a spokeswoman for Human Resources and Skills Development Canada, the department responsible for Services Canada.

"Contracts were awarded following an open and fair competitive procurement process."

Tom Cochran, chief digital strategist at cloud computing firm Acquia and former deputy assistant secretary at the U.S. Department of State, as well as director of digital technology at the White House, said the reason the governmentmade solution wasn't chosen is because there are still too many people who don't understand the value of open-sourced software.

"It is disappointing to see a great opportunity for digital innovation in government and shared economic prosperity fall flat due to old-school IT procurement practices, favouring proprietary software companies," he said.

"A large advantage of our shift to open source was the removal of vendor lock-in, opening up our support contracts to hundreds of small-and medium-size companies. Rather than awarding sizable millions to massive corporations, we were able to work with small local businesses to support the regional tech economy."

Cochran said in the U.S., 11 of the 15 departments in the president's cabinet are using open-sourced software - Drupal - to run their websites. He said 20 per cent of state governments have also shifted to run their websites on the open-source software, and it's also expanding in popularity with municipal governments.

The ballooned $9.2-million Adobe contract does not reflect what it will cost each government department to prepare their websites for the move to Canada.ca. While an overall cost estimate is not available, each department is responsible for rolling the costs into their own budgets, and six federal departments revealed they expected to spend $19.79 million in total of their own funds to prepare for the switch.

The push to consolidate the sites cost the federal government one of its top bureaucrats, who said he resigned from his position specifically because he believed the move to a single unified website could hamper the ability of individual departments to disseminate timely information to Canadians.

"I objected, saying, 'This wasn't going to work for us. Statistics Canada could not go work through this shared website because we would lose control over the dissemination of our information. People wouldn't have access to this information in a timely manner,'" said Wayne Smith, formerly the chief statistician with Statistics Canada. "We fought a long, hard battle over that. They had said there will be no exceptions. You can't have people outside of Statistics Canada having access to extraordinarily sensitive market information before the official release time. There was no way I was ever going to agree with that."

Smith abruptly quit his position in September, accusing the federal government of hobbling his agency's independence by forcing it to participate in the Canada.ca project. Of particular concern to Smith was the mandate to see all content on Canada.ca, which would include Statistics Canada reports and research, published by employees at Services Canada, the department responsible for Canada.ca, and not Statistics Canada employees.

He also said the massive project had become a financial albatross for many departments.

"I am aware that this has turned into a money pit for the departments participating," he said.

The Canada.ca project has become the latest federal government technical initiative to face criticism.

The government's handling of the Phoenix pay system and the rollout of new email addresses and technical services by Shared Services Canada have also come under fire in recent months for having technical issues, being over budget and behind schedule.

Journal de Montréal
Infos entre de mauvaises mains
Monday, 19 December 2016
Byline: Sarah-Maude Lefebvre

Montréal - Des cas survenus par le passé montrent que la perte d'informations confidentielles dans les corps policiers ou les services de renseignements peut avoir des conséquences importantes.
Le 17 décembre 2015, pendant qu'il assiste à un party de Noël avec ses collègues, le commandant au SPVM Patrice Vilceus se fait dérober un sac dans son véhicule. Le sac en question contient une clé USB sur laquelle se trouvent des informations hautement confidentielles concernant une enquête impliquant les Hells Angels. Le voleur, qui semblait ignorer l'identité de la personne dont il avait volé les effets, a ensuite été épinglé et a écopé de sept mois de prison. Les objets volés ont été retrouvés, mais il n'y a eu aucune confirmation officielle quant à la clé USB.

INFORMATIONS DÉROBÉES AU PARTY DE NOËL

TUÉ À CAUSE D'UNE FUITE

Le 3 février 2000, Claude DeSerres, un individu lié aux Hells Angels devenu informateur formateur de la police, a été tué par le motard René Charlebois. Les Hells avaient deviné que DeSerres était devenu un informateur grâce au contenu d'un ordinateur portable volé à un enquêteur de la police provinciale de l'Ontario. Ce dernier avait laissé son ordinateur sans surveillance dans sa chambre d'hôtel alors qu'il épiait les motards en «congrès» à l'hôtel Delta de Sherbrooke. Lorsqu'il a été tué, Claude DeSerres portait sur lui un micro, ce qui a permis par la suite aux policiers d'identifier la voix de René Charlebois.

VOLÉE AU HOCKEY

Le 10 octobre 1999, un dossier hautement confidentiel est volé dans le véhicule d'une employée du SCRS, pendant qu'elle assistait à un match de hockey au Maple Leaf Garden de Toronto. Selon le rapport du SCRS à l'époque, «l'enquête policière révélera que les auteurs du vol, du menu fretin en manque de drogue, ont vraisemblablement jeté les documents classifiés, sans en avoir pris connaissance, dans une benne à déchets». Les documents ne seront jamais retrouvés et le SCRS a licencié l'employée.

Journal de Montréal
Perdus par les services secrets
Monday, 19 December 2016
Byline: Sarah-Maude Lefebvre

Ottawa - Six téléphones cellulaires et un ordinateur portable appartenant à des employés du Service canadien du renseignement de sécurité ont été volés ou perdus depuis quatre ans, a appris notre Bureau d'enquête. et le SCRS ne peut pas garantir que des informations sensibles ne sont pas tombées entre de mauvaises mains.
Le nombre d'appareils électroniques égarés par l'organisme chargé de lutter contre l'espionnage et le terrorisme au Canada peut sembler peu élevé à première vue.

Mais les conséquences peuvent être cruciales pour la sécurité nationale, affirme l'ancien agent du SCRS Michel Juneau-Katsuya.

«Ce n'est pas la quantité de téléphones perdus qui compte, c'est ce qu'il y a dedans. On peut n'en perdre qu'un et tout est perdu», illustre-t-il.

«Ça doit être pris au sérieux. Si quelqu'un avec de mauvaises intentions réussit à franchir le code d'accès d'un téléphone , il peut avoir accès à plusieurs informations importantes: des listes de contacts, des

numéros de téléphone, les endroits où le propriétaire du téléphone s'est rendu avec un GPS, etc. Ce n'est pas négligeable.»

SILENCE DU SCRS

Toutes nos questions au SCRS sont demeurées sans réponses. L'organisme fédéral a refusé de confirmer si des informations sensibles se trouvaient à l'intérieur des téléphones et de l'ordinateur qui ont été perdus ou volés à ses employés.

«Nous ne pouvons pas élaborer davantage. Ce que je peux dire, c'est que le SCRS fonctionne conformément à la Loi sur le SCRS, aux directives ministérielles et à un système solide de politiques et de procédures internes», a indiqué le porte-parole Tahera Mufti.

BIEN PROTÉGÉS ?

Selon Michel Juneau-Katsuya, on peut raisonnablement croire que les téléphones des employés du SCRS sont «bien protégés», voire que de l'information classifiée peut même être détruite à distance si c'est nécessaire.

«Mais il est difficile de déterminer la portée de ces incidents. Si des informations confidentielles ont été la cible d'un vol planifié, ce peut être préoccupant», dit-il.

«Les cellulaires peuvent contenir des mots de passe de bases de données et de serveurs. Le problème, c'est qu'on ne saura jamais si des données sensibles ont été perdues. Cela ferait paraître extrêmement mal le SCRS», souligne aussi le titulaire de la Chaire de recherche du Canada en surveillance et construction sociale du risque, Stéphane Leman -Langlois.

À une époque où chaque pays tente de collecter le plus de données possible sur son voisin, on ne peut risquer de «jouer avec le feu», rappelle le codirecteur de l'Observatoire sur la radicalisation et l'extrémisme violent, Stéphane Berthomet .

«On ne sait pas dans quelles mains sont tombés ces appareils. Est-ce que, par exemple, le cellulaire est simplement tombé dans la neige ou est-ce que quelqu'un avec de mauvaises intentions l'a piraté? Perdre ne serait-ce que deux appareils par année représente suffisamment de stress pour une organisation comme le SCRS pour qu'on s'en préoccupe .»

Vice News Canada
The best defense...
Saturday, 17 December 2016
Byline: Justin Ling

Ottawa - The Canadian Armed Forces is finally upping its game in the realm of cybersecurity -- bolstering its shields against nation-state actors like Russia and China, malicious hacker groups, and "insider threats" that may be looking to follow in Edward Snowden's footsteps.
In a pair of documents published Friday, the Canadian military is asking industry to submit ideas on how they can assess and respond to cyber threats in real- time.

Under the Defensive Cyber Operations Decision Project, which will ultimately culminate in a plan that will be submitted to the federal government, the Department of National Defense will be looking at capabilities that will allow the military to "operate effectively in cyberspace on government-authorized military missions, to support our federal partners in national cyber security efforts, and to work with international allies," according to a departmental spokesperson.

Cyber defense is obviously top-of mind right now, as the American intelligence community stands behind the fact that the results of the presidential election were directly affected by Russian hacking, and with revelations that Russia had targeted the Joint Chiefs of Staff.

Canada is no stranger to state-based hacking. A VICE News report revealed earlier this year that Canada faces 25 sophisticated attacks per day, likely launched by state- backed hackers.

"The future security environment will require a level of domestic integration among agencies that does not exist at the present time."

The request for information published Friday does ask industry to propose technology that can "hunt for APTs" -- referring to Advanced Persistent Threat hacks, which are often complex hacks organized by nation- state hackers.

The documents also ask for technology that can help identify "insider threats," seemingly an allusion to those with access to government systems who might be looking to either sell or publish sensitive data from within military systems.

The project will bring in software, hardware, and training that will help the military collect and store data about domestic and international cyber threats, run forensic analysis of that information, and to create predictive systems that can analyze and alert to possible incoming threats.

Those systems will largely boost the already-growing cyber operations centres run by the department.

"Cyber threats are increasing in both numbers and sophistication, and a growing number of state and non-state actors of concern have already developed and employed cyber capabilities that can be used for intrusive, disruptive or offensive purposes. Our key priorities are to continue to develop [Department of National Defense/Canadian Armed Forces] cyber capabilities and workforce," the spokesperson added.

The new cyber defense plan will be able to operate abroad, to ensure that foreign militaries or governments won't be able to access Canadian systems during battle. "The [Canadian Armed Forces] of the future must be a multi-role, combat capable force that can perform a broad range of tasks and operate in all engagement spaces (land, maritime, air, space, and cyber)," the documents read.

It's how the plan might work in Canada that is particularly interesting.

"Domestic (routine and contingency) operations might involve assisting civil authorities in responding to natural disasters, cyber-attacks, terrorist attacks, crises in urban centres, threats to critical infrastructure, risks to health and food systems, or Chemical, Biological Radiological or Nuclear (CBRN) attack," the document reads.

"Owing to the potential for an increase in domestic threats, [the Department of National Defense/Canadian Armed Forces] as a whole needs to become more integrated within the domestic response community -- in particular, the security and intelligence sectors. In particular, the future security environment will require a level of domestic integration among agencies that does not exist at the present time."

Canadian intelligence-watchers have, for years, noted an uptick in domestic activity amongst Canadian military intelligence units -- which, traditionally, do not run national intelligence-gathering. This journalist reported in 2014 that military counter-intelligence kept tabs on Indigenous protesters, perhaps countering their own mandate. More recently, the Ottawa Citizen reported that military intelligence conscripted the Communication Security Establishment to track a Canadian within the country.

The Communication Security Establishment, the signals intelligence agency that works hand-in- hand with the American NSA, does not appear to be covered by this cyber defense strategy. That agency does not have authority to do surveillance inside Canada, unless specifically mandated to by another department.

A guide to planned spending for the Department of National Defense says the Cyber Operations Decision Support Project is expected to cost between $50 million and $99 million.

Cover: Photo via Canadian Forces Combat Camera, DND

Global News
Canada's military too vulnerable to cyber attacks: documents
Saturday, 17 December 2016
Byline: Monique Scotti

Ottawa - The Department of National Defence and the Canadian Armed Forces are looking to improve their ability to defend against cyber attacks, with newly released documents suggesting the current system remains woefully inadequate.
DND/CAF published a request for "industry feedback" on Friday morning, stating that the Canadian military wants to develop a new system "that will enable a reliable, near-real-time analysis of its Information Technology Infrastructure (ITI) to detect and identify malicious activities and then provide decision aids and tools" to defend against those attacks.

The initiative has been dubbed the "Defensive Cyber Operations Decision Support Project" and it's expected to set taxpayers back between $50 and $99 million.

Friday's documents were released less than a month after the department's main webpage was hacked. Canadians trying to learn about career opportunities with the military at forces.ca instead found themselves staring at the landing page of the Chinese central government's official web portal.

Details of the upgrade plan made public on Friday describe the project as a "complex multi-year requirement" that is still in its infancy. The final delivery date is slated for 2024.

But the documents reveal that the sooner the department's current system for dealing with cyber threats can be replaced, the better. They acknowledge that "state and non-state adversaries are developing increasingly sophisticated cyber capabilities" that can target the Canadian military.

The sensors used to detect cyber attacks are "not sufficient," they go on to say, and when they do come across malicious attempts to compromise the department's computer systems, "analysts must manually piece the data together to understand the extent of the breach and its operational impacts."

On top of that, the current defence system lacks the ability to compare what the technicians are seeing to existing intelligence reports, or to other information that could help them decide how to respond.

The fundamental problem, according to the department, is that DND's cyber defences "mainly focused on yesterday's problem while combating today's adversaries."

Industry stakeholders will now have a chance to submit feedback on possible ways to bring the system into the modern era.

After that, the department will need to examine the feedback, then come up with a business case for approval by September 2017.

Global News has reached out to the department for additional information and comment.

Washington Post

How Russia overtook China as our biggest cyber-enemy
Sunday, 18 December 2016
Byline: James Lewis

Analysis: In June 2015, the U.S. government discovered something horrifying: The Office of Personnel Management had been hacked by China. The attackers had stolen the Social Security numbers, performance ratings and job assignments of millions of current and former federal employees.
It wasn't the first time the Chinese had been tied to security breaches in the government. They had gained access to the computers of the Federal Deposit Insurance Corp.'s top officials as well as sensitive data in government employees' security clearance files. The Chinese military was able to steal weapons designs, data on advanced technologies and insight into U.S. government policies. They had collected information about America's electrical power grid, gas lines and waterworks.

Headlines about China's attacks bordered on the hysterical. "Successful hacker attack could cripple U.S. infrastructure," NBC blared. "China hacks the world," the Christian Science Monitor declared. The National Interest called China's data theft a "national security threat."

Over the past year, though, China has largely faded from the conversation. It's not because its hackers have gone away. The Chinese continue to extract secrets from the U.S. government. But their efforts are, and have always been, far less scary than Russia's brazen new challenge in the information space. Unlike China, the Russians aren't using their cyberspies to steal business insights or gather information that officials can use in private negotiations with the United States. They're looking to disrupt elections in the United States and Europe, break NATO, and undermine democratic values - big strategic goals that President Vladimir Putin energetically pursues. Russia has become the biggest threat in cyberspace, and it will be very hard to defeat.

Both Russia and China have absconded with America's secrets for decades. China's efforts have been better known because Chinese hackers have gotten caught more. As the New York Times reported, they stole "designs for the F-35 fighter jet, corporate secrets for rolling steel, even the blueprints for gas pipelines that supply much of the United States." In 2008, they accessed the campaign servers of Barack Obama and John McCain, stealing internal position papers and communications, the Times said. Those documents were never leaked.

Russian hackers have used more sophisticated techniques and, as a result, have operated mostly under the radar, navigating their way into the networks of major agencies, including the Defense and State departments. They have also gained access to U.S. Central Command, the White House, energy companies and critical infrastructure around the country.

Today, China's cyberespionage efforts have become more refined. But they're still focused on gathering information as quietly as possible. China isn't looking to take down U.S. infrastructure, and its spies generally no longer steal secrets from foreign companies to help their own. President Xi Jinping has

professionalized and centralized cyberspying, and China is careful to avoid anything that could look like an attack.

The Russians are not. The country's aims are much more aggressive - and personal. Its leaders believe that the United States is trying to use the Internet (which the Kremlin calls a tool of the CIA) to remake the world in its own Western liberal image. Putin's henchman Dmitry Medvedev, Russia's prime minister, even claimed that Western social media is part of a plan for Arab Spring-style political unrest in his country, saying that "they have been preparing such a scenario for us, and now they will try even harder to implement it."

As a result, Russian hackers aren't just looking for information that could bolster their business efforts or improve their ability to negotiate with Washington. They're aggressively working to destabilize and destroy democracy. The Democratic National Committee hack, which has been tied to Russia, was only one of several high-profile incidents. The Russians allegedly hacked the German Bundestag. They broke into a leading French TV network (pretending to be the Islamic State) and took it offline. A power plant in Ukraine was hacked as a warning to Kiev. Russian hackers have been accused of planting false news to undercut a partnership between Sweden and NATO. European intelligence services say the Russians are more active and more dangerous than at any other time since the Cold War.

This is what Russia calls a "new generation of warfare," which uses hacking, leaks and nontraditional weapons such as RT, an English- language news site with a strident anti-American tone. Russia's government has hired hundreds of trolls to plant pro-Russian messages in the comment sections of Western media outlets, uses "chatbots" to flood social media with hostile comments, and, of course, leaks purloined emails through various organizations, including WikiLeaks. China doesn't do this.

This past week, Obama pledged to retaliate against Russian hackers, telling NPR that "we need to take action. And we will." But figuring out what comes next has been a struggle. We can't unleash a major U.S. Cyber Command operation without risking war. Some proposals put forward by experts are silly, such as leaking Putin's Botox injection schedule. Others are feckless, such trying to embarrass Putin by publicizing pictures of his girlfriends.

America needs a better strategy, one that's more assertive and nimble. And it can't be focused on Russia alone. Other opponents remain busy and dangerous. North Korea, Iran and China have all tested American cyberdefenses and found them wanting. A good cybersecurity strategy can't play whack-a-mole. We need an approach that convinces opponents it's dangerous to attack the United States, and if they do, there will be consequences. The response to North Korea's Sony hack shows that opponents' behavior can be changed: After the United States imposed retaliatory sanctions, the number of attacks decreased significantly. We can reshape cyber-risk if we take action. We must.

New York Times

Obama Confronts Complexity of Using a Mighty Cyber arsenal Against Russia
Sunday, 18 December 2016
Byline: David E. Sanger

Washington - Obama assembled a menu of options to respond to Russia's hacking during the election, ranging from the obvious -- exposing President Vladimir V. Putin's financial ties to oligarchs -- to the innovative, including manipulating the computer code that Russia uses in designing its cyberweapons. But while Mr. Obama vowed on Friday to "send a clear message to Russia" as both punishment and deterrent, some of the options were rejected as ineffective, others as too risky. If the choices had been better, one of the aides involved in the debate noted recently, the president would have acted by now.

In his last weeks in office that Situation Room debate has confronted a naturally cautious president with a complex calculus that President-elect Donald J. Trump will soon inherit: how to use the world's most powerful cyberarsenal at a moment when the United States, as the election showed, remains highly vulnerable.

"Is there something we can do to them, that they would see, they would realize 98 percent that we did it, but that wouldn't be so obvious that they would then have to respond for their own honor?" David H. Petraeus, the former director of the Central Intelligence Agency under Mr. Obama, asked on Friday, at a conference here sponsored by Harvard's Belfer Center for Science and International Affairs. "The question is how subtle do you want it, how damaging do you want it, how do you try to end it here rather than just ratchet it up?"

The idea of exposing Mr. Putin's links to oligarchs was set aside after some aides argued that it would not come as a shock to Russians. Still, there are proposals to cut off leaders in Mr. Putin's inner circle from their hidden bank accounts in Europe and Asia. There is an option to use sanctions under a year-old executive order to ban international travel for senior officials in the G.R.U., the Russian military intelligence unit that American spy agencies say stole emails from the Democratic National Committee and Hillary Clinton's campaign chairman, then doled them out to WikiLeaks, betting that media outlets eager for insider details would amplify them, doing the Kremlin's work for it.

The National Security Agency and its military cousin, the United States Cyber Command, which is responsible for computer-network warfare, have worked up other ideas, officials said, though some have been rejected by the Pentagon.

Those plans could deploy the world-class arsenal of cyberweapons assembled at a cost of billions of dollars during Mr. Obama's tenure to expose or neutralize some of the hacking tools favored by Russia's spies -- the digital equivalent of a pre-emptive strike. But the selection of targets by Americans and the accuracy of that retaliation could also expose software "implants" that the United States has patiently inserted and nurtured in Russian networks, in case of future cyberconflicts.

And the revelation in August about some of the N.S.A.'s own tools for breaking into foreign computer networks has raised the possibility that the Russians are already inside American networks and are sending a warning that they can respond in kind.

All of this has led Mr. Obama to ask how the Russians might escalate the confrontation, and whether the United States in the end may have more to lose than Russia.

"He doesn't have great options," said Michael D. McFaul, formerly one of Mr. Obama's top national security aides and then his ambassador to Moscow.

Mr. Obama is the president who, in his first year in office, reached for some of the most sophisticated cyberweapons on earth to blow up parts of Iran's nuclear facilities. Now, at the end of his presidency, he has run headlong into a different challenge in the cyberwarfare arena.

The president has reached two conclusions, senior officials report: The only thing worse than not using a weapon is using it ineffectively. And if he does choose to retaliate, he has insisted on maintaining what is known as "escalation dominance," the ability to assure you can end a conflict on your terms.

Mr. Obama hinted as much at his news conference on Friday, as he was set to leave for his annual Hawaii vacation, his last as president.

"Our goal continues to be to send a clear message to Russia or others not to do this to us because we can do stuff to you," he said. "But it is also important to us to do that in a thoughtful, methodical way. Some of it, we will do publicly. Some of it we will do in a way that they know, but not everybody will."

He rejected calls for a big, symbolic show of power, dismissing the idea that if the United States "thumped our chests about a bunch of stuff, that somehow that would potentially spook the Russians."

The goal, Mr. Obama said, was to come up with a response "that increases costs for them for behavior like this in the future but does not create problems for us."

There is not much new in tampering with elections, except for the technical sophistication of the tools. For all the outrage voiced by Democrats and Republicans this week about the Russian action -- with the notable exception of Mr. Trump, who has dismissed the intelligence findings as politically motivated -- it is worth remembering that trying to manipulate elections is a well-honed American art form.

The C.I.A. got its start trying to influence the outcome of Italy's elections in 1948, as the author Tim Weiner documented in his book "Legacy of Ashes," in an effort to keep Communists from taking power. Five years later, the C.I.A. engineered a coup against Mohammad Mossadegh, Iran's democratically elected leader, when the United States and Britain installed the Shah.

"The military coup that overthrew Mosaddeq and his National Front cabinet was carried out under CIA direction as an act of US foreign policy, conceived and approved at the highest levels of government," the agency concluded in one of its own reports, declassified around the 60th anniversary of those events, which were engineered in large part by Kermit Roosevelt Jr., a grandson of President Theodore Roosevelt.

There were similar interferences over the years in Guatemala, Chile and even in Japan, hailed as a model of post-World War II democracy, where the Liberal Democratic Party owes its early grip on power in the 1950s and 1960s to millions of dollars in covert C.I.A. support.

The only differences from what happened this year is that the effort was directed at the United States, and that it was cyberenabled, giving Moscow a tool to amplify its efforts through the echo chamber of social media and news organizations that quoted from the leaked emails.

"What has changed is that this was using cyberspace for advancing a political objective," said Admiral James A. Winnefeld Jr., who served as vice chairman of the Joint Chiefs of Staff until he retired last year.

Cybertechniques, he said, have amplified an old form of "political warfare, and the issue is not whether it successfully influenced the election -- but the fact that they did it."

Over the past few months, an administration that prided itself on its work on cyberoffense and cyberdefense has come face-to-face with a hard reality: When it came to the 2016 election, an economically failing Russia, dismissed by Mr. Obama on Friday for its inability to grow or to innovate, exploited giant holes in the American system.

Mr. Obama conceded that he first heard about the attack on the Democratic National Committee "early last summer," or nine months after the F.B.I. first alerted low-level D.N.C. officials about what happened. That now appears to be critical lost time.

If Mr. Obama had confronted the Russians immediately, in public or in the kind of private warning he said he delivered to Mr. Putin only three months ago during a meeting in China, the United States might have derailed the hacking campaign before it harvested and revealed thousands of emails.

But the election hacking also raised questions about whether the American fixation on a "cyber Pearl Harbor" -- a devastating attack on the power grid, cellphone network, financial system or computer-controlled gas pipelines -- overlooked a more obvious vulnerability.

As a detailed account in The New York Times last Wednesday revealed, the D.N.C. had virtually no protections for its electronic systems, and Mrs. Clinton's campaign chairman, John D. Podesta, had failed to sign up for the "two-factor authentication" on his Gmail account. Doing so probably would have foiled what Mr. Obama called a fairly primitive attack.

Now the question facing Mr. Obama is how public a retaliation to execute.

The president laid out a case on Friday for acting with subtlety, so as not to start a tit-for-tat conflict.

But as Joseph Nye, a strategist on so-called soft power, noted on Friday, "The reason to make some of this public is not just to deter the Russians, it is to deter others as well," in future elections.

It is possible, said Mr. McFaul, the former ambassador to Russia, that Mr. Obama's most lasting contribution may be to get the details of the Russian hack declassified and to publish a report he has instructed the intelligence community to assemble before he leaves office.

"Given that Obama only has a few more weeks in office, I think he needs to focus his remaining time on attribution -- that is declassification of intelligence so that there is no ambiguity about the Russian actions," Mr. McFaul said.

That "is completely within his powers," he added, and would spur more congressional investigations regardless of the stance taken by Mr. Trump on the hack.

Mr. Obama's comments on Friday have led Democrats to demand further action. Representative Adam Schiff of California, the ranking Democrat on the House Intelligence Committee, said the response should mix "additional economic sanctions along with our allies, and clandestine means of exacting a cost on the Russians for their flagrant meddling in our election."

"I have little confidence," he continued, "that the incoming president will take the actions necessary to make the Russians pay any price for the most consequential 'active measures' campaign against us in history."

Huffington Post
Yahoo Lawsuit: Canadian Customers Want To Sue In $50-Million Class Action
Saturday, 17 December 2016

Toronto - Yahoo is now facing a proposed class action on behalf of Canadians whose personal information may have been stolen, according to a notice of action filed Friday.
The $50-million claim would take in Canadians whose user account information was stolen or whose email accounts were accessed in recent years.

According to the notice, the representative plaintiff, Natalia Karasik, of Barrie, Ont., received a letter from Yahoo on Thursday informing her that her information was part of a hack of its servers _ in 2013.

Karasik, who could not immediately be reached, was unaware of the breach until she received the letter, the notice of action filed in Ontario Superior Court states. She has used email to chat about a wide range of personal information, including financial and health information, according to the notice.

"She's been using her Yahoo email account as her exclusive email system," lawyer Ted Charney said in an interview. "So, essentially, she's at risk for someone having access to all of her emails and everything she's done with her email account for a couple of years."

Yahoo, based in Sunnyvale, Calif., did not immediately respond to a request for comment.

Hackers used 'forged cookie files'

In September, the company sent a mass email to users to inform them that their account information had been stolen from its network in a cyberattack in late 2014. The information included email addresses, telephone numbers, dates of birth, passwords and security questions. The company said at least 500 million user accounts were affected.

he notice of action also asserts that documents filed with the Securities and Exchange Commission in November show Yahoo knew about the 2014 breach shortly after it occurred "contrary to its representations to its users."

Toronto-based Rogers Communications, whose customers' email accounts are "powered" by Yahoo, said it had "every reason" to believe some of them would have been affected.

"We have been in contact with Yahoo and understand they are taking steps to notify people potentially impacted," spokesman Rogers Aaron Lazarus said in an email. "We encourage people to regularly change and set strong passwords."

Company facing similar action in U.S.

The unproven claim -- which has yet to be certified as a class action or tested in any court -- alleges Yahoo breached its contract with users, invaded their privacy, and unjustly enriched itself at their expense. The claim also seeks $10 million in punitive damages.

Charney said it was not necessary to prove under Canadian law that anyone actually suffered damages as a result of the hacks. Besides leaning on contract law, he noted relatively recent recognition of the wrongdoing of "intrusion upon seclusion," which presumes damages if a privacy breach is proven.

While a proposed suit has previously been launched on behalf of users in British Columbia, Yahoo's terms of use for Canada requires proceedings to take place in Ontario. The company also faces similar action over the hacks in the United States.

Yahoo is the parent company of Toronto-based Yahoo Canada, which is also named in the action. CEO Marissa Mayer has previously said Yahoo had a total of one billion users. While it's not known how many Canadians might have been affected, Charney estimated as many as eight-million Canadians may have used one of Yahoo's services.

iPolitics.ca
One quarter of Canadian online traffic vulnerable to NSA sweeps: researchers
Saturday, 17 December 2016
Byline: Amanda Connolly

Ottawa - A large amount of Canadian internet traffic is being routed through the United States, leaving it vulnerable to collection and probing by the National Security Agency.
And most Canadians have no idea of how exposed they are to American data sweeps, say the researchers behind a new tool that aims to show Canadians what path their internet traffic takes to connect to the websites they want to visit.

In a new online project launched Thursday, researchers from the University of Toronto and York University have partnered with Open Media to create a tool to show the paths Canadians' internet data take when they access websites or send online communications.

While past estimates have suggested roughly 90 per cent of Canadian internet traffic is routed through the United States -- particularly in cases where a Canadian visits an American or foreign website -- the new data gathered so far by the researchers build on that and suggest that even when both the origin and destination of the traffic are in Canada, there's still a one-in-four chance it goes through the U.S.

"I think most Canadians would be really surprised to learn that quite so much of our internet traffic, even our domestic Canada-to-Canada traffic, actually ends up being routed through the U.S.," said David Christopher, spokesperson for Open Media.

"Canada's lack in sufficient internet exchange points within our borders is really a big reason why so much of our traffic does travel through the U.S. I think nowadays a lot of people think of the internet as almost like a cloud and I think a lot of people don't put a lot of thought into what happens when we visit a website on the other side of the country."

To get a user to a website, internet service providers (ISPs) must connect to internet exchange points -- physical hubs that connect all of the most important cables that connect internet access points -- like your computer -- with the end destination, such as the iPolitics homepage.

There are nine internet exchange points located in Canada: one each in Vancouver, Edmonton, Calgary, Winnipeg, Toronto, Ottawa, Montreal, Halifax and Waterloo, Ont.

(Picture an extension cord connecting your laptop to the power bar across the room: You need some intermediary to help you access the power bar, but you could use one, two or even three extension cords to help you get there.)

"You get to there and then you can connect to other networks that have also reached that," said Andrew Clement, professor emeritus at the University of Toronto and coordinator of the school's Information Policy Research Program. "It's like a big power bar in the sense that everybody just plugs in there rather than making all of these arrangements with individual carriers."

But Canadian internet traffic can also be routed through intermediary exchange points in the U.S., rather than directly through the hubs in major Canadian cities.

Sometimes this is because the U.S. exchange points are cheaper and more developed: Think of routing through the U.S. as being like taking the Trans Canada Highway instead of a winding, two-lane road to drive across country.

Sometimes it can also be because larger internet service providers don't want to directly transport traffic from smaller services piggy-packing on their expensive network infrastructure.

"That's about the pricing policies and the lack of government regulatory intervention," Clement said.

The problem lies in the fact that the use of such "boomerang" routes means Canadian internet traffic loses its protections under Canadian privacy law -- and instead becomes subject to the Patriot Act while it passes through U.S. exchange points. That exposes the Canadian traffic to the National Security Agency's broader powers to intercept and probe both the metadata and content of the traffic.

An example: In the course of setting a time for an interview, iPolitics and Christopher exchanged a number of emails between the iPolitics office in Ottawa and his office in Vancouver. While even internet traffic within cities can be routed through the U.S., the likelihood of traffic crossing south of the border increases between websites or servers that are distant from one another.

"That chance increases when it comes to long-haul traffic, so with you being in Ottawa and me being in Vancouver I think there's a bigger chance than 25 per cent that the emails we've been exchanging have been routing through the U.S. because Canada just lacks sufficient long-haul background capacity in our networks," Christopher said.

And when Canadians access websites based outside North America, the traffic almost always will be routed through the U.S. because the primary seafloor cables -- connecting Asia and North America, for example -- make landfall in the U.S.

While the Canadian Internet Registration Authority, the service that registers domain names for websites hosted in Canada, actively encourages the use of Canadian internet exchange points, there is no regulation requiring internet service providers to do so.

Clement said that if every internet service provider with access to the Canadian exchange points used them, it would help to keep more traffic within Canada.

He pointed to one example where he and his students traced the route their internet data took when they accessed the Ontario Student Assistance Program website from his office just down the street at the University of Toronto.

"The route that that data takes is from Toronto to New York and Chicago, where [provincial government carrier] Telus then connects it back to the provincial government," Clement said. "We've observed this for years and this pattern is fairly reliable."

But that doesn't mean it should stay that way, he said, pointing to the coming inauguration of President-elect Donald Trump as a reason Canadians should be concerned about their internet traffic, including the content of online communications, being routed through the United States.

"Going to the United States exposes it to NSA surveillance and now I think with Trump and his government, it's going to be even worse," Clement said. "It's an unnecessary loss of legal and constitutional protection."

The project itself doesn't advocate for any particular course of action but rather is set up as a platform to allow people to trace the routes their own internet traffic takes so they can better understand the issue.

But that doesn't mean those behind it don't have clear ideas on how to solve the problem.

"Fundamentally it's about education, so people understand how this can happen, and further about the risks to privacy," said Clement, pointing to the need for a baseline level of understanding before Canadians and policy makers can move to find solutions.

"There are a number of things that can be fixed but the easiest thing is to reduce that exposure to US surveillance. Make it easier and require that connection within Canada."

London Times
Tyrie demands clarity on cybercrime
Monday, 19 December 2016
Byline: Marcus Leroux

London - The chairman of the Treasury select committee has written to Britain's cybersecurity chief to highlight "serious concerns" over the reliance of financial regulators on intelligence agencies to stop bank hacks.
In the wake of last month's hacking attack on Tesco Bank, Andrew Tyrie has written to Ciaran Martin, chief executive of GCHQ's National Cyber Security Centre, to ask him to consider a "single point of responsibility" for cybercrime in financial services.

He writes: "The committee has serious concerns [over] the opaque lines of accountability between the relevant authorities, particularly the regulators on the one hand and intelligence agencies on the other, and a very high degree of reliance on information from the intelligence community."

Mr Tyrie argues that it is essential the intelligence community gives regulators the technical and practical support they need to do their job. "It is for consideration whether a single point of responsibility for cyber risk in the financial services sector is now required."

New York Times
Senators Push to Widen Inquiry on Russian Meddling in Election
Monday, 19 December 2016
Byline: Nicholas Fandos

Washington - Pressure mounted on Sunday for a broader congressional investigation of Russian cyberattacks aimed at influencing the American election, even as a top aide to President-elect Donald J. Trump said there was no conclusive evidence of foreign interference.
The effort was being led by a bipartisan group of senators, including John McCain, Republican of Arizona, and Chuck Schumer of New York, the Senate Democratic leader, who called on Sunday for the creation of a Senate select committee on cyberactivity to take the investigative lead on Capitol Hill.

"Recent reports of Russian interference in our election should alarm every American," the senators wrote on Sunday in a letter to Senator Mitch McConnell, Republican of Kentucky and the majority leader, who has said a select committee is not necessary. "Cybersecurity is the ultimate cross-jurisdictional challenge, and we must take a comprehensive approach to meet this challenge effectively."

The developments served to deepen the fissures between high-ranking lawmakers of both parties who see American intelligence reports implicating Russia as the basis for additional inquiries and Mr. Trump, who continues to reject the conclusions of those reports.

But the developments also put new strain on Mr. McConnell. He now faces calls from Mr. McCain and Lindsey Graham, two Senate Republicans considered well versed on national security issues, to form a select committee. If he were to reject that appeal, he would be subject to criticism that he was trying to avoid a spotlight on an issue that senators in both parties believe is worthy of more focused scrutiny.

Mr. McConnell said last week that while he respects the intelligence agencies' conclusions, the Senate Intelligence Committee is "more than capable of conducting a complete review" itself. He also acknowledged that Mr. McCain could conduct an investigation on the Armed Services Committee, an option that remains open should Mr. McConnell decide against a select committee.

Those divisions, coming as the Electoral College prepares to meet on Monday to ratify Mr. Trump's election and the president-elect completes his cabinet choices, all but ensured that the issue would cloud the first months of Mr. Trump's presidency, when he will be asking Congress to approve an aggressive legislative agenda.

Several permanent congressional committees have already been tasked with examining various aspects of the Russian interference, which has been largely accepted as fact by most members of Congress.

But in their letter on Sunday, the lawmakers argued the issue was too important and complicated for an existing committee to take on properly.

"We share your respect for, and deference to, the regular order of the Senate, and we recognize that this is an extraordinary request," the senators wrote to Mr. McConnell. "However, we believe it is justified by the extraordinary scope and scale of the cyber problem."

In addition to undertaking a "comprehensive investigation of Russian interference," the senators recommended that such a committee also develop "comprehensive recommendations and, as necessary, new legislation to modernize our nation's laws, governmental organization, and related practices to meet this challenge."

Select committees, which are typically created to examine a particular issue for a limited time, are rarely formed. The most prominent recent example is the House Select Committee on the attacks in 2012 on the American diplomatic compound in Benghazi, Libya, an inquiry that Democrats have denounced as unduly partisan.

Speaker Paul D. Ryan said last week that the House Intelligence Committee would continue its own examination of Russian hacking.

Mr. Schumer said in a news conference on Sunday that they intended to avoid such charges of partisanship.

"We don't want it to just be finger pointing at one person or another," Mr. Schumer said. "We want to find out what the Russians are doing to our political system and what other foreign governments might do to our political system. And then figure out a way to stop it."

A spokesman for Mr. McConnell, David Popp, referred to Mr. McConnell's earlier comments and said the majority leader would be reviewing the latest letter.

The letter was also signed by Mr. Graham, Republican of South Carolina, and Senator Jack Reed, Democrat of Rhode Island, two members of the Senate Armed Services Committee that Mr. McCain leads. It follows a signed statement from the lawmakers, released last week, warning that any congressional investigation into the hacks "cannot become a partisan issue."

Mr. Trump, for his part, has sought to paint the intelligence community's conclusions about the matter as just that -- a partisan attack against him. He said last week that the reports were "just another excuse" by Democrats frustrated with the election results that might be used to try to undermine his victory.

Asked on CBS's "Face the Nation" on Sunday what information Mr. Trump had received that led him to reject intelligence assessments, Kellyanne Conway, one of Mr. Trump's top advisers, insisted that the reports about the hacking were groundless.

"Where is the evidence?" Ms. Conway asked, turning the question around. "Why, when C.I.A. officials were invited to a House intelligence briefing last week, did they refuse to go?"

Robert M. Gates, the former defense secretary under President Obama and President George W. Bush who has offered counsel to Mr. Trump, speculated on NBC's "Meet the Press" that the president-elect "felt the way this information came out through newspaper stories and so on was somehow intended to delegitimize his victory in the election and that he's reacting to that rather than 'the facts on the ground,' as it were."

But Mr. Gates also said the Russian hacking was aimed at discrediting the American electoral process.

"Whether or not it was intended to help one candidate or another, I don't know," said Mr. Gates, who also served as C.I.A. director under President George Bush. "But I think it clearly was aimed at discrediting our elections, and I think it was aimed certainly at weakening Mrs. Clinton."

Mr. Obama, in a news conference on Friday, vowed that the United States would respond to the attack. He said that he was still weighing a mix of covert and public actions to retaliate before he leaves office. And lawmakers from both parties have proposed new sanctions to punish Russia.

Speaking Sunday on CNN's "State of the Union," Mr. McCain sought to add urgency to the matter.

"There's no doubt they were interfering and no doubt that it was cyberattacks," he said of the Russians. "The question now is how much and what damage and what should the United States of America do? And so far, we have been totally paralyzed."

Mr. McCain said that he had faith that "reality is going to intercede at one point or another" on Mr. Trump, suggesting that the president-elect might come to agree about Russian influence.

Asked on CBS about Mr. Obama's pledge of retaliation, Ms. Conway said Mr. Trump "respects" Mr. Obama's right to respond as he sees fit for the remainder of his presidency. But, she added, that "doesn't mean that new President Trump will agree with it and continue it."

"It does seem to be a political response at this point because it seems like the president is under pressure from Team Hillary, who can't accept the election results," she said.

Press Trust of India
Indian Security Experts Are Confident About Their Cyber Defense
Monday, 19 December 2016

New Delhi - Indian security professionals are confident, despite a global decline in assurance that cyber defenses are meeting expectations, reveals the new 2017 Global Cybersecurity Assurance Report Card released by Tenable Network Security.
According to the survey, India earned the highest overall global score in cybersecurity confidence, with 84 percent (B). India debuted in the annual survey this year, beating out last year's leader in overall score, the United States, which fell two points to second place with 78 percent (C+). The overall global cybersecurity confidence, on the other hand, fell six points over 2016 to earn a 70 percent (C-).

The 2017 Global Cybersecurity Assurance Report Card solicited insights from 700 security practitioners in nine countries and across seven industry verticals to calculate a global index score reflecting overall confidence that the world's cyber defenses are meeting expectations. While the 2017 Global Risk Assessment Index dropped by 12 percent, India stayed ahead of the curve with an above average rating of 73 percent (C).

"India's high cybersecurity confidence is certainly a positive trend, especially when the global outlook is gloomy," said Manoj Taskar, Country Manager India & SAARC, Tenable Network Security. "These scores are a testament to the increased focus Indian enterprises have towards security as they embrace the digital economy. There has been a conscious effort from various stakeholders in the industry to empower the security ecosystem of the country, and we are now seeing the results."

Despite leading in overall grades, Indian security professionals struggle with assessing risks in new and emerging technologies. This year's data indicate that the growing adoption of containerization platforms and DevOps environments poses new challenges, with respondents grading themselves a 68 percent (D+) in their ability to assess risk in both categories.

Globally, security practitioners continue to face challenges in securing cloud and BYOD environments, while web application security emerged as a bigger risk this year than in 2016, dropping 18 points to 62 percent (D-).

"This year's research reveals that Indian CISOs must prepare themselves and their organizations for the new security challenges of the modern workplace," said Taskar. "Across industry verticals and around the world, organizations are struggling to assess IT security risks brought on by new technologies. Leveraging data and insights from the Global Cybersecurity Assurance Report Card, IT teams can improve their security program effectiveness and better prepare themselves for continued technological innovation."

Face the Nation (CBS)
Henry Kissinger says "I hope we're doing some hacking" in Russia
Sunday, 18 December 2016
Byline: Rena Flores

Washington - Former Secretary of State Henry Kissinger, responding to intelligence reports that Russia directed hacks to interfere with the U.S. election, is hoping that the American government is retaliating against the Kremlin with cyberattacks of its own.
"I don't doubt that the Russians are hacking us," Kissinger told CBS' "Face the Nation" in an interview that aired Sunday. "And I hope we're doing some hacking there."

"Everybody has a hacking capability. And probably every intelligence service is hacking in the territory of other countries," he said. "But who exactly does what? That would be a very sensitive piece of information. But it's very difficult to communicate about it. Because nobody wants to admit the scope of what they're doing."

Kissinger, a secretary of state under President Richard Nixon, also offered candid thoughts about Russian President Vladimir Putin, calling him a "character out of Dostoyevsky," referencing the Russian novelist who wrote "Crime and Punishment."

"He is a man with a great sense of connection, an inward connection, to Russian history as he sees it," Kissinger remarked of Putin, who intelligence sources have said gave direct approval for the recent hacks in the U.S. related to the 2016 presidential election.

"He is a cold calculator of the Russian national interest, as he conceives it, and which he believes, probably correctly, has some very unique features," Kissinger said.

"For him, the question of Russian identity is very crucial. Because as a result of the collapse of communism, Russia has lost about 300 years of its history," the former secretary of state continued.

"And so that the question of 'What is Russia?' looms very large in their mind. And that's a problem we have never had."

Kissinger, who declined to endorse either party's candidate in the general election, also commented on President-elect Donald Trump, giving a cautiously optimistic assessment of the businessman's potential on the international stage.

"Donald Trump is a phenomenon that foreign countries haven't seen. So it is a shocking experience to them that he came in to office," Kissinger said. But the president-elect, he acknowledged, presented "extraordinary opportunity" because of it.

"I believe he has the possibility of going down in history as a very considerable president," he continued. "Because every country now has two things to consider. One, their perception that the previous president, or the outgoing president, basically withdrew America from international politics, so that they had to make their own assessments of their necessities."

"And secondly, that here is a new president who's asking a lot of unfamiliar questions," he said. "And because of the combination of the partial vacuum and the new questions, one could imagine that something remarkable and new emerges out of it. I'm not saying it will. I'm saying it's an extraordinary opportunity."

Kissinger added that Mr. Trump's instincts -- which he said were a "different form of analysis as my more academic one" -- have led to him raising issues that were of great import.

"And if they're addressed properly, could lead to good - great results," Kissinger said.

Asked to weigh in with his general impression of the president-elect, Kissinger said at first he had believed the support for Mr. Trump was a "transitory phenomenon."

But, he said, "I give him huge credit for having analyzed an aspect of the American situation, develop a strategy, carry it out against his leadership of his own party, and prevailing. Now, his challenge is to apply that same skill to the international situation."

The Guardian (London)
GCHQ asked to step up action against cyber-attack threat to financial services
Monday, 19 December 2016
Byline: Jill Treanor

London - More action may be needed to protect the financial services industry from a devastating cyber-attack, the head of the Treasure select committee has suggested.

Andrew Tyrie MP wrote to Ciaran Martin, head of the new cybersecurity centre of UK surveillance agency GCHQ, saying the lines of responsibility and accountability for reducing cyber-threats are opaque.

Tyrie's letter to Martin, who is leading the Cheltenham-based National Cyber Security Centre (NCSC), uses last month's incident at Tesco Bank to illustrate the vulnerabilities of the financial system.

In November, the banking arm of supermarket chain Tesco admitted that £2.5m had been stolen from 9,000 accounts in an incident which raised fresh concerns about the methods used by financial services firms to detect cyber- attacks.

Two-thirds of all major UK companies - not just financial services firms - have reported security breaches in the last year. The Bank of England has also listed the threat of cyber-attacks as one of the major risks facing the financial services industry.

In his letter Tyrie, a Conservative MP, outlines the responsibility for cyber-threats as being shared between the Bank's Prudential Regulation Authority (PRA), the Financial Conduct Authority and GCHQ. In turn, the regulatory arms are responsible to the Treasury, while GCHQ reports through the foreign secretary.

In light of this, Tyrie said: "It is for consideration whether a single point of responsibility for cyber risk in the financial services sector, with full ownership of - and accountability for - financial cyber- threats is now required. It may be necessary to create a line of accountability to the Treasury for financial cybercrime."

Tyrie also asks Martin for clarity on the objectives of NCSC, which was set up two months ago to take charge of the UK's defences against cyber-offences.

"Legacy systems, human error and deliberate attack have resulted in unacceptable interruptions to vital banking services and weakened the public's confidence in the banking system as a whole. The recent attack on Tesco Bank is only the latest example of criminals exploiting vulnerabilities in the banking industry's IT systems," said Tyrie.

A spokesman for the NCSC said: "We have received this letter and there will be a government response in the New Year."

The parliamentary committee has been asking questions about the need for a clearer command structure to tackle cyber-attacks during its evidence sessions. Last week, Sam Woods, the Bank's deputy governor who runs PRA, was asked his views on the need for a single point of contact.

Woods replied it was important to know which body was in charge of each incident rather than have the same point of contact.

"It is essential that the intelligence community gives the regulators the technical and practical support they need to do their job. This means making sure that financial cybercrime has a high priority, and is not subordinate to other work," said Tyrie.

"Certainly, as millions of customers are exposed to the risks of cybercrime, a higher level of scrutiny and accountability for existing arrangements is needed," he added.

This Week (ABC)
DNC Chair Contradicts Obama: Russian Hackers Came After Us 'Until End of Election'
Sunday, 18 December 2016
Byline: Nicki Rossoll

Washington - Democratic National Committee Chair Donna Brazile said Russian hackers persisted in trying to break into the organization's computers "daily, hourly" until after the election -- contradicting President Obama's assertion that the hacking stopped in September after he warned Russian President Vladimir Putin to "cut it out."
"They came after us absolutely every day until the end of the election. They tried to hack into our system repeatedly," Brazile told ABC's Martha Raddatz in an exclusive interview on "This Week" Sunday.

Obama said at a press conference Friday that Russia's "tampering" with the U.S. election process stopped in early September after he spoke to Putin at an international conference.

"In early September when I saw president Putin in China, I felt that the most effective way to ensure that that didn't happen was to talk to him directly and tell him to cut it out, and there were going to be serious consequences if he didn't," Obama said. "In fact we did not see further tampering of the election process. But the leaks through Wikileaks had already occurred."

Brazile said she supports Obama's call for a thorough investigation of the hacking but she lamented the administration's failure to protect the party and its infrastructure.

"We were attacked by a foreign adversary, and I think it's the responsibility of the government to help individual citizens -- as well as institutions, nonprofits, corporations -- to protect us," she said.

While critical of President Obama, Brazile also slammed President-elect Donald Trump, accusing him of using information obtained in the hack to "sow division" during the campaign.

"The emails were weaponized," the Democratic chair said of the thousands of emails that were hacked from the DNC and Hillary Clinton campaign staff and then released publicly. "Donald Trump used this information in ways to also sow division. I was very disappointed in his repeated usage some of the stolen information. He used it as if he received daily talking points."

But Brazile refused to blame Russia's interference in the election for Democrats' loss.

"I'm not going to sugarcoat what happened on Election Day. We, the Democratic Party have a lot of things that we have to do. Donald Trump cracked the blue wall," she said, referring to the once reliably Democratic-voting states Michigan, Pennsylvania, and Wisconsin. "He cracked the blue wall. We had a blue wall; we should've maintained it."

Brazile, who took over as chair months after the cyberattacks had begun, also accepted that the DNC was partly responsible for the hack after leaving itself vulnerable to this kind of intrusion.

"There's no question; I took full responsibility ... I spent the entire month of July, all of August, apologizing because of the leaks," she said, while highlighting the "appropriate steps" the party took to prevent another attack afterwards.

She added that although she is outraged by the hacking, the country needs to look to the future to ensure it doesn't happen again.

"I'm still outraged by it," Brazile said. "But I want to make sure that this never happens again because this country deserves to have the kind of cybersecurity experts involved to make sure that our homeland is protected."

In particular, she sent a letter to Congress on Sunday on behalf of the DNC, asking for an independent, bipartisan commission to study the entire episode.

The Daily Beast
How to Really Punish Russia for Hacking
Saturday, 17 December 2016
Byline: James Lewis
Section: Analysis

Analysis: After much hand-wringing, the Obama administration admitted that the Russian government interfered with the presidential election. (It was not a 400-pound hacker, unless that hacker lives in Moscow.) It's true that people often question attribution, but the critics were wrong on Sony and they are wrong now. It was the Russians.
What the U.S. worries about when it comes to responding to cyberattacks, once attribution has been determined, is the risk of escalating conflict or damaging other important equities.

One reason for Obama's delay in addressing the hacking was a desire not to appear to be interfering in the election--which seemed like a safe calculation back when the White House thought Clinton was certain to win. There was also the pious hope--don't laugh--for a peace deal with Moscow on Syria.

The Obama administration's response options were ready in August. So why only act now? The most likely reason is domestic politics (and maybe a final realization of the futility of negotiating over Syria). The goal is to hem in the new administration on Russia. If President Obama imposes sanctions, President Trump will have to take action to lift them, complicating his relations with the Hill and the nominating process. This muddles what should be a straightforward story, since one essential lesson for cybersecurity is that unpunished acts are seen as a green light by an attacker.

The Russians calculated that they could manipulate the U.S. without punishment. So far, they have been right. They have succeeded beyond their greatest hopes. There is no reason for them to stop of their own accord and the likelihood of further Russian action is high if the U.S. does not take action in response.

On a secondary note, the Germans, French, and British have found that the Russians are doing to their upcoming elections what they did to ours. We need to do something to help our friends.

The administration is considering an "all tools of government" approach. The agencies involved are CIA, NSA, Cyber Command, Treasury, and the Department of Justice. The most likely public action will be to use the cybersecurity sanctions announced in April 2015, accompanied by some kind of covert response involving either interference with Russian attack servers or, perhaps, leaks of documents detailing Russian corruption.

Any response raises important issues. First, the U.S. and Russia agreed sever

al years ago to create a hotline for cybercrises and to consult before acting. Russian sources imply the U.S. has used neither. Any call would be pro- forma, as the Russians will deny everything, but it sets a bad precedent if we create a crisis management structure and then do not use it in the first test.

Second, the U.S. has struggled for a decade with how to respond to cyberattacks. If an attack produces an effect equivalent to a kinetic weapon, destroying physical infrastructure or harming American citizens, the nature of the response is clear. But when the attacks do not involve force (or its cyberequivalent) as is the case with espionage or the kind of information warfare the Russians are using now, how to respond is unclear.

There are several reasons for this. In discussing how to respond to Russia, people ask when we will unleash Cyber Command without noting that using Cyber Command for offensive action would likely be disproportional and counterproductive. We are not going to go to war with Russia over their blatant intrusions. The Russians know this and it gives them a kind of freedom. The only thing that has changed is that now, the Russians will want to avoid damaging their relationship with the incoming administration. That gives Obama room to be a little more aggressive, if he wants.

Third, international law and the Laws of Armed Conflict, which the U.S. tries to follow, define when force can be used in self-defense and require that it be proportional to the attack. International law and state practice do not define espionage, crime, or disinformation as actions that justify the use of force in response.

For example, some years ago a U.S. general threated that a cyberattack might provoke a cruise missile in response. This threat had no effect because it was not believable. A cruise missile is not proportional to most cyberattacks. Sending a cruise missile in response to a cyberattack risks the opponent sending a missile back. The threat was aimed at China, which ignored it and kept on spying. Faced with widespread PLA hacking, it took the U.S. a decade to define a realistic and proportional response, settling on indictment and the threat of sanctions.

Finally, the U.S. is constrained by its Constitution. The Russians clearly committed a crime when they stole private emails, and we may not like WikiLeaks publishing those emails, but the publication raises difficult First Amendment issues about freedom of speech and the right to publish, rights that protect WikiLeaks as well as The New York Times. The Russians know this complicates our decision-making and take advantage of it.

One question about a response to Russian hacking is how we will control the risk of escalation without being ineffective. Unplugging a few servers will not end Russian action, but unplugging many servers may lead to broader conflict. When facing an opponent who is nimbler in decision-making, less bound by law, and more willing to take risks, the chance of escalation is greater.

So retaliation probably means a lawful response not involving force and that does not unduly risk escalating the conflict. This response cannot be that old favorite of amateur cyberstrategists, name-and-shame. Vladimir Putin cannot be shamed. He believes his actions are justified against an aggressive U.S. that is implacably hostile to Russia. While some kind of counterattack by Cyber Command is tempting, any retaliation must have political effect, and in Russia, that means going after relationships and money.

It is important to lay down a marker with the Russians. They have gone too far and need to be checked. The U.S. needs to navigate a narrow and difficult path between inaction and escalation. We can start by recognizing that this is cyberconflict, not the kind of cyberconflict we planned for--no cyber Pearl Harbor or cyber 9/11--but a conflict nonetheless. Anything we do should reinforce (or at least not undercut) the long-term goal to create a framework of agreements for stability in cyberspace. The U.S. needs a new strategy for dealing with Russia and its new style of conflict that uses hybrid warfare, including a mix of cyberaction, threats, disinformation, and corruption. It is too late for this administration to define that new Russia strategy, but it can lay the groundwork for it with the actions it takes now. This sounds like a long list of requirements, but none of these are impossible or preclude action.

New York Times
Russia's Hacks Followed Years of Paranoia Toward Hillary Clinton

Saturday, 17 December 2016
Byline: Max Fisher

Washington - Russia's unprecedented intervention in the United States election came amid more than United States-Russia tension and Donald J. Trump's praise of Vladimir V. Putin, the Russian president. It also coincided with a growing belief, in Moscow, that Russia faced an imminent threat in Hillary Clinton's candidacy.
Mrs. Clinton is viewed in Moscow as innately hostile to Russia. Widely held conspiracy theories portray her as seeking to foment unrest that will return Russia to the chaos and depression of the 1990s. Even many government technocrats view her with suspicion that at times verges on paranoia.

She referred to these views at an event on Thursday, telling donors that Mr. Putin's "personal beef" with her had driven Russia's intervention in the American election.

Mark Galeotti, a Russia expert at the Institute of International Relations, based in Prague, said the Kremlin was consumed by something more urgent than petty revenge: self-preservation.

"It's not just they didn't like Clinton, but they actually thought that she represented a threat," he said, describing Russia's actions as a matter of "policy, not pique."

No one factor can fully explain Russia's decision to hack and pass on Democratic emails, analysts say, and intelligence agencies appear divided on assessing Russian motives. But, in Moscow, fear of Mrs. Clinton has loomed as large or larger than any warmth for Mr. Trump.

Mr. Putin accused Mrs. Clinton of instigating protests against him in late 2011.

"She set the tone for some actors in our country and gave them a signal," he said, reflecting a widespread view in Moscow that Mrs. Clinton, then secretary of state, had sought to topple Russia's government.

Mr. Putin returned to the presidency a few months later, appearing to believe that the United States had engineered the Middle East's descent into chaos and was targeting his country to be next. He put Mrs. Clinton at the center of these plots.

Mrs. Clinton is indeed more hawkish than other Democrats, including toward Russia. In 2008, while a senator, she mocked President George W. Bush's claim that he had looked into Mr. Putin's soul.

"I could have told him -- he was a K.G.B. agent. By definition, he doesn't have a soul," Mrs. Clinton joked. The line is still remembered in Moscow.

But the Kremlin's views of Mrs. Clinton go beyond defining her as hawkish. They are also layered with a pre-existing Russian belief that promoting American democracy is a ploy to unseat unfriendly

governments, that the United States remains bent on Russia's destabilization or even destruction, and that there is an American hand behind nearly every Russian misfortune.

These suspicions go back decades. But, since Mrs. Clinton's tenure as secretary of state, popular telling has cast her as the culprit responsible for America's misdeeds and, therefore, Russia's setbacks.

In the summer of 2015, when Russian hacking groups first infiltrated Democratic National Committee servers, I happened to be reporting in Moscow. The American name on everyone's lips was not Mr. Trump's, who was already praising Mr. Putin, but rather Mrs. Clinton's.

Fyodor Lukyanov, a prominent Russian foreign policy commentator, told me at the time that there was a widespread view in his country's government that Mrs. Clinton, as president, would take "a very hostile approach" toward Russia.

Consensus in Moscow, Mr. Lukyanov said, was that "Hillary is the worst option of any president, maybe worse than any Republican."

It was conventional wisdom, he added, that Mrs. Clinton considered her husband's efforts to reform Russia in the 1990s an unfinished project, and that she would seek to finish it by encouraging grass-roots efforts that would culminate with regime change.

This summer, when Russian hacking groups began releasing Democratic emails through third parties such as WikiLeaks, many Americans suspected an effort to help Mr. Trump, who had promised to realign the United States with Russia.

But Mr. Galeotti, the Russian expert, said that, in all his time in Moscow, "I didn't speak to anyone who thought a Trump presidency was possible."

Rather, conversation there followed the same polls that dominated the discussion in America, and which all projected a landslide for Mrs. Clinton.

Even as Mr. Putin deemed Mr. Trump "colorful" and suggested they might get along, officials in Moscow "were absolutely working from the assumption that Clinton was going to get it," Mr. Galeotti said.

This belief may have informed Russia's actions during the campaign, which a number of analysts still suspect were aimed at weakening, rather then preventing, Mrs. Clinton's presumedly imminent presidency.

But if Moscow does gain an ally in Mr. Trump, it will lose a foil in Mrs. Clinton -- something that has been politically useful for Mr. Putin as his country's economy has sank and its isolation deepened.

New York Times
Obama Says He Told Putin: 'Cut It Out' on Hacking
Saturday, 17 December 2016
Byline: Mark Landler and David E Sanger

Washington - President Obama said for the first time on Friday that he had held back before Election Day from retaliating against Russia for meddling in the presidential race for fear of inciting further hacking "that could hamper vote counting." But he said he was weighing a mix of public and covert actions against the Russians in his last 34 days in office, actions that would increase "the costs for them." Mr. Obama said he was committed to sending the Kremlin a message that "we can do stuff to you," but without setting off an escalating cyberconflict.

"There have been folks out there who suggest somehow if we went out there and made big announcements and thumped our chests about a bunch of stuff, that somehow it would potentially spook the Russians," he said. "I think it doesn't read the thought process in Russia very well."

The president did not reveal what steps he was considering if he decided to retaliate against the Russians and suggested that some of the options, if they were carried out, could remain secret. "Some of it we will do in a way that they will know, but not everybody will," he said.

Mr. Obama made his comments at an annual end-of-year news conference, one tinged with melancholy at the impending end of his presidency, foreboding about the changes that could follow President-elect Donald J. Trump into office next month, and uneasiness about the role Russia played in the political earthquake that has resulted from his election.

The president spoke hours after Hillary Clinton, addressing campaign donors in New York, bluntly accused President Vladimir V. Putin of Russia of orchestrating the hacks against her campaign and the Democratic National Committee "to undermine our democracy," as part of a "personal beef against me."

Mr. Obama declined to place the blame for the hacking so squarely on Mr. Putin, though he noted, "Not much happens in Russia without Vladimir Putin." Mr. Obama also sought to diminish the specter of Russian influence over the American political process, saying Russia was a smaller, weaker country that "doesn't produce anything that anybody wants to buy, except oil and gas and arms."

Still, the president was clearly wrestling with what he said the hacking affair and the reaction to it revealed about the state of American politics. Citing a recent poll that showed more than a third of Trump voters saying they approved of Mr. Putin -- "Ronald Reagan would roll over in his grave," Mr. Obama said -- the president appealed to Americans not to allow partisan hatred and feuds to blind them to manipulation by foreign powers.

"Unless that changes," Mr. Obama said, "we're going to continue to be vulnerable to foreign influence because we've lost track of what it is that we're about and what we stand for."

Mr. Obama offered a long list of accomplishments that he said marked his eight years in office. But his victory lap has been attenuated by the messy aftermath of Mr. Trump's defeat of Mrs. Clinton, which has raised questions about Mr. Obama's pre-election response to the hacking, ignited a nasty squabble between Mr. Trump and the nation's intelligence agencies, and left a residue of suspicion over the vote itself.

The president continued to defend his cautious approach to reports of hacking -- an approach that has come under criticism from Democrats after it emerged last week that the intelligence agencies had concluded Russia was trying to help Mr. Trump win the election.

"We were playing this thing straight -- we weren't trying to advantage one side or the other," Mr. Obama said. "Imagine if we had done the opposite. It would have become one more political scrum."

The president, however, is likely to face further questions after his C.I.A. director, John O. Brennan, issued a statement Friday disputing reports of a rift between the intelligence agencies and the C.I.A. over Russia's motives in hacking the D.N.C. and handing over emails to WikiLeaks, which released them in the weeks leading up to the vote.

In his statement, first reported by The Washington Post, Mr. Brennan said he had met with the director of the F.B.I., James B. Comey, and the director of national intelligence, James R. Clapper, and "there is strong consensus among us on the scope, nature and intent of Russian interference in our presidential election."

That statement will also challenge Mr. Trump, who has seized on reports of an interagency squabble to undermine the credibility of the hacking findings. He has criticized the C.I.A. analysis, saying it was supplied by the same agency that provided erroneous intelligence about Saddam Hussein's weapons of mass destruction before the Iraq War.

Mr. Obama held out hope that when Mr. Trump takes office, he would take a more sober approach. He said he had had "cordial" conversations with his successor, and that Mr. Trump had listened to his suggestions about "maintaining the effectiveness, integrity, cohesion of our office, our various democratic institutions," though he was not specific.

The president also defended the F.B.I., which has come under fierce criticism from Mrs. Clinton and her aides because of Mr. Comey's 11th-hour announcement that the bureau was considering reopening its investigation of Mrs. Clinton's email, which she has said cost her the election.

Mrs. Clinton's remarks on Thursday underscored longstanding differences she has had with her former boss in how the United States should view Mr. Putin.

"This is not just an attack on me and my campaign," she told donors. "This is an attack against our country."

For his part, Mr. Obama also made a startling admission as he described how his administration had reacted to the Russian hack: He said it was not until the "beginning of the summer" that the White House was "alerted to the possibility that the D.N.C. has been hacked."

That was nine months after an F.B.I. agent had first contacted the Democratic National Committee with evidence that a major, government-linked hacking group was inside the committee's networks, raising the question of why it took so long for that news to reach the president.

Mr. Obama made it clear that he went out of his way to play down the news, because "in this hyperpartisan atmosphere" he did not think he or anyone else at the White House could talk about it without risking to appear to be acting on behalf of Mrs. Clinton.

But the unintended result, as some of Obama aides concede, was that the Russians faced very little resistance. Not until September, when Mr. Obama pulled Mr. Putin aside at a Group of 20 meeting in Hanghzhou, China, was the Russian leader given a warning directly from the United States. Mr. Obama said he told him "to cut it out, there were going to be serious consequences if he did not."

The president made it sound like that worked, saying "we did not see further tampering of the election process." But the leaks of D.N.C. emails, and those of John D. Podesta, the Clinton campaign manager, continued, because they were already in the hands of WikiLeaks, which doled them out to an eager news media until the last days of the campaign.

The Russian government's motives were hardly a mystery, Mr. Obama said, "because you guys wrote about it every day, every single leak about every little juicy piece of political gossip, including John Podesta's risotto recipe."

National Post
Digitally secure, but private
Thursday, 22 December 2016
Byline: Adam Belsher
Section: oped

Historically, liberal democratic societies have tried to balance security challenges and reconcile the limits on civil liberties required to maintain the peace. In the 1950s, in an effort to curb the growing number of drunk drivers, Canadians became subject to breath tests and subsequently random spot checks without a reasonable doubt of guilt.
Over 25 years ago, we accepted the collection of DNA samples of suspects in major crimes such as murder and rape. This personally intrusive investigative tool, which could be argued as self-incriminating, was deemed an acceptable limit on civil liberties, because it would lead to truths in some of the most horrendous crimes against humanity.

This debate has reemerged in the contemporary, digital age. However, the nuance seems to have been lost.

Police agencies, both in Canada and abroad, have looked for leadership from their governments since investigations into major crimes such as human-trafficking, terrorism, murder and the sexual abuse of children have been enabled by digital devices or the internet. The magnitude of the challenge was highlighted by the Royal Canadian Mounted Police's unprecedented looks into the challenges they face in securing Canadians in the digital age.

Law enforcement agencies largely have the legal framework they need to investigate digital devices that enable crimes. However, the increasing levels of encryption that now exist on commonly used smartphones and applications will render these authorities borderline toothless.

Here in Canada, privacy commissioners from around the country came together recently to caution lawmakers against legislating against encryption. Their argument is that any weakening of encryption would result in both risks to our civil liberties and unintended security challenges as we weaken the security architecture of commonly used platforms.

The civil liberties argument against providing police the powers to collect and share the private data of citizens is not misguided. Security agencies around the world were alleged to have violated civil liberties in the name of national security by former U.S. National Security Agency contractor, Edward Snowden. This has created a sense of distrust by citizens and frustration on the part of police and security agencies who are struggling to perform their societal role in the digital age.

The polarizing nature of this debate is not helpful as it leaves citizens trying to reconcile what is presented as an intractable dichotomy: They either accept that their civil liberties will be trampled in exchange for their security. Or they allow for what is presented as absolute guarantees of their privacy,

through modern technologies, while placing their security at risk, given the global and virtual nature of crime today.

The reality is that there is no absolute right to privacy in a liberal-democratic society. We cede portions of our civil liberties for our own protection and to uphold a common good.

We would not tolerate an individual building impenetrable physical walls around a home where it was known children were being sexually exploited. However, we are inadvertently doing this as we accept virtually impenetrable digital encryption on our smartphones and in social media we commonly use, and that are also used by those creating and disseminating child sexual abuse images and videos. This is an area of crime that has exploded both in Canada and around the world in the digital age.

This is not to suggest police agencies should expect citizens simply accept constant surveillance or backdoors to encryption. There is need for a reset on this debate, one which places a commitment to securing citizens in the context of our digital age and protecting civil liberties as equal pillars.

Technology itself is not to blame for the security and civil liberties challenges we face since many of online products we use were not purpose-built to secure vulnerable populations from internet-enabled crimes. Nor were the tools used by police agencies developed to respect civil liberties.

Technological innovation at its best enables the world we wish to build for ourselves and future generations. If we truly want our security and our civil liberties to be respected, we must call for a rethink of laws governing these issues and invest in the technologies that our law enforcement and security agencies require to reconcile this dichotomy.

Adam Belsher is CEO of Magnet Forensics, a Waterloo-based technology company that develops tools for law enforcement and national security agencies.

London Times
European ruling raises risk of terror, says ex-MI5 chief
Thursday, 22 December 2016
Byline: Sean O'Neill

London - Weakening surveillance laws in response to a European court ruling that they are excessive would leave Britain at greater risk of a terrorist attack, former spy chiefs have warned.
The Court of Justice of the European Union said yesterday that Britain's retention of bulk data on calls, emails and text messages for a year "exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society".

The case concerned emergency legislation from 2014 but the ruling opens the door to further challenges to the powers, and others contained in the new Investigatory Powers Act.

The Home Office said that it was disappointed by the ruling and would argue against it in the British courts. It is studying the implications but former intelligence chiefs and police leaders cautioned against any dilution of their ability to track and thwart terrorists and serious criminals.

Lord Evans of Weardale, the former head of MI5, said that the impact of the ruling on intelligence agencies may be limited because the EU has no remit over national security issues.

The ruling could, however, damage the police's ability to access communications data and hamper the work they do alongside MI5.

"Anything that impacts on their operational effectiveness would be a concern and could leave us more vulnerable to attacks such as those we have seen only too frequently in recent months elsewhere in Europe, including that in Berlin," Lord Evans said.

Sir David Omand, the former head of GCHQ, said that British data- retention powers were stronger than those available to our European allies. "My expectation is that we have a better picture of what is going on in the UK and the links between suspects and jihadists in Syria than the German authorities," he told BBC Radio 4.

David Davis, the secretary for exiting the European Union, was a party to the action against the so-called snooper's charter before withdrawing when he joined the cabinet.

The court ruled that mass retention of every citizen's communications data for access by the authorities was "likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance". It added that the only justification for retaining data was "the objective of fighting serious crime" and that could not be made out when every electronic communication was logged and retained.

Security agencies said that communications data had been used in every MI5 anti-terrorism operation for the past decade and in 95 per cent of serious crime prosecutions.

Tom Watson, Labour's deputy leader and a party in the case, said the judgment showed it was "counterproductive to rush new laws through parliament without proper scrutiny".

Liberty, the human rights group, said the ruling "upholds the rights of ordinary British people". The case will return to the Court of Appeal.

Q&A

What exactly is communications data? The who, what, where, when, how -- but not the content -- of calls and electronic messages. Logs of when suspects were in contact with each other and for how long are core evidence in many criminal cases.

What are the rules? The government requires the data to be retained for 12 months so it can be accessed by police or spy agencies. In Germany data is retained for ten weeks.

Is everyone's data held? Yes. Opponents of the power say it means everyone is treated like a suspect. They want tighter rules on who can access the data and the reasons for accessing it.

If you haven't done anything wrong, why worry? Because the police have a habit of abusing these powers -- eg, hoovering up information from journalists' phones after leaks to the press.

What law was challenged? The arguments pertain to the Investigatory Powers Act, which recently received royal assent.

Brexit is coming, why do we care what Europe thinks? The government is anxious not to antagonise the EU before negotiations

What happens now? The Court of Appeal has asked the EU for clarification and the matter will return to the British courts for further arguments.

CBS News
Russian hacks into Ukraine power grids a sign of things to come for U.S.?
Thursday, 22 December 2016
Byline: Holly Williams

New York - Russian hacking to influence the election has dominated the news. But CBS News has also noticed a hacking attack that could be a future means to the U.S. Last weekend, parts of the Ukrainian capitol Kiev went dark. It appears Russia has figured out how to crash a power grid with a click. Last December, a similar attack occurred when nearly a quarter of a million people lost power in the Ivano-Frankivsk region of Ukraine when it was targeted by a suspected Russian attack.

Vasyl Pemchuk is the electric control center manager, and said that when hackers took over their computers, all his workers could do was film it with their cell phones.

"It was illogical and chaotic," he said. "It seemed like something in a Hollywood movie."

The hackers sent emails with infected attachments to power company employees, stealing their login credentials and then taking control of the grid's systems to cut the circuit breakers at nearly 60 substations.

The suspected motive for the attack is the war in eastern Ukraine, where Russian-backed separatists are fighting against Ukrainian government forces.

But hackers could launch a similar attack in the U.S.

"We can't just look at the Ukraine attack and go 'oh we're safe against that attack,'" said Rob Lee, a former cyberwarfare operations officer in the U.S. military, investigated the Ukraine attack.

"Even if we just lose a portion, right? If we have New York City or Washington D.C. go down for a day, two days, a week, what does life look like at that point?" he said.

He said that some U.S. electric utilities have weaker security than Ukraine, and the malicious software the hackers used has already been detected in the U.S.

"It's very concerning that these same actors using similar capabilities and tradecraft are preparing and are getting access to these business networks, getting access to portions of the power grid," he said.

In Ukraine, they restarted the power in just hours. But an attack in the U.S. could leave people without electricity for days, or even weeks, according to experts. Because, ironically, America's advanced, automated grid would be much harder to fix.

Washington Post
Cybersecurity firm finds evidence that Russian military unit was behind DNC hack
Thursday, 22 December 2016
Byline: Ellen Nakashima

Washington - A cybersecurity firm has uncovered strong proof of the tie between the group that hacked the Democratic National Committee and Russia's military intelligence arm -- the primary agency behind the Kremlin's interference in the 2016 election.
The firm CrowdStrike linked malware used in the DNC intrusion to malware used to hack and track an Android phone app used by the Ukrainian army in its battle against pro- Russia separatists in eastern Ukraine from late 2014 through 2016.

While CrowdStrike, which was hired by the DNC to investigate the intrusions and whose findings are described in a new report, had always suspected that one of the two hacker groups that struck the DNC was the GRU, Russia's military intelligence agency, it had only medium confidence.

Now, said CrowdStrike co-founder Dmitri Alperovitch, "we have high confidence" it was a unit of the GRU. CrowdStrike had dubbed that unit "Fancy Bear."

The FBI, which has been investigating Russia's hacks of political, government, academic and other organizations for several years, privately has concluded the same. But the bureau has not publicly drawn the link to the GRU.

CrowdStrike's fingering of the GRU helps to deepen the public's understanding of how different arms of the Russian government are carrying out malicious and deeply troubling cyber acts in the United States. The director of national intelligence and the homeland security secretary in October publicly blamed the Russian government for interfering in the U.S. election, including through hacks of political organizations and targeting of state election systems.

After the election, the CIA and other intelligence agencies concluded that one of Russia's aims was to help President-elect Donald Trump win the election through a campaign of "active measures" or influence operations that included the hacking and dumping of emails onto public websites.

The GRU, evidently, was key to this operation.

"The GRU is used for both tactical intelligence collection in the battlefield in support of Russian military operations and also strategic active measures or psychological warfare overseas," said Alperovitch, who is an expert on Russia and a senior fellow at the Atlantic Council. "The fact that they would be tracking and helping the Russian military kill Ukrainian army personnel in eastern Ukraine and also intervening in the U.S. election is quite chilling."

CrowdStrike found that a variant of the Fancy Bear malware that was used to penetrate the DNC's network in April 2016 was also used to hack an Android app developed by the Ukrainian army to help artillery troops more efficiently train their antiquated howitzers on targets.

The Ukrainian army's D-30 towed howitzers, which date to the Soviet era, typically take a number of minutes to position based on hand-drawn targeting data. With the Android app, positioning takes 15 seconds, CrowdStrike found.

The Fancy Bear crew evidently hacked the app, allowing the GRU to use the phone's GPS coordinates to track the Ukrainian troops' position. In that way, the Russian military could then target the Ukrainian army with artillery and other weaponry.

Ukrainian brigades operating in eastern Ukraine were on the front lines of the conflict with Russian-backed separatist forces during the early stages of the conflict in late 2014, CrowdStrike noted. By late 2014, Russian forces in the region numbered about 10,000. The Android app was useful in helping the Russian troops locate Ukrainian artillery positions.

According to the International Institute for Strategic Studies, Ukrainian artillery forces lost more than 50 percent of their weapons in the two years of conflict and more than 80 percent of their D-30 howitzers, the highest percentage of loss of any artillery piece in their arsenal, the report stated.

The app was not available in the Android app store and was distributed only through the social media page of its developer, who is a Ukrainian artillery officer, Yaroslav Sherstuk, according to CrowdStrike. It could be activated only after the developer was contacted and a code was sent to the individual downloading the application.

The other group that hacked the DNC also works for Russian intelligence, CrowdStrike reported earlier this year. But the firm is not sure if it is the more internally focused FSB, or the foreign intelligence arm, the SVR. Both grew out of the KGB.

That group, which CrowdStrike has called Cozy Bear, has not apparently been deployed in the influence operation, Alperovitch said. Rather, it is focused on traditional espionage. It is the group that is believed to have hacked unclassified networks of the State Department, White House and the Joint Chiefs of Staff.

Reuters
Yahoo email scan shows U.S. spy push to recast constitutional privacy
Wednesday, 21 December 2016
Byline: Joseph Menn

San Francisco - Yahoo Inc's secret scanning of customer emails at the behest of a U.S. spy agency is part of a growing push by officials to loosen constitutional protections Americans have against arbitrary governmental searches, according to legal documents and people briefed on closed court hearings.
The order on Yahoo from the secret Foreign Intelligence Surveillance Court (FISC) last year resulted from the government's drive to change decades of interpretation of the U.S. Constitution's Fourth Amendment right of people to be secure against "unreasonable searches and seizures," intelligence officials and others familiar with the strategy told Reuters.

The unifying idea, they said, is to move the focus of U.S. courts away from what makes something a distinct search and toward what is "reasonable" overall.

The basis of the argument for change is that people are making much more digital data available about themselves to businesses, and that data can contain clues that would lead to authorities disrupting attacks in the United States or on U.S. interests abroad.

While it might technically count as a search if an automated program trawls through all the data, the thinking goes, there is no unreasonable harm unless a human being looks at the result of that search and orders more intrusive measures or an arrest, which even then could be reasonable.

Civil liberties groups and some other legal experts said the attempt to expand the ability of law enforcement agencies and intelligence services to sift through vast amounts of online data, in some

cases without a court order, was in conflict with the Fourth Amendment because many innocent messages are included in the initial sweep.

"A lot of it is unrecognizable from a Fourth Amendment perspective," said Orin Kerr, a former federal prosecutor and Georgetown University Law School expert on surveillance. "It's not where the traditional Fourth Amendment law is."

But the general counsel of the Office of the Director of National Intelligence (ODNI), Robert Litt, said in an interview with Reuters on Tuesday that the legal interpretation needed to be adjusted because of technological changes.

"Computerized scanning of communications in the same way that your email service provider scans looking for viruses - that should not be considered a search requiring a warrant for Fourth Amendment purposes," said Litt. He said he is leaving his post on Dec. 31 as the end of President Barack Obama's administration nears.

DIGITAL SIGNATURE

Reuters was unable to determine what data, if any, was handed over by Yahoo after its live email search. The search was first reported by Reuters on Oct. 4. Yahoo and the National Security Agency (NSA) declined to explain the basis for the order.

The surveillance court, whose members are appointed by U.S. Supreme Court Chief Justice John Roberts, oversees and approves the domestic pursuit of intelligence about foreign powers. While details of the Yahoo search are classified, people familiar with the matter have told Reuters it was aimed at isolating a digital signature for a single person or small team working for a foreign government frequently at odds with America.

The ODNI is expected to disclose as soon as next month an estimated number of Americans whose electronic communications have been caught up in online surveillance programs intended for foreigners, U.S. lawmakers said.

The ODNI's expected disclosure is unlikely to cover such orders as the one to Yahoo but would encompass those under a different surveillance authority called section 702. That section allows the operation of two internet search programs, Prism and "upstream" collection, that were revealed by former NSA contractor Edward Snowden more than three years ago. Prism gathers the messaging data of targets from Alphabet Inc's Google, Facebook, Microsoft, Apple among others.

Upstream surveillance allows the NSA to copy web traffic to search data for certain terms called "selectors," such as email addresses, that are contained in the body of messages. ODNI's Litt said ordinary words are not used as selectors.

The Fourth Amendment applies to the search and seizure of electronic devices as much as ordinary papers. Wiretaps and other surveillance in the internet age are now subject to litigation across the United States. But in the FISC, with rare exceptions, the judges hear only from the executive branch.

Their rulings have been appealed only three times, each time going to a review board. Only the government is permitted to appeal from there, and so far it has never felt the need.

PUBLIC LEGAL CHALLENGES

The FISC's reasoning, though, is heading into public courts. The 9th U.S. Circuit Court of Appeals on Dec. 5 cited FISC precedents in rejecting an appeal of an Oregon man who was convicted of plotting to bomb a Christmas tree lighting ceremony after his emails were collected in another investigation.

Groups such as the American Civil Liberties Union and the Electronic Frontier Foundation are fighting the expansion of legalized surveillance in Congress and in courts.

On Dec. 8, the ACLU argued in the 4th U.S. Circuit Court of Appeals that a lawsuit by Wikipedia's parent group against the NSA should not have been dismissed by a lower court, which ruled that the nonprofit could not show it had been snooped on and that the government could keep details of the program secret.

The concerns of civil libertarians and others have been heightened by President-elect Donald Trump's nomination of conservative Representative Mike Pompeo of Kansas to be director of the CIA. Pompeo, writing in the Wall Street Journal in January, advocated expanding bulk collection of telephone calling records in pursuit of Islamic State and its sympathizers who could plan attacks on Americans. Pompeo said the records could be combined with "publicly available financial and lifestyle information into a comprehensive, searchable database."

Yahoo's search went far beyond what would be required to monitor a single email account. The company agreed to create and then conceal a special program on its email servers that would check all correspondence for a specific string of bits.

Trawling for selectors is known as "about" searching, when content is collected because it is about something of interest rather than because it was sent or received by an established target. It is frequently used by the NSA in its bulk upstream collection of international telecom traffic.

The Privacy and Civil Liberties Oversight Board, an appointed panel established by Congress as part of its post-9/11 expansion of intelligence authority, reported in 2014 that "about" searches "push the program close to the line of constitutional reasonableness."

A glimpse of the new legal arguments came in a FISC proceeding last year held to review NSA and FBI annual surveillance targets and four sets of procedures for limiting the spread of information about Americans.

Judge Thomas Hogan appointed Amy Jeffress, an attorney at Arnold and Porter and a former national security prosecutor, to weigh in, the first time that court had asked an outside privacy expert for advice before making a decision.

Jeffress argued each search aimed at an American should be tested against the Fourth Amendment, while prosecutors said that only overall searching practice had to be evaluated for "reasonableness." Hogan agreed with the government, ruling that even though the Fourth Amendment was all but waived in the initial data gathering because foreigners were the targets, the voluminous data incidentally gathered on Americans could also be used to investigate drug deals or robberies.

"While they are targeting foreign intelligence information, they are collecting broader information, and there needs to be strong protections for how that information is used apart from national security," Jeffress told Reuters.

ODNI's Litt wrote in a February Yale Law Review article that the new approach was appropriate, in part because so much personal data is willingly shared by consumers with technology companies. Litt advocated for courts to evaluate "reasonableness" by looking at the entirety of the government's activity, including the degree of transparency.

Litt told Reuters that he did not mean, however, that the same techniques in "about" searches should be pushed toward the more targeted searches at email providers such as Yahoo.

Although speaking generally, he said: "My own personal approach to this is you should trade off broader collection authority for stricter use authority," so that more is taken in but less is acted upon.

This position strikes some academics and participants in the process as a remarkable departure from what the highest legal authority in the land was thinking just two years ago.

That was when the Supreme Court's Roberts wrote for a majority in declaring that mobile phones usually could not be searched without warrants.

After prosecutors said they had protocols in place to protect phone privacy, Roberts wrote: "Probably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols."

With little evidence that the Supreme Court agrees with the surveillance court, it remains possible it would reverse the trend. But a case would first need to make its way up there.

Agence France-Presse
China rights website founder held over 'state secrets': Amnesty
Thursday, 22 December 2016
Byline: Staff reporter

Beijing - The founder of one of China's few websites dedicated to reporting human rights abuses has been formally arrested for "leaking state secrets", Amnesty International said Thursday -- the latest blow in a broad crackdown on activists.
Huang Qi ran the website "64 Tianwang", named in part after the bloody June 4, 1989 crackdown on Tiananmen Square protestors, for nearly two decades.

Its headlines -- "Village Officials Stab Campaigner", "Gangsters Detain Protestor" -- are rarely seen in ordinary Chinese media, and the content is blocked on the mainland.

The site was awarded the Reporters Without Borders (RSF)-TV5 Monde Press Freedom Prize in early November. Twelve years ago, he received RSF's "Cyber-Dissident Prize."

Just weeks after receiving the most recent prize, Huang was detained by police in his hometown of Chengdu, the capital of the southwestern province of Sichuan, according to Amnesty -- his third detention this year.

Last Friday, his family received official notice that he had been formally arrested for leaking state secrets to overseas entities, the campaign group said.

It remained unclear whether he had access to a lawyer, Amnesty China researcher Patrick Poon told AFP, stating that Huang was "at risk of torture and other mistreatment".

"He may have been targeted because of the international attention he and his website received" from the RSF prize, Poon said.

Huang's arrest might also be intended as a warning to websites chronicling grassroots activism in advance of a controversial new law set to impose restrictions on foreign NGOs operating in China, which will come into force in January.

The law gives police wide-ranging powers over overseas charities and bans them from recruiting members or raising funds in the country.

"I'm quite worried that the government is trying to send a signal to organisations that they believe to have foreign links," said Poon, noting that authorities had detained Liu Feiyue, founder of the Civil Rights and Livelihood Watch website, around the same time as Huang.

President Xi Jinping has overseen a wide-ranging clampdown on civil society since assuming power in 2012.

But Huang's struggles to continue his work date even further back.

In 2000 he was jailed for five years, the first ever Chinese "cyber-dissident" to be imprisoned for online activism.

He was imprisoned again for a further three years in 2009 for reporting on low-quality school buildings that collapsed in a massive earthquake the previous year in Sichuan which claimed 87,000 lives.

He had been physically abused while in jail, Huang told AFP during an interview last year, but stated that he nevertheless felt that authorities now appreciated his coverage, as the exposure of injustices committed by local officials dovetailed with an anti-corruption campaign also launched under Xi.

"The top levels of government no longer think of me as a threat," he said at the time. "They even see me as useful, because I expose a lot of cases which they don't know about."

Jerusalem Post
Government likely to okay bill to ban terrorism content from Internet
Thursday, 22 December 2016
Byline: Yonah Jeremy Bob

Jerusalem - Justice Minister Ayelet Shaked and Public Security Minister Gilad Erdan announced on Wednesday that they expect their much- anticipated bill for removing terrorism content from the Internet and social media to be approved by the government on Sunday.
The bill would empower courts to order social media providers such as Facebook, Google, YouTube and Twitter to remove content which is, in itself, criminal and constitutes a danger to personal, public or state security.

Shaked said that the effect of such posts "going viral, where what one person types in one place creates a genuine storm which can even lead to killings in another place, without any measure of control or law enforcement capability, is grossly unreasonable and must end."

Erdan added: "Despite the incitement leading to terrorism, Facebook and social media companies do not respond to all of the complaints by police for removal of posts of incitement." The bill would give vast powers to the state that it currently lacks in standard proceedings.

That could allow it to seek court orders for removal of content without notifying the social media platform, introduce classified evidence, or bring evidence which would not normally be admissible.

In justifying these unusual powers, the ministers have emphasized the uniqueness of the problem and that content removal is not a criminal proceeding, in which removing standard defenses is a more serious action that can end with a jail sentence.

Additionally, if someone is convicted of a crime for such a post, the conditions for its removal can be assumed to have been proven. On June 22, the ministers had instructed their respective ministries and the police to draft the legislation.

The expected principles of the bill were advertised on June 22. They would start with the state issuing a warning letter to the Internet domain name and social media providers which indirectly host or have the ability as site administrators to remove the content. If the providers remove the terrorist content there would be no further action.

If they did not remove the content, the bill would allow the state to request the courts to order the providers to do so. However, Wednesday's announcement was unclear as to whether threat letters would be issued in all cases or whether some would go straight to court.

Wednesday's announcement also did not clarify if the sanctions against providers that ignore the court order would include criminal sanctions, a point which the bill's promoters have treated inconsistently.

The bill moved forward as ministers made aggressive statements, despite Shaked's September 21 announcement that Facebook removed 95% of 158 inciting posts and YouTube, owned by Google, removed 80% of 13 videos at the government's request.

"These are impressive numbers; however, we understand that there is too much online incitement, and we must continue to increase our efforts," Shaked said at the International Institute for Counter-Terrorism's World Summit at the Interdisciplinary Center in Herzliya in September.

Various petitions to courts in the past to remove content that could cause incitement have often failed because of free speech concerns, such as a 2012 petition by then- MK Taleb a-Sana to order Google to remove a YouTube video disgracing the prophet Muhammad.

The bill would carve out an exception to free speech concerns for incitement to terrorism as has been done in recent years in other criminal areas, such as child pornography.

Times of Israel
US-Israel cybersecurity collaboration act signed into law
Thursday, 22 December 2016

Byline: Staff Report

Jerusalem - US President Barack Obama on Friday enacted legislation to strengthen collaborative cybersecurity research and development efforts between the United States and Israel, one of the congressman involved in drafting the bill said Monday.
The US-Israel Advanced Research Partnership Act of 2016, which had bipartisan support, will expand existing joint research and create a grant for new development.

Reps. John Ratcliffe, R-Texas, and Jim Langevin, D-R.I., introduced the measure after returning from a congressional trip to Israel in July that focused on addressing cybersecurity issues facing both countries, Ratcliffe's office said in the statement issued Monday. Ratcliffe is chairman of the House Homeland Security subcommittee on cybersecurity, infrastructure protection and security technologies.

Langevin in a statement said cybersecurity is "the national and economic security challenge of our time, and we must use every resource at our disposal to support research, foster innovation, and fortify our cyber defenses. This must include a collaborative approach that allows us to work with our leading partners, like Israel, to develop new technologies for our cyber incident responders."

The lawmakers said their meetings with top Israeli officials, including Prime Minister Benjamin Netanyahu and then-defense minister Moshe Yaalon, laid a critical foundation for their US-Israel cybersecurity legislation.

"Our discussions with Israeli national security and cybersecurity leaders revealed the immense wealth of untapped potential we can leverage together to collectively vamp up our efforts to combat growing cyber threats," Ratcliffe said in the statement. "We are extremely grateful for the opportunity to work more closely with a country that's a proven pioneer in cyber science and a top leader in cyber expertise."

La Croix
En Grande-Bretagne, une législation très poussée sur la surveillance
Thursday, 22 December 2016
Byline: Tristan de Bourbon

Londres - Pour lutter contre la menace terroriste, Theresa May, alors ministre de l'intérieur, avait fait voter une législation très dure pour permettre la collecte de données. Mais la Cour européenne de justice a considéré, hier, que cette loi n'était pas justifiée.
Le gouvernement britannique s'est doté, à l'été 2014, de l'une des législations sur la surveillance les plus poussées au monde. Au point que, mercredi, la Cour européenne de justice a estimé qu'elle « excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique » . Concrètement, la loi permet aux autorités de récupérer en masse les données liées aux communications Internet et téléphoniques des Britanniques. Elle impose également aux opérateurs de

téléphonie et aux fournisseurs d'accès Internet de garder les historiques de tous leurs utilisateurs pendant douze mois. Devenue première ministre, Theresa May justifie en effet aujourd'hui la collecte de données par « la menace terroriste » et le « crime organisé » .

Mais les juges luxembourgeois ont estimé que ces pouvoirs n'étaient pas assez restreints, car ils ne se limitent pas à « une période donnée et/ou une zone géographique et/ou un cercle de personnes susceptibles d'être mêlées à une infraction grave » .

Bien qu'ayant exprimé « sa déception » , le gouvernement britannique ne peut être surpris. Le 17 juillet 2015, la Haute Cour de justice britannique avait déjà donné raison aux plaignants, deux députés de la Chambre des communes opposés à la législation. Le gouvernement avait immédiatement fait appel de cette décision. Les juges de la cour d'appel britannique avaient alors demandé l'éclairage de la Cour européenne de justice.

Comme l'explique Pamela Cowburn, l'une des responsables de l'organisation non gouvernementale Open Rights, « je comprends très bien le besoin de surveiller les utilisateurs à risque de terrorisme. Mais cette loi permet (aux autorités) d'écouter tout le monde. Les autorités ont même admis que l'immense majorité des gens suivis sont innocents de tout crime » .

Elle indique que, si la plupart des citoyens lambda pensent ne pas être concernés car ils n'ont rien à cacher, cette surveillance « met fin au secret professionnel des journalistes et des avocats. Par ailleurs, n'importe quel manifestant, même quand il respecte la loi, pourra être suivi par les autorités. C'est la loi la plus intrusive au monde » .

Est critiqué notamment le fait que pas moins de 48 entités gouvernementales sont autorisées à accéder aux métadonnées des internautes. Quel rôle peuvent bien jouer, dans la lutte contre le terrorisme, le ministère de la santé, celui du travail et des retraites, le service des impôts, l'administration chargée de la supervision de la qualité de l'alimentation, etc.?

Pamela Cowburn réfute également l'argument du gouvernement affirmant que lui retirer sa capacité de surveillance le rendrait incapable de lutter contre le terrorisme. « Les attentats belges et parisiens ont prouvé que les services secrets et la police connaissaient les terroristes mais qu'ils n'avaient pas les moyens humains et financiers de les suivre et d'analyser les données les concernant » , rappelle l'activiste. « Cette loi ne fera qu'accentuer le problème: les autorités disposeront d'encore plus de données et pourront donc encore moins cibler efficacement leurs suspects. »

Radio-Canada - Télévision - Ottawa
Des dizaines d'agents de la GRC ont fouillé dans la vie privée de Canadiens sans permission
Thursday, 22 December 2016
Byline: Guillaume Dumont et Valérie Ouellet

Ottawa - Des documents obtenus par Radio-Canada révèlent que des dizaines d'agents de la Gendarmerie royale du Canada (GRC) se sont servis de bases de données policières pour chercher des informations sur la vie privée de Canadiens sans autorisation.
Selon des documents obtenus grâce à la Loi sur l'accès à l'information, de 2010 à 2015, 62 agents de la GRC se seraient servis sans permission de bases de données policières pour fouiller dans la vie privée de proches ou de citoyens.

Selon notre analyse des plaintes portées contre ces agents, 33 d'entre eux ont été blâmés pour avoir utilisé des renseignements confidentiels à des fins personnelles. Notons par exemple le cas d'un agent du Manitoba reconnu responsable d'avoir cherché sans autorisation le numéro d'une plaque d'immatriculation dans la base de données du Centre d'information de la police canadienne (CIPC).

D'autres cas sont beaucoup plus inquiétants : en 2012, un agent a été reconnu responsable d'avoir recueilli de l'information sans autorisation d'une base de données de la GRC, en plus d'avoir entretenu des liens avec un criminel connu. Sa sanction? Une simple réprimande informelle.

Une plainte déposée en février 2015 accuse un agent de s'être servi d'une base de données de façon inappropriée, d'avoir envoyé des photos à caractère sexuel à un mineur et d'avoir utilisé sa position en tant que policier pour entretenir une relation avec cette personne.

L'information ne précise pas quelle sanction a été appliquée et la GRC a refusé de nous dévoiler plus de détails sur cette plainte sans une autre demande d'accès à l'information.

Plusieurs plaintes considérées comme fondées par la GRC précisent que les renseignements confidentiels ont été transmis à un tiers parti. Dans d'autres cas, la plainte inclut aussi des allégations de harcèlement ou d'intimidation.

Dans la majorité des cas identifiés, les agents reconnus responsables d'avoir « mal utilisé » ou de « s'être servis à des fins personnelles » de ces bases de données policières n'ont reçu qu'une simple réprimande, parfois accompagnée d'une formation ou d'une séance de thérapie.

L'une des punitions les plus sévères est une suspension de dix jours sans salaire, en 2014, dans le cas d'un agent qui a utilisé une base de données liée à une opération d'infiltration.

Une seule plainte fondée s'est soldée par un renvoi, en lien avec des recherches faites par un policier de la Saskatchewan en 2011.

« Un manquement à l'éthique flagrant et important », selon un éthicien

Le NPD veut des actions concrètes du gouvernement fédéral pour éviter que des gestes répréhensibles commis par des agents de la GRC restent impunis.

Une casquette de la Gendarmerie royale du Canada (archives). Photo : Radio-Canada

Selon le sénateur et ancien commissaire adjoint de la GRC, Vernon White, ces recherches sont très graves.

Personne ne devrait avoir la possibilité d'accéder à cette information privée à propos d'autres personnes, à moins que ce soit pour le travail.

Vernon White, sénateur et ex-commissaire adjoint de la GRC

« Quand nous faisons notre travail de policier, nous sommes dans une position très avantageuse où nous avons accès à de l'information que personne ne possède », souligne-t-il. « Mais c'est une relation fragile. »

L'éthicien René Villemure, président d'Éthikos, va encore plus loin, affirmant que ces recherches peuvent entacher tout le processus judiciaire si les policiers perdent la confiance du public.

« Si dans le cadre d'une enquête, on me demande de dire certaines choses et que je ne parle pas parce que j'ai peur que l'information se retrouve ailleurs, la police ne pourra pas faire son travail », soutient-il.

À son avis, les corps policiers ont tendance à banaliser ces recherches à des fins personnelles, alors qu'elles démontrent « un manquement à l'éthique flagrant et important ».

Alors que de plus en plus de données confidentielles sont colligées et partagées dans des bases de données du genre, René Villemure croit qu'il est essentiel que la GRC révise la gravité des sanctions octroyées pour ces fautes qui « passent inaperçues, ou presque ».

« Il y a 20 ans, la base de données avait des informations comme des numéros de téléphone seulement. Maintenant, il y a des éléments de preuve, des dossiers qui peuvent vraiment intéresser les criminels », ajoute M. Villemure.

Nous avons tenté à plusieurs reprises, mais sans succès, d'obtenir une entrevue avec la GRC et davantage de détails sur les plaintes fondées qui n'ont mené à aucune sanction.

Dans un courriel, une porte-parole de la GRC affirme que « la GRC prend très au sérieux les contraventions au code de déontologie, et elle s'emploie résolument à gérer les affaires disciplinaires

avec diligence, efficacité et équité ». Elle ajoute que les employés de la GRC « doivent se comporter de façon non seulement à satisfaire, mais à dépasser les attentes élevées et justifiées des Canadiens. »

Quels renseignements détient la GRC?

Centre d'information de la police canadienne (CIPC) : 10 millions de dossiers traités chaque année incluant des casiers judiciaires, des permis de conduire, des plaques d'immatriculation, des véhicules volés, des mandats d'arrêt et des armes à feu enregistrées.

Système d'incidents et de rapports de police de la GRC (SIRP ou PROS en anglais) : 1,6 million de dossiers traités chaque année par 24 corps policiers, incluant les contacts de victimes, suspects, témoins ou contrevenants qui ont été en contact avec des policiers.

PRIME-BC : Créée après l'enquête gouvernementale sur l'affaire Paul Bernardo, cette base de données permet aux policiers de la Colombie- Britannique de coordonner les enquêtes majeures et multijuridictionnelles sur les prédateurs en série avec d'autres forces policières.

« Une situation très préoccupante » pour le NPD

Le porte-parole du NPD en matière de Sécurité publique, Mathieu Dubé, affirme que la situation est préoccupante.

« Les informations confidentielles de la GRC doivent être gérées avec le plus de précautions possible », affirme-t-il.

Ce genre de comportements d'agents qui accèdent à de l'information privilégiée sans raison valable nous inquiète et j'espère que le ministre va faire enquête.

Mathieu Dubé, porte-parole du NPD en matière de Sécurité publique

Plusieurs experts à qui nous avons parlé ont souligné que de nombreux garde-fous sont déjà en place pour limiter et surveiller l'accès à des bases de données hautement confidentielles, comme celles utilisées par la GRC. Par exemple, tous les agents doivent se connecter au système avec un identifiant unique, ce qui permet à la GRC de surveiller la nature et la pertinence de leurs recherches.

Le sénateur Vernon White ajoute que la GRC prend maintenant au sérieux l'accès aux bases de données policières sans autorisation, « mais ce ne l'était pas il y a 15 ans ».

Dans un courriel, le Commissariat à la protection de la vie privée du Canada souligne quant à lui que la GRC a mis en place la vaste majorité des recommandations suggérées par le commissaire en 2011.

Son rapport avait dénoncé un « manque de surveillance » de la GRC vis-à-vis des recherches des policiers sur ses bases de données et le fait que la GRC « ne pouvait pas prouver » que les renseignements personnels étaient toujours utilisés en conformité avec ses politiques dans tous les corps policiers avec lesquels elle partageait ses accès.

En 2015-2016, le Commissariat à la protection de la vie privée du Canada a reçu 107 plaintes contre la GRC, incluant 12 alléguant une atteinte à la vie privée.

Selon nos chiffres, le nombre de plaintes fondées en lien avec l'usage inapproprié de bases de données policières n'a toutefois pas baissé depuis 2011.

Quelles conséquences dans d'autres corps policiers au Canada ?

2016 - Une policière de Gatineau perd son emploi après avoir consulté à six reprises des bases de données policières sans raison apparente.

2012 - Une femme dépose une plainte au Commissaire à la protection de la vie privée du Canada alléguant que deux propriétaires d'appartements, membres de la GRC, ont vérifié ses antécédents criminels dans une base de données policière sans sa permission. Une enquête prouvera que la plainte est fondée.

2011 - Un policier de Windsor est renvoyé après avoir, entre autres, fait des recherches dans la base de données CIPC sur ses partenaires d'affaires et des compétiteurs de restaurants dans lesquels il avait investi.

2005 - Un avocat qui défend les droits de détenus accuse dix agents de la police d'Edmonton d'avoir cherché son nom à 16 reprises dans une base de données de la GRC sans raison valable.

1995 - Un policier de Delta, en Colombie- Britannique, comparaît en cour après avoir cherché les plaques d'immatriculation de véhicules stationnés devant une clinique d'avortement.

Le Soleil
Tous les accès aux sites de la Grande Allée sécurisés le 31 décembre
Friday, 23 December 2016
Byline: Annie Morin

Québec - Tous les accès au site des festivités du 31 décembre sur la Grande Allée seront sécurisés pour éviter qu'un camion puisse pénétrer, a annoncé jeudi le maire Régis Labeaume.
«Du cours du Général-De Montcalm jusqu'au parlement, toutes les rues transversales seront - entre guillemets - sécurisées et bloquées», a expliqué en après-midi le maire de Québec en marge d'une

activité avec des réfugiés. Il n'a pas voulu préciser la forme et le volume des obstacles qui seront ajoutés. Il s'agit généralement de blocs de béton. Des policiers seront également postés aux entrées.

«Un camion normalement ne devrait pas entrer sur le site», a souligné M. Labeaume. La référence à Berlin est directe. Lundi, un terroriste a projeté un camion-remorque sur la foule d'un marché de Noël, tuant 12 personnes et faisant des dizaines de blessés dans la capitale de l'Allemagne.

Mercredi, la mairie a tenu une séance de travail avec des représentants de la police, de la direction générale ainsi que les organisateurs de la fête du 31 décembre sur le thème de la sécurité. «Évidemment, ce n'est pas nouveau. Ce sont des mesures de sécurité qui étaient envisagées depuis longtemps», a tempéré M. Labeaume. «Je le dis parce qu'il y a des gens qui avaient une certaine inquiétude, mais tout a été fait, vraiment tout a été fait» pour que le public soit bien protégé, a-t-il insisté, assurant que la circulation piétonne demeurerait fluide.

Le maire n'est pas en mesure de dire combien il en coûtera pour toutes les mesures de sécurité : «On verra ça après. On investit l'argent qu'il faut pour sécuriser le site.»

Du côté de la police de Québec, le porte-parole n'a ni confirmé ni infirmé les informations. «On ne veut pas dévoiler nos stratégies, justement pour des raisons de sécurité», a souligné David Poitras. Selon le policier, les mesures sont «les mêmes que pour les autres grands événements». «Ce n'est pas une réaction à Berlin», a-t-il déclaré jeudi.

Agence QMI
Bases de données La GRC a fouillé dans la vie privée de Canadiens
Friday, 23 December 2016
Byline: Journaliste maison

Ottawa - Une soixantaine d'agents de la Gendarmerie royale du Canada (GRC) ont fouiné dans la vie privée de Canadiens sans autorisation entre 2010 et 2015, a révélé Radio-Canada hier matin.
En tout, 62 policiers auraient fouillé dans des bases de données policières pour y obtenir des informations sur des proches ou des citoyens. Un agent aurait notamment recherché un numéro de plaque d'immatriculation, tandis qu'un autre aurait recueilli des informations et entretenu des liens avec un criminel. Plus de la moitié des plaintes formulées, soit 34, ont été jugé fondées. Des renseignements formels ont notamment été transmis à des tiers partis.

Le Point
Services secrets français - NSA contre DGSE, petites écoutes entre amis
Thursday, 22 December 2016
Byline: Jean Guisnel

Paris - L'espionnage informatique est l'arme fatale de prédilection du renseignement, et, au sein de la DGSE, les Français ne sont pas en reste.
Nous sommes en juin 2012. Edward Snowden est pour une année encore l'un de ces bons petits soldats de l'ombre, tapi dans une base secrète de la NSA à Hawaï. À Paris, Nicolas Sarkozy termine son mandat, quand le chef des services informatiques de l'Élysée, un homme de la DGSE, s'inquiète. Sur les réseaux de la présidence, il a découvert des mouvements préoccupants et en avertit son ancien service, qui enquête. L'affaire sera révélée dès le mois de juillet 2012 par le quotidien Le Télégramme. Mais il a fallu attendre juin 2016 pour que l'ingénieur centralien Bernard Barbier, à cette époque patron des « grandes oreilles » de la DGSE, choisisse d'en parler devant les élèves de son ancienne école. L'ex-directeur technique de Mortier confirme alors que l'attaque a été conduite par la NSA avec sa méthode de piratage la plus puissante, dont Edward Snowden avait révélé l'existence : le Quantum Attack. Les espions américains ont lancé leur opération en faisant croire à l'ordinateur d'un collaborateur de l'Élysée qu'il se connectait sur Facebook. En réalité, la page d'accueil vers laquelle la machine élyséenne était orientée n'était autre qu'une copie conçue par la NSA. Une fois le lien entre les machines établi, la puissante agence américaine de renseignement technique injectait un logiciel malveillant lui ouvrant un accès complet au réseau élyséen.

L'opération de cyberespionnage Snowglobe © DR

Envoyé aux États-Unis, le 12 avril 2013, pour une explication de gravures, l'expert en cryptographie et en interception des communications entend Keith Alexander, directeur de la NSA, lui dire qu'il est « déçu » car il pensait que « jamais on ne [les] détecterait ». Barbier aura la désagréable surprise de voir quelques mois plus tard les documents préparatoires à cette rencontre transmis par Snowden au Monde. Et le truculent Barbier, joueur de rugby à la faconde méridionale, de poursuivre : « Avant la publication, j'ai convoqué le correspondant de la NSA à Paris pour qu'il me donne une copie du papier. Il me répond : C'est impossible, Bernard, seul le président Obama peut le déclassifier. Je lui ai dit d'arrêter de m'emmerder, 10 millions de Français allaient lire cette note et je ne peux pas la voir ? Je l'ai finalement eue un jour avant sa publication. » À la fin des années 1980 déjà, le FBI découvre que des taupes françaises ont été placées par la DGSE dans ses entreprises les plus performantes.

Et puis les choses se sont arrangées. Les révélations incessantes ? Les preuves que la NSA a organisé à l'échelle planétaire le siphonnage électronique de ses alliés ? Les communications des présidents français successifs interceptées par les autorités américaines ? Les moyens de l'État américain mis au service des entreprises pour déstabiliser leurs concurrents ? Une station d'écoutes installée sur le toit de l'ambassade américaine à Paris ? Calembredaines... Bernard Barbier n'en veut pas le moins du monde aux Américains : « Le patron de la NSA, c'est un copain, on est très amis. Lui et moi, on s'entendait très bien. J'ai beaucoup apprécié de travailler avec les Américains, il faut travailler avec les meilleurs. Il faut savoir que, dans les services de renseignements, on n'a pas d'amis, on a des partenaires. »

Ancien chef de poste de la CIA à Paris, espion de la vieille école, Charles Cogan, 88 ans, brille aussi par sa lucidité. Il sait qu'en matière d'espionnage les deux pays, « plus vieux alliés, amis prudents », conserveront toujours une certaine circonspection. Entre services, c'est le ping-pong perpétuel : à la fin

des années 1980 déjà, le FBI découvre que des taupes françaises ont été placées par la DGSE dans ses entreprises les plus performantes. Les espions français éviteront la prison grâce à Michel Rocard, et on jura qu'on ne jouerait plus à ces jeux pervers. Mais les Américains, dans la foulée, se déchaînent et Charles Pasqua, alors ministre de l'Intérieur, fera expulser sans ménagement, en 1995, tous les responsables de la CIA en poste à Paris, violant les règles les plus sacrées du savoir-vivre entre espions !

Signé « Titi »

Dans ce monde si curieux, les Français affirment aujourd'hui qu'ils n'espionnent plus leurs alliés. On a le droit de les croire, mais ce serait un grand changement ! Il y a quelques années, en 1998, Le Point avait révélé de quelle manière la France espionnait le monde, y compris les États-Unis, en interceptant massivement les communications. Mais faut-il s'en étonner ? Au gré des documents de l'affaire Snowden, on a appris qu'une étrange peuplade informatique est récemment apparue sous les yeux ébahis des experts des services secrets canadiens, le Centre de la sécurité des télécommunications du Canada (CSEC). Ils ont découvert qu'un redoutable logiciel d'attaque circulant clandestinement sur les réseaux ciblait des organisations francophones, le programme nucléaire iranien, d'anciennes colonies françaises comme l'Algérie ou la Côte d'Ivoire. Quand ils ont vu que ce logiciel avait été baptisé « Babar » et que son créateur avait signé « Titi », ils en ont conclu que la DGSE était à la manoeuvre. Des entreprises de sécurité informatique ont fouillé et découvert d'autres logiciels-espions portant les mêmes marques de fabrique, à des degrés divers d'évolution, souvent nommés d'après des personnages de dessins animés : « Bunny », « Dino », « Tafacalou » - qui a provoqué de gros dégâts en Syrie - et surtout « Casper », actif depuis 2014. Tous ces moyens d'intrusion hypersophistiqués ont été rangés sous l'appellation générique d'« Animal Farm », titre du roman antistalinien de George Orwell publié en 1945. Quand on demande à un cadre de la DGSE ce qu'il pense de l'attribution de ces logiciels malveillants à ses experts informaticiens, il botte en touche : « À quoi croyez-vous qu'on nous paie ? »

Lancée en 2008 par Nicolas Sarkozy, la lutte informatique active est une composante désormais intégrée à la stratégie française, dans laquelle l'état-major des armées et la DGSE - pour la composante clandestine - sont étroitement associés. Jean-Yves Le Drian et François Hollande n'ont lésiné ni sur les moyens financiers ni sur les moyens humains, et les moyens offensifs « sont désormais totalement intégrés à l'ensemble des opérations françaises », souligne un expert. Manière de dire que, dans ce domaine, les Français ne sont pas si loin des Américains.

Washington Free Beacon
CIA, NSA Missed Warning Signs of Snowden Betrayal
Friday, 23 December 2016
Byline: Bill Gertz

Washington - Both the CIA and National Security Agency missed warning signs that renegade contractor Edward Snowden was a disgruntled worker who would eventually steal 1.5 million secret documents, according to a congressional study made public Thursday.

Snowden, who fled to Moscow after publicizing some of the documents through left-wing journalists, also "has had, and continues to have contact with Russian intelligence services" and voiced admiration for China during his brief career at the CIA and then NSA.

A declassified and redacted report by the House Permanent Select Committee on Intelligence concluded that Snowden's actions resulted in the Obama's administration's most damaging intelligence failure.

"The American people can now get a fuller account of Edward Snowden's crimes and the reckless disregard he has shown for U.S. national security, including the safety of American servicemen and women," said Rep. Devin Nunes (R., Calif.), the intelligence committee chairman. "It will take a long time to mitigate the damage he caused, and I look forward to the day when he returns to the United States to face justice."

Rep. Adam Schiff (D., Calif), the committee's ranking member, added that "Snowden and his defenders claim that he is a whistleblower, but he isn't, as the committee's review shows. Most of the material he stole had nothing to do with Americans' privacy, and its compromise has been of great value to America's adversaries and those who mean to do America harm."

The report concluded that intelligence documents disclosed by Snowden "caused massive damage to national security." All examples of the damage, however, were blacked out in the report.

On Twitter, Snowden stated in response to the report: "Was I a pain in the ass to work with? Perhaps; many technologists are. But this report establishes no worse."

"Bottom line: this report's core claims are made without evidence, and are often contrary to both common sense and the public record," he said.

The report is dated Sept. 15 and was originally classified "top secret." Markings indicate the report dealt with signals intelligence--sensitive data collected electronically by NSA around the world.

"In June 2013, former National Security Agency contractor Edward Snowden perpetrated the largest and most damaging release of classified information in U.S. intelligence history," the report said.

The findings were based on a two-year committee probe that did not include interviews with Snowden, who is currently facing U.S. espionage charges.

Contrary to some media portrayals, the House report indicates Snowden was a disgruntled employee who argued with his superiors, ultimately fleeing NSA's Kunia facility in Hawaii in May 2013. He then began disclosing documents in what he asserted was a bid to expose improper NSA surveillance.

The committee's findings "demonstrate that the public narrative popularized by Snowden and his allies is rife with falsehoods, exaggerations and crucial omissions, a pattern that began before he stole 1.5 million sensitive documents," the report said.

Snowden compromised secrets that once protected American troops overseas and secrets that were used in countering terrorism along with dealing with threats from states such as China and Russia.

Some of the disclosures "resulted in the loss of intelligence streams that had saved American lives," the report said.

The Pentagon identified 13 high-risk areas of potential damage from future intelligence disclosures, including several that related to defense capabilities. "If the Russian or Chinese governments have access to this information, American troops will be at greater risk in any future conflict," the report said.

Snowden was described as a "serial exaggerator and fabricator" who intentionally lied about his past in order to promote himself to senior positions and gain greater access to secrets.

However, the report includes new disclosures that security officials at both CIA and NSA failed to recognize that Snowden was likely to betray the government's trust and disclose significant U.S. intelligence capabilities that have been lost or restricted as a result.

For example, NSA security officials failed to conduct a routine check of Snowden's educational background. Had they done so, NSA would have learned that Snowden had dropped out of high school in his sophomore year, yet falsely stated on his resume he had graduated from "Maryland High School" in 2001. There is no high school in Maryland with that name.

Snowden also was granted a "top secret" security clearance in 2005 despite an associate warning security investigators he should not be given access to secrets.

Snowden was hired as a computer technician by a CIA contractor and converted to CIA employment in 2006 after obtaining a security clearance. While at CIA, he complained of harassment by a supervisor.

He was posted overseas, but was relieved of his position after altering CIA software improperly and disobeying orders.

Snowden then applied for work at NSA and was hired by an NSA contractor in 2009. However, the report revealed that CIA failed to update a security database with derogatory information about Snowden. As a result, NSA failed to learn of his problems at CIA before hiring him.

The Office of Personnel Management updated Snowden's security clearance in 2011 with an investigation later found to have been incomplete.

"Among other flaws, the investigation never attempted to verify Snowden's CIA employment or speak to his CIA supervisors, nor did it attempt to independently verify Snowden's self- report of a past security violation--areas where further information could have alerted NSA to CIA's concerns," the report said.

Investigators also failed to check job references on Snowden beyond those he offered: his mother and girlfriend.

While working for NSA in Hawaii, Snowden was described by coworkers as "arrogant" and "squirrelly." They said he was chronically late for work, and would claim he overslept as a result of staying up late to play video games.

Coworkers said Snowden expressed few political views, but voiced sympathies for China based on meetings with Chinese hackers.

Snowden, according to the report, once claimed "the United States caused problems for China but China never caused problems for the United States."

Another NSA coworker said Snowden defended Wikileaks' collaborator Army Pvt. Bradley Manning, who stole tens of thousands of State Department and Pentagon documents while posted in Iraq.

The report also disclosed the methods used by Snowden to break into NSA's classified computer networks and download large numbers of documents.

The secrets were stolen from NSANet, the agency's internal computer network, and from an intelligence community-wide system called the Joint Warfighter Information Computer System. The 1.5 million documents, if printed out, would form a pile more than 3 miles high.

As a computer systems administrator, Snowden used downloading tools called scraping software, specifically a program called "wget" and "DownThemAll!" that allowed large numbers of files to be downloaded over slow networks.

NSA failed to use monitoring tools that could have detected the illegal document downloading, the report said.

Snowden also used a desktop computer in Hawaii, a loophole that allowed him to avoid security scrutiny while stealing documents.

The document theft began in the summer of 2012 at the same time Snowden sought full-time NSA employment. According to the report, Snowden was able to cheat on a test he was given in pursuit of full-time NSA position by accessing the test answers on an NSA network.

He was offered a post in NSA's hacking intelligence unit, the Tailored Access Operations office. However, Snowden's demand for a higher salary derailed the job offer.

Snowden contacted leftwing journalist Glenn Greenwald and filmmaker Laura Poitras in December 2012 and January 2013, respectively, and provided both with documents.

By late 2013, Snowden went to work for intelligence contractor Booz Allen Hamilton in an NSA office that battled cyber attacks from Russia and China. While working there, Snowden stole additional documents from the NSA National Threat Operation Center--information that would be valuable to governments in Russia and China.

Snowden boarded a flight for Hong Kong on May 19, 2013. The first disclosures from Greenwald were published on June 5, 2013.

The report said Snowden did not use legal whistleblower protections to raise his objections to NSA surveillance.

In a heavily redacted section on foreign influence, the report quoted a Russian official as saying Snowden shared intelligence with the Russian government.

Intelligence agencies conducted limited damage assessments of the Snowden case, and have not investigated his motive or whether he worked as an agent of a foreign intelligence service.

The disclosures of NSA documents to date represent what the report called the "tip of the iceberg" of more damaging disclosures, the report said.

The cost of mitigating the damage could reach $1 billion.

Security reforms also have not been fully implemented by NSA and other agencies to prevent future insiders from compromising secrets.

"The committee remains concerned that NSA, like the [intelligence community] as a whole, have not done enough to reduce the chances of future insider threats like Snowden," the report concludes.

Vice News
Extract, decode, analyze
Friday, 23 December 2016
Byline: Justin Ling

As the RCMP tries to convince the public that phone encryption is hobbling its investigations, new documents obtained by VICE News show that the federal police agency already has the ability crack encrypted and locked cellphones without help from the owner or the manufacturer.
The records, obtained via access to information request, show that the RCMP's British Columbia branch just renewed its license for the Cellebrite Touch Ultimate.

That device, according to the documents, "enables the most technically advanced extraction, decoding, analysis, and reporting of mobile data. It performs physical, logical, file system, and password extraction of all data (even if deleted) from the widest range of devices including legacy and feature phones, smartphones, portable GPS devices, tablets, and phones manufactured with Chinese chipsets."

The cost of the renewal, dated February, 2016, was redacted from the documents. The records show that they were sent out to both the B.C. division of the RCMP, and the local RCMP detachment in Nanaimo. Other contract documents suggest that, for the Cellebrite device and an enclosure in which police can hack the phone -- one that blocks all outside cell, Wi-Fi, and other signals -- the total cost was just above $90,000.

The police went through TEEL Technologies Canada, the Canadian distributor for Israel-based Cellebrite, to buy the technology.

Cellebrite has become a handy tool for investigators worldwide. And there's good reason. The company recently reported that their devices can even extract user data from Pokemon Go.

In San Bernardino, California, the FBI reportedly went to Cellebrite after Apple refused to help them crack the iPhone of two terror suspects.

While it's not exactly a secret that the RCMP uses Cellebrite -- the only public admission from the force is a testimonial posted to the Cellebrite website by an RCMP officer, lauding the technology and saying his team uses it "every day" -- the federal police have otherwise been publicly silent about the phone-hacking technology.

VICE News has followed the RCMP's surveillance powers closely. Last April, VICE News and Motherboard reported how the RCMP obtained BlackBerry's global decryption key. More recently, we've covered how the force deploys phone-tracking hardware, how they've been trying to keep it secret, and how they've worked to build a "new public narrative" to obtain even more powers.

The RCMP refused to address their use of Cellebrite technology for this story, just as they have refused to address questions on other stories regarding their sensitive investigative techniques.

"We generally do not comment on specific investigative methods, tools and techniques outside of court," an RCMP spokesperson told VICE News over email.

Staying mum on their current techniques hasn't stopped the force from launching a public relations campaign on the problem of encryption -- dubbed "going dark" -- aimed at getting new powers, however.

In a five-part series where the RCMP made a public case for those new powers, the federal police provided a summary of an ongoing investigation to the Toronto Star and CBC where a locked phone thwarted their efforts to solve a child abuse case. "The phone is locked by a pass code and investigators have not been able to access the video," the two outlets reported. "Police have no legal authority to compel the man to unlock his phone."

That is exactly the sort of case where Cellebrite has come in handy for the RCMP.

In a sexual assault and child pornography case from this past April, an RCMP investigator had an iPhone 5 that was password protected. Corporal Gary Luk, of the Richmond, B.C. detachment of the RCMP, cracked it.

"Cpl. Luk explained that Cellebrite creates a mirror image of the data stored on a mobile device without altering the content of that information. This preserves the integrity of the data," wrote a B.C. judge in a ruling pertaining to the case. The judge noted that Luk limited the search of the devices to the search warrant that authorized the use of the Cellebrite, and managed to obtain some 10,000 messages, as well as photos and video from the iPhone, and five other devices.

In another case, a drug investigation in Calgary, the RCMP used the Cellebrite device to extract call records, contacts, text messages, and images.

In the half-dozen court rulings where Cellebrite is mentioned by name, the RCMP managed to crack a variety of phone models -- iPhone, BlackBerry, Sony, and LG.

But there are a variety of other cases where the nature of the RCMP's phone-hacking prowess simply isn't detailed in court.

In one Vancouver kidnapping case that wrapped-up in 2015, the RCMP cracked into three encrypted BlackBerry phones, and "GPS tracking information was extracted from the laptops and encrypted emails were extracted from the Blackberries and decrypted by the RCMP Technical Assistance Team." The police also obtained text messages, including some messages that had been deleted by the users.

One of the RCMP officers involved in that case is the same officer whose signature appears on the invoice receipts for the Cellebrite technology sold to the RCMP's B.C. division.

The RCMP, behind closed doors, appear to even recognize that existing technology can fix their 'going dark' problem -- within the confines of existing laws.

Next month, Constable Frank Dudas of the RCMP's Technological Crime Section, is slated to speak on a panel regarding the "cutting-edge solutions" for search warrants, especially for encrypted and locked smartphones, "to maximize technology investments and respect privacy rights within Canada."

Dadas will be joined on that panel by Daniel Embury, a technical director at Cellebrite.

Ultimately, mention of this sort of technology appears nowhere in the federal government's national security consultations, which were designed to give the public a voice in drafting new legislation that could authorize -- or forbid -- certain intrusive investigative techniques.

A backgrounder prepared for that consultation specifically mentions that "encryption challenges also apply to the court- ordered production of historical data, such as email, text messages, photos and videos from lawfully seized smartphones, computer hard drives and other digital devices," and mentions such difficulties in the San Bernardino case.

The government consultation, however, fails to mention how police are already able to obtain and analyze such data.

Sent to: !INTERNAL; !INTERNAL 2; RCMP Breaking News

Global Times
Draft standards could help development of cyberspace
Friday, 23 December 2016
Byline: Chu Daye

The rolling out of cyber standards is a good thing, as it helps facilitate the communication of data in cyberspace, an expert said on Thursday, following the publication of a string of draft standards seeking public input on Tuesday.
The National Information Security Standardization Technical Committee, a standard-setting committee jointly supervised by the Standardization Administration of China and the Cyberspace Administration of China, on Tuesday released seven sets of draft standards related to cyber security and data privacy for public comment. The deadline for feedback is February 2, 2017.

Qin An, director of the China Institute of Cyberspace Strategy, said the standardization of data together with the governing of behavior of man are two components of cyberspace governance and will make cyberspace a better place.

"The standardization will help cyberspace grow economically, and facilitate cyberspace communication and data flow crossing national borders in an orderly manner," Qin told the Global Times on Thursday, noting that data standardization is also one of the hallmarks of what he called cyber civilization.

The standardization process is also the channel through which the State exercises its governance in cyberspace, noted Qin.

The new draft standards include information security technology on personal information security specifications and security capability requirements for Big Data services technique requirements.

Hindustan Times
Govt hires Cisco to help it handle cyberattacks
Friday, 23 December 2016
Byline: Anirban Ghoshal

New Delhi - Demonetisation has given a big boost to digital payments, and also to the threat of cyberattacks in the country. American technology services company Cisco has signed a memorandum of understanding (MoU) with the government's Computer Emergency Response Team (CERT-In) to tackle issues related to cyberattacks.
India's currently doesn't have a national encryption policy, CERT-In is the nodal agency under the ministry of electronics and IT that deals with cyber security threats such as hacking and phishing, and strengthens the Indian Internet domain. "In light of rapidly evolving cyber tactics and shared risks in cyberspace, the need to work side-by-side with industry partners on pressing cyber-challenges becomes important. Our collaboration with Cisco looks to enhance the security of India's digital infrastructure and speed up digitalisation of India" electronics and IT minister Ravi Shankar Prasad said.

Prasad had said that e-wallet usage has seen a 271% increase in volume and 267% in value since high-value currency was demonetised last month. Cisco will open a security operations centre (SOC) in Pune, a cyber range lab in Gurgaon and a security and trust office (S&TO) to enhance cyber security capabilities.

The announcement is as a part of the $100-million investment, which chairman and ex-CEO John Chambers had announced earlier in the year. "The SOC will provide a broad range of services, from monitoring and management to comprehensive threat solutions and hosted security, which can be customised to meet customer needs," said Dinesh Malkani, president for India and SAARC, Cisco.

The unit will have 24-hour continuous monitoring and advanced analytics capabilities. Cisco currently has three SOCs globally - in Poland, the US and Japan. It has signed similar MoUs with the French and German governments. "Most cyberattacks or breaches take an average detection time of 205 days from the time of breach," Malkani said; nearly 35 records are breached every second globally, he said.
Malkani said the government has asked Cisco to train startups to help create more security solutions from India.

This training will be provided by the cyber range lab. SOC will be operational next quarter. The cyber range lab is already functioning. "A significant amount of investment has gone into the facilities. Nearly

20% of our cybersecurity workforce operates from India. We can scale this up as need arises," Malkani said.

Reuters
Lithuania said found Russian spyware on its government computers
Friday, 23 December 2016
Byline: Staff report

Vilnius - The Baltic state of Lithuania, on the frontline of growing tensions between the West and Russia, says the Kremlin is responsible for cyber attacks that have hit government computers over the last two years.
The head of cyber security told Reuters three cases of Russian spyware on its government computers had been discovered since 2015, and there had been 20 attempts to infect them this year.

"The spyware we found was operating for at least half a year before it was detected - similar to how it was in the USA," Rimtautas Cerniauskas, head of the Lithuanian Cyber Security Centre said.

When presented with the allegations, President Vladimir Putin's spokesman Dmitry Peskov told Reuters they were "laughable" and unsubstantiated.

"Did it (the spyware) have 'Made in Russia' written on it?" quipped Peskov. "We absolutely refute this nonsense." He said Russia itself was targeted in cyber attacks "round the clock," but said it would be stupid to accuse foreign governments.

Fears of Russian cyber attacks have come to the fore since the U.S. election campaign when hacking of Democratic Party emails led to allegations from U.S. intelligence that Moscow was involved.

Lithuania, Estonia and Latvia, all ruled by Moscow in communist times, have been alarmed by Russia's annexation of Ukraine's Crimea peninsula in 2014 and its support for pro-Russian separatists in eastern Ukraine.

In what Baltic officials say was a wake-up call, Estonia was hit by cyber attacks on extensive private and government Internet sites in 2007. State websites were brought to a crawl and an online banking site was closed.

Lithuanian intelligence services, in their annual report, say cyber attacks have moved from being mainly targeted at financial crimes to more political spying on state institutions.

Russian spyware was transferring all documents it could find, as well as all passwords entered on websites such as GMail or Facebook, to an internet address commonly used by Russian spy agencies, Cerniaukas said.

"This only confirms that attempts are made to infiltrate our political sphere," said Cerniaukas.

PREPARATIONS

Germany's domestic intelligence agency reported earlier this month a striking increase in Russian targeted cyber attacks against political parties and propaganda and disinformation campaigns aimed at destabilizing German society.

The domestic intelligence chief said Russia may seek to interfere in its national elections next year.

Although no Russian cyber meddling was detected in the run up or during the Lithuanian general election in October, Cerniauskas said his country needs to understand it is vulnerable to such meddling.

"Russians are really quite good in this area. They have been using information warfare since the old times. Cyberspace is part of that, only more frowned upon by law than simple propaganda", he said.

"They have capacity, they have the attitude, they are interested, and they will get to it - so we need to prepare for it and we need to apply countermeasures."

Lithuanian officials targeted by the Russian spyware held mid-to-low ranking positions at the government, but their computers contained a stream of drafts for government decisions of its positions on various matters, said Cerniauskas.

The head of the Lithuanian counter-intelligence agency Darius Jauniskis said Russia tried to sow chaos in Lithuania by orchestrating a cyber attack in 2012 against the Lithuanian central bank and its top online news website.

"It is all part of psychological warfare," he told Reuters earlier this month.

NPR
CIA Director Urges Caution In U.S. Response To Russia Hacking
Friday, 23 December 2016
Byline: Staff report

Washington - The director of the Central Intelligence Agency, John Brennan, is warning against in-kind retaliation by the U.S. government for Russian hacking during the election.
In an interview with NPR's Mary Louise Kelly, Brennan said, "They do some things that are beyond the pale," referencing those who would undermine democratic processes, adding:

"I don't think we should resort to some of the tactics and techniques that our adversaries employ against us. I think we need to remember what we're fighting for. We're fighting for our country, our democracy, our way of life, and to engage. And the skullduggery that some of our opponents and adversaries engage in, I think is beneath this country's greatness."

Brennan said that, despite the fact that forces loyal to Syrian President Bashar Assad had taken the city, which was controlled by rebels for much of the five-year conflict, he did not believe the violence would end.

"Aleppo's fall, to me is not a sign that there is going to be an end this conflict because I am convinced that many, many of those oppositionists, the ones who are trying to reclaim their country for their families for their neighbors, for their children, will continue to fight," he said.

"This insurgency is not going to go away until there is some type of viable and genuine political process that will bring to power in Damascus a government that is representative of the Syrian people and really will try to repair and recover from this this awful war."

Assad himself appeared to confirm Brennan's assessment earlier this month in an interview with Russian television, in which he said, "Liberating Aleppo doesn't end with liberating the city itself, for it needs to be secured on the outside. Afterwards, identifying which city comes next depends on which city contains the largest number of terrorists."

Brennan also said he felt some responsibility for the horrific bloodshed of the Syrian war. "I think we always like to say that we wish that we would have been able to make a difference, in a way that would have prevented the slide and the situation there," he said.

"There's no way you can divorce yourself or be emotionally or mentally from these situations that you play a role in."

But, he said, he thinks there are limits to American power, saying, "...as great a country -- as powerful country -- as the United States is, we have, in many areas, limited ability to influence the course of events."

Politico
U.S. government begins asking foreign travelers about social media
Friday, 23 December 2016
Byline: Tony Romm

Washington - The U.S. government quietly began requesting that select foreign visitors provide their Facebook, Twitter and other social media accounts upon arriving in the country, a move designed to spot potential terrorist threats that drew months of opposition from tech giants and privacy hawks alike.

Since Tuesday, foreign travelers arriving in the United States on the visa waiver program have been presented with an "optional" request to "enter information associated with your online presence," a government official confirmed Thursday. The prompt includes a drop-down menu that lists platforms including Facebook, Google+, Instagram, LinkedIn and YouTube, as well as a space for users to input their account names on those sites.

The new policy comes as Washington tries to improve its ability to spot and deny entry to individuals who have ties to terrorist groups like the Islamic State. But the government has faced a barrage of criticism since it first floated the idea last summer. The Internet Association, which represents companies including Facebook, Google and Twitter, at the time joined with consumer advocates to argue the draft policy threatened free expression and posed new privacy and security risks to foreigners.

Now that it is final, those opponents are furious the Obama administration ignored their concerns.

"There are very few rules about how that information is being collected, maintained [and] disseminated to other agencies, and there are no guidelines about limiting the government's use of that information," said Michael W. Macleod-Ball, chief of staff for the American Civil Liberties Union's Washington office. "While the government certainly has a right to collect some information ... it would be nice if they would focus on the privacy concerns some advocacy groups have long expressed."

A spokeswoman for Customs and Border Protection, who said the government approved the change on Dec. 19, told POLITICO on Thursday the new policy is meant to "identify potential threats." Previously, the agency had said it wouldn't prohibit entry to foreigners who didn't provide their social media account information.

The question itself is included in what's known as the Electronic System for Travel Authorization, a process that certain foreign travelers must complete to come to the United States. ESTA and a related paper form specifically apply to those arriving here through the visa-waiver program, which allows citizens of 38 countries to travel and stay in the United States for up to 90 days without a visa.

As soon as the government unveiled its draft proposal in June, however, consumer protection advocates expressed outrage. In a letter sent in August, the ACLU, Center for Democracy and Technology charged it posed immense privacy risks, given that social media accounts serve as "gateways into an enormous amount of [users'] online expression and associations, which can reflect highly sensitive information about that person's opinions, beliefs, identity and community." The groups also predicted the burden would "fall hardest on Arab and Muslim communities, whose usernames, posts, contacts and social networks will be exposed to intense scrutiny."

After the policy changed, Nathan White, the senior legislative manager of Access Now, again blasted it as a threat to human rights.

"The choice to hand over this information is technically voluntary," he said. "But the process to enter the U.S. is confusing, and it's likely that most visitors will fill out the card completely rather than risk additional questions from intimidating, uniformed officers -- the same officers who will decide which of your jokes are funny and which ones make you a security risk."

Opponents also worry that the U.S. change will spark similar moves by other countries.

"Democratic and non-democratic countries -- including those without the United States' due process protections -- will now believe they are more warranted in demanding social media information from visitors that could jeopardize visitors' safety," said Internet Association general counsel Abigail Slater. "The nature of the DHS' requests delves into personal information, creating an information dragnet."

Yahoo News
Snowden is still in contact with Russian intelligence, House report charges
Thursday, 22 December 2016
Byline: Michael Isikoff

Washington - Newly declassified passages from a highly critical House Intelligence Committee report on Edward Snowden assert that since arriving in Moscow the former NSA contractor "has had, and continues to have, contact with Russian intelligence services."
Minutes after the report was released Thursday, Snowden's chief lawyer, Ben Wizner, tweeted that the report was "petulant nonsense." Snowden has adamantly denied such contacts, most recently this month in an interview with Yahoo Global Anchor Katie Couric. Snowden told Couric he gave Russian officials "the stiff-arm" when they first approached him in 2013, and that since then, while living with President Vladimir Putin's approval as a fugitive in Moscow, "they have left me alone, for the most part."

The panel's newly declassified 33-page report, which is being released this morning, cites classified U.S. intelligence reporting to support its assertion of continuous contacts with Russian intelligence -- an especially explosive charge in light of the current uproar in Washington over Russian interference in the U.S. election.

But all details of that intelligence reporting are still classified and blacked out in the report, making it difficult, if not impossible, for the public to assess. The charge comes at a time when Snowden's defenders -- who portray him as a courageous whistleblower who exposed U.S. surveillance abuses -- are making their final, uphill pitch for a pardon before President Obama leaves office.

His lawyers have also repeatedly pointed out he has also criticized Russian surveillance practices; in his interview with Couric, Snowden said these "severe" criticisms have made him a "liability" to the Russians.

"The House committee spent three years and millions of dollars in a failed attempt to discredit Edward Snowden, whose actions led to the most significant intelligence reforms in a generation," Wizner said in a statement after the committee's release. "The report wholly ignores Snowden's repeated and courageous criticism of Russian surveillance and censorship laws. It combines demonstrable falsehoods with deceptive inferences to paint an entirely fictional portrait of an American whistleblower.

"For all of its harsh rhetoric, the report contains no evidence whatsoever that Snowden's intentions were anything other than public-minded, that his actions caused harm, or that he is under foreign influence -- because no such evidence exists," he added. "In fact, the NSA's former deputy director has stated publicly that he does not believe that Snowden acted under the influence of a foreign power."

A U.S. government official told Yahoo News the committee's characterization of continuing contacts between Snowden and Russian intelligence reflects "the current thinking" of the U.S. intelligence community. But U.S. officials do not have evidence that Snowden has actually shared NSA documents with the Russians, said the official, who did not provide any further details about the nature of the alleged contacts. A congressional staffer familiar with the matter said the committee and the intelligence community have "high confidence" in the reports of continuous contacts and "you don't have high confidence based on a single [intelligence] report."

House Intelligence Chair Rep. Devin Nunes said in a statement Thursday the newly declassified report shows Snowden's "reckless disregard" for U.S. National Security, adding "I look forward to the day when he returns to the United States to face justice."

California Democratic Rep. Adam Schiff, the panel's ranking minority member, added: "Snowden and his defenders claim that he is a whistleblower, but he isn't, as the committee's review shows."

The House report fleshes out a three-page executive summary that was released in September and was approved on a bipartisan basis by all members of the intelligence committee. That summary -- denounced as "aggressively dishonest" by one of the journalists who received documents from Snowden -- labeled him a "serial exaggerator and fabricator" as well as a disgruntled employee who did "tremendous damage to national security" by disclosing classified material about U.S. surveillance practices. (The summary did not include the allegation about Snowden's contacts with Russian intelligence, which was declassified by the U.S. intelligence community only this week.)

After the release of the executive summary, the committee asked Director of National Intelligence James Clapper to declassify the panel's full report (much of which is based on secret U.S. intelligence reports and interviews with officials at the National Security Agency and other U.S. agencies). Many key sections of the document remain classified and blacked out -- including 20 specific examples of damage that U.S. officials believe was caused by Snowden's disclosures. Also still classified are estimates about the cost to the U.S. government -- believed to be in the billions of dollars -- to rebuild and repair U.S. signals intelligence systems capabilities as a result of his disclosures.

Still, the newly declassified version cites a wealth of previously undisclosed internal emails, memos and interviews to draw a highly unflattering portrait of Snowden as an intelligence Community misfit driven as much by personal grievances as by his publicly stated concerns about invasions of U.S. privacy.

It also reveals a glaring internal screwup by U.S. intelligence officials that allowed documented concerns about Snowden's conduct by the CIA to go undetected when he landed a job as an NSA contractor.

Among the highlights:

-- Snowden had a troubled work history within the U.S. intelligence community. He'd raised multiple complaints about his treatment that had nothing to do with U.S. surveillance practices. Less than three months after obtaining his first job with the CIA as a telecommunications information system officer (TISO) in 2006, he sent an email to the agency's inspector general complaining that he was being "unfairly targeted" by his supervisor because he had raised concerns about "morale and retention issues" including the pay of TISOs compared with contractors doing similar work. Snowden, then 23, had surveyed other TISOs in his office and then written up his findings, sending them directly to the CIA's deputy director for support, one of the 10 most senior executives in the agency. What prompted Snowden to complain to the inspector general, according to the report, was that his supervisors -- after learning that he had gone over their heads -- had pulled him into their offices for unscheduled "counseling," during which, he asserted to the IG, they were "extremely hostile" and "seemed to believe I have trouble bonding with my classmates." Snowden asked the IG to help protect him from "reprisal for speaking truth to power." Notably, the report said, this was the only record of Snowden contacting the inspector general during his tenure at the CIA.

-- Snowden later landed a CIA TISO post overseas -- in Geneva, it has been publicly reported, although the city is blacked out in the report -- despite the concerns of his previous supervisor, recorded in a Sept. 8, 2008, internal memo, that Snowden "often does not positively respond to advice from more senior officers ... does not recognize the chain of command, often demonstrates a lack of maturity, and does not appear to be embracing the CIA culture." Snowden later modified the software for his performance review "by manipulating the font," the report says. (Snowden has said that while writing his annual self-evaluation he discovered flaws in the software of the CIA's personnel Web applications that would make them vulnerable to hacking. With his supervisor's approval, he asserted, he wrote some code and text in his personnel evaluation, but a more senior manager grew furious and wrote a critical comment in his personnel file.)

His behavior caused him to be recalled for "professional consultations" with the chief of all CIA technical officers in Europe, according to the committee report. His supervisor called him in for six counseling sessions between October 2007 and April 2008. When he flew home to Washington with his girlfriend in September 2008 for medical appointments -- "disobeying orders," the report says -- his supervisors recommended that he not return to his position. Although Snowden has since asserted that he had ethical qualms about working for the CIA in Geneva -- the Oliver Stone movie "Snowden" depicts him recoiling at being asked to blackmail a potential Pakistani asset over sexual misconduct -- the report says

records of Snowden's multiple counseling sessions show no evidence he ever raised such issues at the time.

-- When Snowden applied for a new position with an NSA contractor (Perot Systems, later purchased by Dell) in March 2009, NSA Security checked with an intelligence community-wide database known as "Scattered Castles" to verify his security clearance and, seeing no red flags, approved his hiring on April 7 of that year. This happened because CIA Security had yet to update Scattered Castles with the issues raised about Snowden's employment in Geneva. Thirteen days later, on April 20, the CIA did, entering negative information about Snowden that was unknown to NSA and was apparently never detected. "Because NSA had checked the database three weeks earlier, NSA Security did not learn of the (blacked out) in his record at that time," the report states. In the fall of 2010, a government contractor, U.S. Information Services, did a periodic background investigation of Snowden and cleared him in a report that never verified his CIA employment or checked with any of his supervisors. Nor did it request any character references beyond the two Snowden had provided: his mother and his girlfriend.

-- In early 2012, Snowden took a new position with Dell as a systems administrator at the NSA's Hawaii Cryptologic Center. Some co-workers recall him expressing strong political opinions, complaining about bills in Congress that he believed would be harmful to online privacy and -- according to one co-worker's account -- indicating sympathy for China. (He claimed that, based on his meeting with Chinese hackers at a conference, "the United States caused problems for China but China never caused problems for the United States," the report states, citing a committee interview with a co- worker.) He soon got into an email dispute with his supervisor over an issue that is blacked out in the report. But, much like he did at the CIA, Snowden went outside channels, according to the committee: He copied a deputy head of NSA's technical services directorate in one of his replies during which he accused one of his middle managers of "evasion and finger-pointing." This earned him a rebuke from an NSA civilian employee in Washington who, on June 22, 2012, wrote him in an email that his response was "totally UNACCEPTABLE" because "under no circumstances will any contractor call out or point fingers at any government manager whether you agree with their handling of an issue or not."

-- Snowden has publicly claimed that his "breaking point" for disclosing classified documents was Director of National Intelligence Clapper's March 13, 2013, testimony before Congress in which he (falsely) denied that the NSA collected data on Americans. But the report states that Snowden began his mass downloading of documents from NSA networks on July 12, 2012, barely three weeks after his rebuke from the NSA official. (Snowden has asserted that, while he had already begun his downloading and had reached out to journalist Glenn Greenwald in December 2012, he didn't actually disclose any documents until after Clapper's testimony.) He used blunt "scraping" tools to download the material and used his systems administrator privileges to search across other NSA employees personal network drives and copy what he found, the report states. He also asked several of his unwitting co-workers for their security credentials so he could obtain information he could not access, causing at least one NSA co-worker to lose his security clearance and resign. Snowden's searches "quickly expanded beyond surveillance programs" and included searches for "human resource files" and files relating to promotion

and hiring decisions, as well as the personal network drives of individuals belonging to individuals involved in the hiring decision for a job for which Snowden had applied, the report states.

Jakarta Post
Police step up cyberoperation
Friday, 23 December 2016
Byline: Haeril Halim, Arya Dipa, Fadli

Jakarta/Bandung/Batam - The recent terrorism plots foiled by the police's counterterrorism squad all have the same feature: They were inspired and orchestrated remotely by an Indonesian militant with the Islamic State (IS) group in Syria.
The 33-year-old militant, Bahrun Naim, who is known to be tech-savvy, allegedly managed to recruit new militants and created a number of new terrorist cells across the country through online chat groups.

Terrorist groups, the police have said, are now engaging in cyber-jihad, which includes activities such as recruitment of followers, online training on bomb making and the spread of radical thought to potential followers, as well as the transfer of money from jihadists overseas to Indonesian extremists.

In the past 12 days following the foiled plot to attack the State Palace on Dec. 10, the nation's counterterrorism squad, Densus 88, has uncovered at least 13 terrorist cells in West Java, Central Java, Banten, North Sumatra, West Sumatra and Batam, arresting a total of 21 people who had allegedly planned attacks during Christmas and New Year's Eve this year.

The raids were only possible because the police had stepped up their cybersurveillance, National Police chief Gen. Tito Karnavian said on Thursday. "This is the result of launching massive cybercounterterrorism as we are really concerned about what's going on in the cyberworld. We have been stepping up efforts for cybersurveillance on them [terrorist groups]," he added.

Tito said that the police's cybertroops worked every day to monitor and track activities of radical groups on the internet. Its members usually create fake accounts so that they could join chat rooms of terrorist groups after they introduce themselves as potential followers.

Participants of the online chatting, the police chief said, would later exchange phone numbers so that the cybertroops could join their Whatsapp groups for daily conversations among suspected terrorists to find out where they might launch attacks and with which other terrorist groups they actively communicate.

"These kinds of cyberpatrolling techniques are actually the same as the methods in undercover activities in the real world," Tito said, adding that the only difference was they were conducted online.

Tito, however, admitted that the cybertroops had difficulties monitoring terrorism plots that were devised by lone wolves, as they usually did not join any terrorist group chats online. "Lone wolves independently study from the internet and carry out attacks alone," Tito said, adding that Densus 88 had arrested a total of 40 suspected terrorists this year.

Police officers stand guard at a residential neighborhood where police conducted a raid on a house used by suspected militants, in South Tangerang, Banten, on Dec. 21. Three suspected militants who were planning a holiday season suicide bombing were killed in the raid.(AP/Tatan Syuflana)

From the recent arrests, the police identified three terrorism plots devised by followers of the arrested Bahrun. They were allegedly planning to attack the State Palace, a police station in Tangerang, and an unspecified location in Bali.

"We have arrested members of the group that wanted to attack Bali. The female [alleged suicide bomber intended for an attack in Bali] has also been arrested," the police chief said.

Of the 23 terrorists Densus 88 arrested recently, two were women who were alleged to be suicide bombers, namely Dian Yulia Novia and Ika Puspitasari. Bahrun had allegedly assigned Dian to attack the State Palace and Ika to undertake the attack in Bali.

Densus 88 has reportedly arrested about 1,000 terrorists since its establishment in 2004 and since the deadly JW Marriot Hotel bombing it has derailed a total of 50 terrorism plots.

Terrorism expert Noor Huda said that the fast growing use of social media had changed discourse on terrorist activities in Indonesia.

In the past, would-be terrorists would have had to join major radical groups like Jamaah Islammiya (JI), Jamaah Ansharut Tauhid (JAT), or Jamaah Ansharut Daulah (JAD) to be involved in terrorism, but nowadays with the help of the internet they are able to establish small cells quickly after chatting with people with similar visions online.

"[Under the new discourse], some easily become members of unknown groups, although they have never met each other. This has been proven in the case of Dian who was exposed to radicalism through Facebook and got connected with Bahrun's network," Noor said.

Officers infiltrate chat groups to track terrorism plots Cybersurveillance cannot detect lone wolves, police chief says.

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

13 01 2016 to/au 19-01-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

'Troubling' Conservative torture policy up for review, Goodale says
Canadian Press, Jim Bronskill, 2016 01 19
Ottawa - **The Trudeau Liberals will review controversial directives enacted by the Harper government that allow for the sharing of information even when it might lead to torture**, says the public safety minister. The ``troubling set of issues'' raised by the foreign information-sharing policy ``will be raised in the course of our consultations'' on the overall national security direction of the new government, Ralph Goodale said in a recent interview with The Canadian Press. The news follows pressure from human-rights and privacy advocates to conduct a wide-ranging examination of security policies introduced by the Conservatives, whisked from office in the October election. The federal policy on foreign information-sharing has been roundly criticized for effectively condoning the torture of people in overseas prisons, contrary to international law and Canada's United Nations commitments. A four-page 2010 framework document, released under the Access to Information Act, says when there is a ``substantial risk'' that sending information to, or soliciting information from, a foreign agency would result in torture _ and it is unclear whether the risk can be managed through assurances or other means _ the matter should be referred to the responsible deputy minister or agency head. In deciding what to do, the agency head will consider factors including the threat to Canada's national security and the nature and imminence of the threat; the status of Canada's relationship with _ and the human rights record of _ the foreign agency; and the rationale for believing that sharing the information would lead to torture. Critics say when there is a serious risk of torture, there should be no sharing _ period. **The Canadian Security Intelligence Service, the RCMP, the Canada Border Services Agency, National Defence and the Communications Security Establishment, Canada's electronic spy agency, are bound by the federal policy on sharing information with foreign agencies.**

Burkina Faso attack shows need to boost information-gathering: Sajjan
Ottawa Citizen, Lee Berthiaume, 2016 01 19
St. Andrews, N.B. - **Defence Minister Harjit Sajjan says better intelligence capabilities, as well as co-operation with Canada's allies, are essential for preventing the types of terror attacks that have struck Burkina Faso and other parts of the world**. Six Canadians were killed over the weekend when militants linked to al-Qaida stormed a hotel in Ouagadougou, the capital of Burkina Faso in West Africa. Days earlier, a Canadian was killed during an attack by Islamic State-inspired terrorists in Indonesia. Speaking on the sidelines of a three-day retreat between Prime Minister Justin Trudeau and his cabinet ministers, Sajjan said Canada has "to get better at our intelligence capabilities in other parts of the world so that we have a better chance of preventing attacks like this from happening. Edward Snowden revealed that American and Canadian spy agencies have been running massive intelligence-gathering **operations. The previous Conservative government also enacted controversial anti-terror legislation, Bill C-51, that increased the scope and powers of Canada's intelligence operations.** The Liberals promised during the election to amend the law, but haven't said how. Instead, they have promised broad consultations first. Sajjan, who is responsible for the ultra-secret **Communications Security Establishment**, which is Canada's electronic spy agency, said "the safety of Canadians will always be paramount," but also that there "has to be a balance."

L'armée veut épier les réseaux sociaux
Le Devoir, Fabien Deglise, 2016 01 15
Ottawa - **Surveiller, pour mieux protéger. Le ministère de la Défense nationale du Canada souhaite créer une escouade d'une quarantaine d'analystes chargés d'espionner en temps réel les grands réseaux sociaux, de manière confidentielle**, et ce, afin d'identifier les " nouvelles instabilités ", tout comme les personnes ou groupes pouvant représenter une menace pour le Canada, a découvert Le Devoir. Selon un document d'appel de soumissions, les réseaux Twitter, Facebook, LinkedIn, Instagram et Reddit, entre autres, sont dans la mire des Forces canadiennes, qui cherchent à faire l'acquisition d'une plateforme complète de surveillance, d'analyse et de filtrage des données personnelles et publiques des internautes transitant sur les réseaux sociaux.

Top Employers for Young People tap into the next generation
Globe and Mail, Diane Jermyn, 2016 01 15
Analysis: **Employers for Young People sends out a message of confidence in today's students and recent grads just starting their careers**. The 95 winning companies for 2016 not only welcome young people into their ranks, but also offer unique opportunities for them to develop their knowledge and skill sets through a variety of paid internships, educational support, job shadowing, rotational programs and the chance to travel and work abroad. These employers also profit by giving young talent a voice, allowing them to put forward ideas that add value and bring fresh energy to the workplace. **Canadian Security Intelligence Service (CSIS), Ottawa. Federal government; 3,299 employees. Staff attended more than 100 recruitment events in the past year, including 10 networking sessions, and held 11 career information sessions.**

Government may take extra steps to examine security agencies
Ottawa Citizen, Ian MacLeod, 2016 01 14
Ottawa - **Public Safety Minister Ralph Goodale says the Grits may consider more than just a new committee of parliamentarians to scrutinize the effectiveness and lawfulness of Canada's growing national security activities**. His comments coincide with a new discussion paper circulating within government by national security law scholars Craig Forcese and Kent Roach. It calls for a three-pronged reform of national security review and oversight based on the experiences of Canada's leading allies. Goodale and Ottawa Liberal MP David McGuinty, chair of the yet-to-be-struck special committee, were in Europe this week, where they appraised the workings of Britain's respected Intelligence and Security Committee of Parliament. Speaking to reporters, **Goodale said his priority is that the Liberal's proposed national security committee of parliamentarians be a credible, trustworthy body capable of substantive review of Canada's spy agencies and other classified government intelligence operations**. Canada is the only nation among major western allies that does not allow parliamentarians access to classified security and intelligence information about spying, policing and other sensitive national security operations. While they agree with the need for such a committee, Forcese and Roach, who led the expert assault on the Conservative's controversial Bill C-51 security legislation last year, say it is probably not the best tool for detailed review. They propose two additional review mechanisms. One revives the idea of revamping the existing **Security Intelligence Review Committee (SIRC)**, responsible for expert monitoring of select **Canadian Security Intelligence Service**, into a "super-SIRC" responsible for expert scrutiny of all of **Canada's national security establishment**. As it now stands, there is no dedicated, external monitoring of the **Canada Border Services Agency**, which has a dual intelligence-law enforcement role, or of the intelligence arms of the RCMP, Citizenship and Immigration Canada, the Privy Council Office, Department of Foreign Affairs, Trade and Development, and the Financial Transactions and Reports Analysis Centre of

Canada. A super agency also would consolidate the existing functions of the expert review body monitoring the activities **of Canada's electronic spying service**, as well as the Civilian Review and Complaints Commission for the RCMP, which has very limited review powers over RCMP national security operations.

Canada campaigners to demand public debate on controversial anti- terror law
The Guardian (London), Jessica Murphy, 2016 01 13
Ottawa- **Opponents of Canada's sweeping new anti-terror law are planning a major campaign to pressure the Liberal government to launch broad public consultations before overhauling the controversial legislation**. Civil society groups, legal scholars and labour unions are calling on the government to hold a public debate on reforms for the legislation - known as C-51 - which they say are necessary to protect Canadian civil liberties, freedoms and personal privacy. "We know very little about the government's plans for C-51, so our hope is they are going to listen to the huge number of Canadians who expressed deep, deep concerns about this bill when it was passed," British Columbia Civil Liberties Association executive director Josh Paterson says. "They need to be very clear on what their intentions are before actually doing anything." Federal public safety minister Ralph Goodale is in London this week looking to the UK's intelligence and security committee of Parliament - which examines the policy, administration and expenditure of that country's intelligence agencies - as a possible model. Goodale's spokesman, Scott Bardsley, said: "Work on our platform commitments on C-51 is ongoing. The full details will be unveiled in due course." Those commitments include a guarantee all **Canadian Security Intelligence Service (CSIS**) warrants respect the charter and a statutory review of the full anti- terror act after three years.

Conservatives say security committee is a 'radical departure,' breaks election promises
CBC.CA, Staff Writer, 2016 01 13
Ottawa - **Conservative critics are panning last Friday's announcement that veteran Liberal MP David McGuinty will have a "leadership role" on a new statutory committee of Parliamentarians responsible for reviewing security-related issues**. Public Safety Minister Ralph Goodale's announcement came without "any meaningful dialogue with the security and intelligence community in Canada and without any consultation with Parliamentarians," said public safety critic Erin O'Toole and Conservative House Leader Andrew Scheer in a press release issued Tuesday. "Minister Goodale's approach undermines the establishment of a committee that is supposed to be free from political agendas." Goodale, who is in the U.K. this week consulting with parliamentarians and intelligence officials there who have experience with a similar oversight body, confirmed Tuesday that McGuinty was the government's choice to chair the committee. "The prime minister has invited Mr. McGuinty to serve as chair and I'm very glad that David has been with me in these consultations, to have the benefit of that first hand reflection," he said. McGuinty is travelling with Goodale but was not available for comment. Goodale said it's time Canada added parliamentary oversight to its security agencies, something other members of the so-called **Five Eyes intelligence alliance -- the spy group comprising Canada, the U.S., Britain, Australia and New Zealand -- already have.** The previous Conservative government was criticized for weakening the oversight of Canada's spy agency, **CSIS**, when its internal watchdog office was shut down. The Security Intelligence Review Committee, which reports to Parliament, not the minister, has been criticized as insufficiently transparent and accountable. It also lacks sufficient power over the security agencies it supervises.

The government doesn't want you to click here
Embassy, Marie-Danielle Smith, 2016 01 13

Ottawa - **Government of Canada users should avoid clicking on suspicious or catchy articles or email links, warns a Canadian spy agency in its Cyber Defence Report for the first quarter of 2015.** "Clickbait," it explains, "are websites or online articles designed to drive visitor traffic by containing catchy sensationalist headlines like 'must see' or 'unbelievable' and are distributed over social media and online ads." They want to exploit curiosity, the **Communications Security Establishment warns**-- to "drive web traffic and generate advertising revenue" or to "launch exploits against systems that visit a seeded website." Though the former sounds like the behaviour of any modern news organization, it's the latter that concerns Canada's government. Luring users through email links, or phishing, is one of the ways that hackers can attempt to compromise systems or access classified data. The report, obtained with an access to information request, is heavily censored, citing Access to Information Act restrictions: information can't be released that could reasonably be expected to expose the vulnerability of computer or communication systems. A pair of incidents were being investigated at the **Canadian Security Intelligence Service** in March, Embassy reported last year. They consisted of an "unauthorized disclosure of information" and an "inadvertent release of classified information which was ultimately accessed." Documents obtained through access to information law didn't offer many details about what happened, so whether Canadian spies are as susceptible to clickbait as the rest can't be verified.

Révision constitutionnelle : les Algériens du Canada se mobilisent contre l'article 51
El Watan, Samir Ben, 2016 01 13
Montréal - **Le projet de révision de la constitution entérinée par le conseil des ministres de lundi dernier fait réagir les Algériens du Canada qui représentent la deuxième communauté nationale à l'étranger, avec un peu plus de 100 000 citoyens dont une majorité de binationaux**. Un rassemblement devant le consulat d'Algérie à Montréal est prévu le samedi 16 janvier à partir de 14 :30 pour dénoncer la disposition contenu dans l'article 51 du projet de révision constitutionnelle qui exclut les Algériens détenteurs d'une seconde nationalité ou plus de la possibilité d'accéder « aux hautes responsabilités de l'Etat et aux fonctions publiques». Lancé par l'organisme Mouvance migratoire O Canada que préside l'Algérien Ahcène Moussi, l'appel dénonce l'article 51 qui de crée « deux classes de citoyens, diamétralement opposées : les Algériens qui résident en permanence en Algérie et les Algériens établis à l'étranger, appelés aussi "émigrés ou binationaux". ». Pour cet organisme qui s'occupe, entre autres, de réfugiés au Canada, l'article 51 « porte atteinte à l'unité nationale, en plus d'être discriminatoire.

Sajjan wants increased use of Canadian intelligence in ISIS mission
CTV.CA, Michelle Zilio, 2016 01 14
Ottawa - **Defence Minister Harjit Sajjan says the government is looking at ways to increase Canadian intelligence capabilities in the U.S.- led coalition against ISIS.**
Speaking to CTV's Power Play on Wednesday, Sajjan emphasized the importance of the Canadian intelligence skills in the fight against the terror group. "**Our intelligence capability is second to none. It's always sought after and we are looking at different forms of capabilities, how we can increase that,"** said Sajjan. "We have a robust intelligence capability and how do we integrate that into our training that we're already doing?" Sajjan said the need for increased medical assistance also came to mind during his recent visit to Iraq. He said the government is still considering what is needed in terms of medical help, and is cautious not to propose options that won't work on the ground.Last week, the Globe and Mail reported that the federal cabinet is reviewing options to boost Canada's role in the coalition against ISIS, ranging from clandestine operations to the maintenance of surveillance and refuelling aircraft. The report also said cabinet is expected to make a decision within 30 days of Jan. 7. The minister said he and Chief of the Defence Staff Jonathan Vance have been talking frequently about options for

the future of Canada's role in the coalition. He added that his list of options has been refined "considerably," but did not say when exactly he plans to delivery that finalized list to cabinet.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

'Teens' Who Hacked CIA Director Also Hit White House Official
Motherboard (Vice), Lorenzo Franceschi-Bicchierai, 2016 01 19
New York - **The hacking group that has been targeting government officials since October, when it broke into the AOL email account of CIA Director John Brennan**, has claimed yet another victim. This time, the victim is President Barack Obama's senior advisor on science and technology John Holdren, Motherboard has learned. One of the cybercriminals linked to the group that hacked Brennan broke into Holdren's home telephone and email account and set it so that all the calls would get forwarded to the Free Palestine Movement. This is exactly what happened to **US Director of National Intelligence James Clapper** last week. On Monday, one of the members of the hacking group, which is known as Crackas With Attitude, or CWA, sent me an email to tell me about his latest feat. "If you don't believe me you can call the home phone," he said, before sending me a phone number that belongs to Holdren, according to public records. When I called the number, the founder of the Free Palestine Movement Paul Larudee picked up the phone. Larudee said that the same person who called him last week to tell him that he would receive calls directed at Clapper called him again on Monday morning. Cracka told me on Monday that the group hacked several other government officials, including some the group never publicly bragged about. He mentioned Amy Hess, the FBI's executive assistant director for science and technology, White House Communications Director Jen Psaki, White House Chief of Staff Denis McDonough, the Deputy Secretary of State Tony Blinken, and the White House Deputy National Security Advisor Avril Haines.

Michael Bay's Benghazi movie 13 Hours is 'inaccurate', according to CIA officer
The Guardian, Scott Bixby, 2016 01 19
London - **Bay's film, which depicts the events of the deadly terrorist attack in Libya, has been criticised by an officer who says a main plot point never happened.** Michael Bay has assured audiences that his Libyan-set military thriller 13 Hours: The Secret Soldiers of Benghazi is an accurate retelling of the events surrounding the terrorist attack in Benghazi in 2013, which resulted in the death of four people, including the US ambassador to Libya. But **according to the CIA officer in charge of the American intelligence agency's top-secret Benghazi facility that night, one of the most important moments of the film is entirely wrong.** "There never was a stand-down order," the officer – the former chief of the so-called Annex who identified himself as 'Bob' – told the Washington Post. "At no time did I ever second-guess that the team would depart."

Court Requires NYPD to Purge Docs on Terrorists Inside U.S.
Washington Free Beacon, Adam Kredo, 2016 01 18
Washington - **The New York Police Department has been directed by a U.S. court to remove from its online records an investigation pertaining to the rise of Islamic extremists** in the West and the threats these individuals pose to American safety, according to legal documents. As part of a settlement agreement reached earlier this month with Muslim community advocates in U.S. District Court, the NYPD will purge from its website an extensive

report that experts say has been critical to the department's understanding of radical Islam and its efforts to police the threat.

When the CIA had a magazine
National Post, Robert Fulford, 2016 01 16
Column: **In 1953 a remarkable magazine called Encounter appeared, as if out of nowhere, in London. There were two editors - the famous English poet Stephen Spender and the New York intellectual Irving Kristol, who would later be called the godfather of the neo-conservatives.** With Spender's tentacles reaching every corner of British literature and Kristol's shrewd sense of American thinking, they proved an impressive pair. Their magazine was full of life and ideas. John Berryman, the first-class American poet, called Encounter "the most consistently interesting magazine now being published." The writers ranged from Evelyn Waugh to Mary McCarthy and from Arthur Schlesinger, Jr., a leading American liberal, to Anthony Crosland, a Labour cabinet minister and theorist. Somehow Encounter managed to get the best work that most of these people, and a few dozen others, could produce. For 14 years it was a success, but then it was disgraced. Ramparts, a magazine of the then New Left, disclosed that Encounter was financed by the Paris-based Congress for Cultural Freedom, a creature of the Central Intelligence Agency. This was in 1967 when anger at the Vietnam War threw a shadow over anything done by the U.S. government - especially anything secretive. Fighting the Cold War, Washington had noticed that Soviet propaganda was succeeding among artists and leftists. **The West needed to demonstrate the superiority of freedom as against the stultifying censorship in the U.S.S.R. In 1951 the CIA made Nicolas Nabokov (Vladimir Nabokov's composer cousin) head of the Congress for Cultural Freedom**. He organized festivals and conferences around Europe while encouraging Encounter and other CIA-backed magazines in Germany, Japan and elsewhere.

No word on former FBI agent missing since 2007
Washington Post, Adam Goldman, 2016 01 17
Washington - **As the families of Americans celebrate the release of their loved ones held in Iran, the authorities in Tehran said they would not be freeing a businessman arrested in October and were silent on the fate of a former FBI agent who disappeared in the country**. It was unclear why Siamak Namazi, 44, an Iranian American based in Dubai, was arrested in October while visiting a friend in Tehran where he had done consultant work over the previous decade. Namazi is the son of a prominent family in Tehran who couldn't be reached. Namazi immigrated to the United States in 1983, and he later returned to Iran after graduating from college to serve in the Iranian military. "I don't know what's going on," said Ahmad Kiarostami, a friend.

More recently though, it's been pretty clear the cat is out of the bag
Motherboard Blog, Joshua Kopstein, 2016 01 17
Washington - **A federal judge has ruled that the FBI must release documents it improperly withheld about StingRays, the now-infamous cellphone mass-surveillance devices that police and federal agencies have deployed in secret for decades**. The judgment comes courtesy of Daniel Rigmaiden, a reclusive former tax fraudster-turned-government transparency advocate who first exposed the StingRay's existence after being busted by one in 2008. Initially writing appeals while imprisoned on fraud charges, Rigmaiden has worked for years sleuthing out the secretive devices, resulting in revelations of their use by dozens of agencies and police departments across the country. Rigmaiden was released on probation in 2014 after taking a plea deal. Now the federal judge working Rigmaiden's FOIA lawsuit has ordered the FBI to release 8 additional StingRay documents, saying the information was "not properly withheld."

The agency had tried to hide the documents, invoking the broadly-written Exemption 7(E), which can exclude records that might reveal "techniques and procedures" used in law enforcement investigations.

Ex-CIA Operative Faces Italian Prison Term
Wall Street Journal, Patricia Kowsmann and Manuela Mesco, 2016 01 16
Washington - **A Portuguese court has ruled that a former U.S. Central Intelligence Agency operative convicted in Italy for kidnapping under the U.S. rendition program should be turned over to Italian authorities to serve a seven-year prison sentence. Sabrina de Sousa**, a dual citizen of the U.S. and Portugal, was briefly detained at Lisbon's airport in October while preparing to board a flight to India. Her Portuguese lawyer, Manuel Magalhaes e Silva, confirmed the court's ruling Friday and said she would be allowed to remain in Portugal while appealing it. "Unexpected," Ms. de Sousa wrote via Twitter early Friday after learning of the ruling. Ms. de Sousa and 25 other Americans, mostly CIA agents, were tried and convicted in absentia by an Italian court in 2009 for participating in the 2003 kidnapping of Egyptian cleric Osama Mustafa Hassan Nasr, also known as Abu Omar, on a street in Milan. The CIA and Italian police considered the cleric to be a recruiter for al Qaeda. Italian magistrates said Ms. de Sousa and others gave logistical support to the operation

Ex-CIA chief in Benghazi breaks silence to dispute film
Washington Post, Adam Goldman Greg Miller, 2016 01 16
Washington - **It is the most fateful moment in a movie that purports to present a searingly accurate account of the 2012 attacks that left four Americans dead in Benghazi, Libya**: a scene in which the highest- ranking CIA operative at a secret agency compound orders his security team to "stand down" rather than rush off to rescue U.S. diplomats under siege less than a mile away. **According to the officer in charge of the CIA's Benghazi base that night, the scene in the movie is entirely untrue**. "There never was a stand-down order," said the **base chief known as Bob**, speaking publicly for the first time. "At no time did I ever second-guess that the team would depart." Nor, he said, did he say anything that could be "interpreted as equivalent" to an order to stand down. In a lengthy interview with reporters from The Washington Post, Bob provided new details about the attacks and his interactions with J. Christopher Stevens, the U.S. ambassador to Libya who perished in them. The account from the CIA base chief adds a critical and previously missing voice to the public record on Benghazi, an attack that even three years later remains so politically charged that Sen. Ted Cruz (Tex.), a Republican presidential candidate, made it the center of his closing remarks during this week's GOP debate.

A News Agency With Scoops Directly From ISIS
New York Times, Rukmini Callimachi, 2016 01 15
New York - The San Bernardino shootings. The killing rampage this week in a Baghdad mall. On Thursday, it was the explosion that ripped through a Starbucks in Jakarta. **In each of those terrorist attacks, an outlet called the Amaq News Agency was first with the news that the Islamic State was going to claim responsibility. The agency has been getting the scoops because it gets tips straight from ISIS,** and for those of us on the terrorism beat, that has made Amaq a must-read every time a bomb goes off. It publishes a heavy stream of short releases on an encrypted phone app called Telegram, functioning much like an official news agency might inside a totalitarian state. The alerts, articles and videos take on the trappings of mainstream journalism, with "Breaking News" and "Exclusive" headings. And its reporters try to appear objective, toning down the jihadist hyperbole ISIS uses in its official releases. (The

Jakarta attackers were "Islamic State fighters" rather than the ISIS-preferred "soldiers of the Caliphate."

Secretary of Defense Lauds Push Against ISIS
New York Times, Michael S. Schmidt, 2016 01 14
Fort Campbell, Ky. - **Defense Secretary Ashton B. Carter provided an upbeat assessment on Wednesday of the Obama administration's efforts to defeat the Islamic State** and said that **missions now underway by a new deployment of Special Operations forces are "generating a virtuous cycle of action" against the extremist group**. Mr. Carter's speech here to troops set to deploy to Iraq came as the Obama administration tried to convince an apprehensive public that it has an effective strategy to destroy the Islamic State, also known as ISIS or ISIL. Mr. Carter lauded Iraqi security forces who, aided by American airstrikes, reclaimed the western city of Ramadi from the Islamic State last month as the latest example that the United States and its allies have the right approach. The defense secretary also said other measures -- cutting off the Islamic State's supply routes, destroying its oil fields and disrupting its finances -- "are significantly constraining its ability either to defend or attack." "We have not only gathered momentum but done even more, and are now pressuring ISIL in Iraq and Syria on more fronts than at any other point in the campaign," Mr. Carter said.

U.S. official sees more cyber attacks on industrial control systems
Reuters, Staff report, 2016 01 14
Miami - **A U.S. government cyber security official warned that authorities have seen an increase in attacks that penetrate industrial control system networks over the past year**, and said they are vulnerable because they are exposed to the Internet. Industrial control systems are computers that control operations of industrial processes, from energy plants and steel mills to cookie factories and breweries. "We see more and more that are gaining access to that control system layer," said Marty Edwards, who runs the **Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Tea**m, or ICS-CERT. ICS-CERT helps U.S. firms investigate suspected cyber attacks on industrial control systems as well as corporate networks.

Ex-CIA boss: ISIS gaining affiliates 'faster than Al Qaeda ever did'
Fox News, Staff report, 2016 01 12
Washington - **The Islamic State's web of affiliates is growing faster than Al Qaeda's ever did, a former top CIA official told Congress on Tuesday - on the heels of yet another attack blamed on ISIS. Michael Morell**, President Obama's former deputy and acting CIA director, issued the warning in testimony to the House Armed Services Committee. He said the number of militant groups now swearing allegiance to ISIS has grown to cover nearly 20 countries, from practically "nothing" a year ago. "ISIS has gained affiliates faster than Al Qaeda ever did," Morell said. The Islamic State's web of affiliates is growing faster than Al Qaeda's ever did, a former top CIA official told Congress on Tuesday - on the heels of yet another attack blamed on ISIS. Michael Morell, President Obama's former deputy and acting CIA director, issued the warning in testimony to the House Armed Services Committee. He said the number of militant groups now swearing allegiance to ISIS has grown to cover nearly 20 countries, from practically "nothing" a year ago. "ISIS has gained affiliates faster than Al Qaeda ever did," Morell said.

Ex-spy chief: Ukrainian cyberattack a warning sign for US utilities
Christian Science Monitor, Paul F. Roberts, 2016 01 13
Washington - **Former National Security Agency chief Gen. Michael Hayden warned that a**

recent malware attack on the Ukrainian power grid is yet another troubling sign that the US electric supply is vulnerable to hackers. The Dec. 23 attack on utilities serving the Ivano-Frankivsk region of Ukraine appears to be the second confirmed incident of a computer-based attack to damage physical infrastructure. The attack led to blackouts throughout the region for several hours before power was restored. The Stuxnet worm that targeted the Iranian nuclear program is the only other such incident. What happened in Ukraine is a harbinger for the kinds of cyberthreats the US faces, possibly from rival nations such as Russia and North Korea, the retired Air Force general told a crowd of critical infrastructure experts at the S4x16 security conference in Miami.

Hacker claims to tap into intelligence chief's email
Washington Post, Ellen Nakashima, 2016 01 13
Washington - **One of the hackers who boasted last fall of breaking into the private email account of the CIA director apparently has struck again - this time targeting the director of national intelligence**. A prankster who goes by the nickname "Cracka" told a reporter for the online magazine Motherboard that he had broken into a series of accounts linked to National Intelligence **Director James R. Clapper**. They included Clapper's home telephone and Internet, his personal email and his wife's Yahoo email account, according to the site, which is owned by Vice. The reporter, Lorenzo Franceschi-Bicchierai, said Cracka provided him with screenshots of some of that material but not Clapper's personal email. A spokesman for Clapper, Brian Hale, said the Office of the Director of National Intelligence was "aware of the matter and reported it to the appropriate authorities." The FBI is investigating.

Teen Who Hacked CIA Email Is Back to Prank US Spy Chief
Motherboard (Vice), Lorenzo Franceschi-Bicchierai, 2016 01 12
New York - **One of the "teenage hackers" who broke into the CIA director's AOL email account last year hasn't given up targeting government intelligence officials**. His latest victim is the **Director of National Intelligence James Clapper**, Motherboard has learned. A group of hackers calling themselves "Crackas With Attitude" or CWA made headlines in October, hacking into CIA Director John Brennan's email account and apparently getting access to several online tools and portals used by US law enforcement agencies.The hackers' exploits prompted the FBI to issue an alert warning government officials of their attacks. One of the group's hackers, who's known as "Cracka," contacted me on Monday, claiming to have broken into a series of accounts connected to Clapper, including his home telephone and internet, his personal email, and his wife's Yahoo email. While in control of Clapper's Verizon FiOS account, Cracka claimed to have changed the settings so that every call to his house number would get forwarded to the Free Palestine Movement. When they gained notoriety last year, Cracka and CWA claimed their actions were all in support of the Palestine cause. "I'm pretty sure they don't even know they've been hacked," Cracka told me in an online chat. But Brian Hale, a spokesperson for the Office of the Director of National Intelligence, confirmed the hack to Motherboard on Tuesday. "We're aware of the matter and we reported it to the appropriate authorities," Hale said, declining to answer any other questions on the record. (The FBI declined to comment.)

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

MI5 is voted best place to work for homosexuals
The Daily Telegraph, Tom Whitehead, 2016 01 19
London - **MI5 has been named Britain's most gay-friendly employer, only 25 years after homosexual candidates were first allowed to apply**. The security service, which has a "reverse mentoring" scheme that matches straight managers with junior gay staff, topped the index of the best 100 employers for lesbian, gay, bisexual and transgender (LGBT) equality compiled by the charity Stonewall. The domestic intelligence agency has appeared on the list since 2012 and was ranked seventh last year. **It jumped to first place thanks to an increased commitment to diversity, holding events to improve awareness of LGBT issues and sharing ideas with GCHQ and MI6.** The ban on homosexual people working for MI5 persisted until the early Nineties, long after male homosexual acts were decriminalised in 1967. But these days the reality of being a spy in Britain is very different from the macho, womanising James Bond stereotype. Initiatives at MI5 include an active LGBT network, which meets socially and formally to improve diversity, and having an LGBT "champion" on the board who promotes equality.

Inquiry into foreign backers of UK extremists gets green light
The Observer, Mark Townsend, 2016 01 17
London - **David Cameron has authorised an investigation into the foreign funding and support of jihadi and extremist groups in the UK**, a development that could lead to a potential standoff with the government's key Gulf ally Saudi Arabia. Political pressure on Cameron to investigate extremist revenue streams in the UK has come from the Liberal Democrats who requested the inquiry in exchange for supporting the extension into Syria of British airstrikes against Islamic State. The Home Office's new extremism analysis unit has been directed by Downing Street to specifically examine the scale and origin of funding of extremist groups in the UK with a remit to follow overseas funding streams. Home Office sources would not give details on the level of resources which will be assigned to the inquiry. Its findings will be sent directly to the home secretary Theresa May and Downing Street this spring. The Gulf kingdom has repeatedly been accused of funding mosques and groups with links to Islamist terrorism in the west. Last month Angela Merkel's deputy, Sigmar Gabriel, told the Bild am Sonntag newspaper that the Saudi regime posed a danger to public security through its support for Wahhabi mosques around the world. Wahhabism, a fundamentalist form of Islam practised in Saudi Arabia, has been identified by the European parliament as a driver of global terrorism.

A former MI5 agent told us why it's so easy for Islamic State terrorists to move around without being noticed
Business Insider, Jim Edwards, 2016 01 17
Interview: **One of the most depressing aspects of the appearance of a "new Jihadi John" video is that the man killing the prisoners in the video, Siddhartha Dhar, was known to UK security services before he fled to Syria** and had even been arrested by British police before being let go on bail. Dhar had also repeatedly shown up at Islamic extremist rallies in the UK and had appeared on TV advocating the terrorist cause. This is not unusual. The first "Jihadi John," Mohammed Emwazi, escaped from the UK to go to Islamic State/ISIS/Daesh even though he was known to MI5 and was on the Home Office Warnings Index. The ringleader of the Paris attacks, Abdelhamid Abaaoud, entered and left the UK before planning the attacks. And five other Islamists linked to Dhar left the UK undetected in the months prior to Dhar's execution video. So why is the UK so bad at keeping tabs on terror suspects? Business Insider has noted before that the job is more complicated than it sounds, even after the suspect has been identified. In France, for instance, former French intelligence counterterrorism chief Louis Caprioli estimated that it takes 18 to 20 officers to keep an eye, 24 hours a day, on any one suspect. **There are 6,000 employees at GCHQ and 4,000 at MI5. But there are up to 3,000**

suspects in the UK. At the French ratio, you would need 60,000 officers to track them all. That's almost half of Britain's total number of police officers, 127,000 (PDF). It's an impossible job. So we asked a former MI5 operative, Annie Machon, how they do it. Machon was once responsible for monitoring IRA suspects in the UK in the 1990s.

Trident is old technology': the brave new world of cyber warfare
The Guardian (London), Julian Borger, 2016 01 16
London - Forget debates about Britain's nuclear deterrent. **New technology means a country can be brought to its knees with the click of a mouse. The naval base at La Spezia in northern Italy is in an advanced state of decay. The grand Mussolini-era barracks are shuttered; the weeds won their battle with the concrete some time ago**. But amid the crumbling masonry, there is an incongruously neat little building, shaded behind a line of flags, with smartly outfitted security men behind its glass doors. This is **Nato's Centre for Maritime Research and Experimentation (CMRE).** As one battleship after another has been removed from what remains of the Italian navy, and the base is wound down, the centre is preparing for a new kind of marine warfare amid the wreckage of the old. In a line of workshops along the quay, technicians tinker at the innards of the next generation of naval weapons. They may look like large bright yellow torpedoes, but they are in fact underwater drones, capable of being remote controlled on the surface and taking autonomous actions in the deep. But the technicians here insist they are working on the state of the art.In the wake of criticisms that the UK's cyber fortifications are inadequate, **George Osborne announced in November that the government would spend nearly £2bn on cyber defence and establish a National Cyber Centre, led by GCHQ.** As well as data collection, mass surveillance and monitoring terrorist threats, the UK is prepared to carry out offensive operations. Officials say these might include infecting and disconnecting enemy computers, or creating "real world effects" by targeting computer systems that control civilian infrastructure - the power grid, for instance.

Snooper's charter: cafes and libraries face having to store Wi-Fi users' data
The Guardian (London), Alan Travis, 2016 01 14
London - **Coffee shops running Wi-Fi networks may have to store internet data under new snooping laws**, Theresa May has said. Small-scale networks such as those in cafes, libraries and universities could find themselves targeted under the legislation and forced to hand over customers' confidential personal data tracking their web use. The home secretary has also given her first hint that the costs of her snooper's charter are likely to go far beyond the official £240m estimate. May told peers and MPs that talks were under way with internet and phone companies over costs and their technical capacity to deliver the measures, after being told that Vodafone, O2 and EE had testified that each company could each spend that amount alone in implementing the proposed surveillance law.

Met chief cannot say if more terror suspects skipped bail
London Daily Telegraph, Tom Whitehead, 2016 01 14
London - **The head of Scotland Yard admitted yesterday that he had no idea if more terrorism suspects have fled police bail after he ordered an urgent review**. Sir Bernard Hogan-Howe, the Metropolitan Police Commissioner, has ordered officers to review dozens of bail cases to check if any others have "slipped through" in the wake of the blunders that allowed Siddhartha Dhar to escape. The Londoner fled to Syria in 2014 after failing to surrender his passport while on police bail but officers did not realise for up to six weeks. **The former bouncy castle salesman is now suspected of being Isil's new "Jihadi John", who fronted a recent video in which prisoners were killed.** On Tuesday, David Cameron pledged to toughen up the

police bail system after Mark Rowley, the Met's counterterrorism chief, branded it "weak" and "toothless". Mr Rowley said around 110 terrorism suspects are on police bail.

Colin Duffy 'targeted in Majorca MI5 sting operation'
BBC News, Staff report, 2016 01 14
London - **High-profile dissident republican Colin Duffy was allegedly targeted in an MI5 sting operation in Majorca, a court has been told**. An agent said he posed as a holidaying Serbian businessman with criminal links in a bid to secretly record discussions about potential arms dealing. Another operative acted as his girlfriend during the assignment aimed at securing an encounter with Mr Duffy. A hearing took place to decide if he is to stand trial on terror charges. Mr Duffy is accused of directing and belonging to an IRA grouping, and attempting to murder members of the PSNI. He faces further counts of possessing firearms and ammunition, and conspiring with Alex McCrory and Henry Fitzsimons to murder security force members.

Russian whistleblower may have spoken to MI6 before his death, court hears
The Guardian (London), Luke Harding, 2016 01 14
London **- A Russian whistleblower may have "talked to Britain's spy agencies" before his mysterious death in November 2012, when he was possibly poisoned by a lethal fern, a coroner's court has been told**. Alexander Perepilichnyy collapsed and died outside his luxury home in Weybridge, Surrey, after he had been out jogging. He was 44. Surrey police insist there are no suspicious circumstances surrounding his death. Previous hearings, however, have heard that faint traces of a rare and deadly Himalayan plant, Gelsemium elegans, were found in Perepilichnyy's stomach. Perepilichnyy was instrumental in exposing a massive alleged money-laundering ring involving the Russian mafia and the Russian state. He provided details of an alleged $230m (£148m) fraud carried out by senior Russian tax officials. The money was allegedly stolen from taxes paid by Hermitage Capital, a hedge fund run by the US-born financier Bill Browder. On Wednesday Hermitage's lawyer, Geoffery Robertson QC, accused Surrey police of covering up vital information. T

UK Home Sec stumbles while trying to justify blanket cyber- snooping
The Register (UK), Alexander J. Martin, 2016 01 14
London - **UK Home Secretary Theresa May was grilled on Wednesday by a Parliamentary committee scrutinizing fresh powers proposed for GCHQ**. Crucially, she was unable to explain to the panel exactly why Blighty's **intelligence services need the ability to carry out mass surveillance on millions of innocent Brits** - which would be strongly authorised if a draft law - the Investigatory Powers Bill (IPB) - is passed. While the joint committee was pleased that **GCHQ's bulk surveillance** and hacking operations are being brought under parliamentary scrutiny for the first time, having previously been effected through royal prerogative, the panel noted that the agency's sweeping powers have yet to be fully justified. The committee specifically asked the Home Secretary to make an operational case for GCHQ's abilities. May replied instead that she wished "to give a greater degree of transparency" to the intelligence agency's efforts, and promised to write in with some more information.

Return to Table of Contents/ Retour à la table des matières

Australia/ Australie

Australia not prepared for cyber war
ABC (Australia), Francis Keany, 2016 01 19

Canberra - **A new report warns Australia is not adequately prepared for cyber war, with the nation "badly lagging" behind overseas counterparts and the Defence Force also at** risk. Research by the **Australian Centre for Cyber Security (ACCS)** said Australian government and civilian organisations were well behind China and the United States, which have gone to great lengths to prepare themselves. The report released by Professor Greg Austin called for a "rapid catch-up in Australian capabilities for military security in the information age", warning Australia's response to the threats that have emerged in cyberspace has been "slow and fragmented". Another report by the ACCS has also warned the Australian Defence Force (ADF) has not done enough to test its ability to ward off cyber attacks against weapons systems. While Australia has relied on the United States for its security needs for the past 60 years, the report warned that support would be limited when it came to cyber warfare. This is despite Australia's involvement in the Five Eyes intelligence alliance. "The reliance by middle powers such as Australia on the United States for extended deterrence may not have as much impact in cyber space as for kinetic operations," Professor Austin said. He said while there was public debate about the future of Australia's naval, air and ground capabilities, there has been "no effort in public by the government to benchmark Australian national security needs in cyber space in the same way".

Airports step up security checks for returning jihadis
The Australian, Dan Box & Jannine Khalik, 2016 01 16
Canberra - **Counter-terrorism teams at Australia's international airports have been "recalibrated" to increase their focus on foreign fighters returning from the warzone in Syria and Iraq, alongside checks for those travelling to join Islamic State**. Australian Border Force chief executive Roman Quaedvlieg said the change, made over the past month, reflected fears that those who returned might bring with them both combat experience and the more radical ideologies the terrorist group promoted. "The focus when the Counter Terrorism Unit was established was on the outbound travel because that was where the foreign fighter problem was manifesting but we've recalibrated," he said. "When they come back in, presumably battle-hardened, more extreme, my fear is that they will form a leadership role in the community." Established in August 2014 with almost $50 million in federal government funding, these units are now based at all eight Australian international airports. Responding to automated alerts on passengers as well as making real-time assessments of potential threats, they play a key role in preventing those travelling to join the roughly 110 Australians thought to be fighting with Islamic State. In December, **ASIO director-general of security Duncan Lewis** said this number appeared to have reached a plateau, while about 40 more Australians were thought to have died on the battlefields of Syria and Iraq.

Return to Table of Contents/ Retour à la table des matières

New Zealand/Nouvelle-Zélande

(Light coverage / couverture légère)

Return to Table of Contents/ Retour à la table des matières

International

China/Chine

College established to fight terrorism
China Daily, 2016 01 18
China's first educational institute of its kind focusing on counterterrorism law has been created at a university in Northwest China, which aims to build a pool of legal experts to help **China combat terrorism**. The institute was set up by the Northwest University of Political Science and Law in Xi'an, Shaanxi province, and is expected to receive its first class of undergraduates in spring semester. "To better fight terrorism under new circumstances, China has an urgent and strategic need for a team of qualified experts who have comprehensive knowledge in the field," Jia Yu, president of the university, said at the launching ceremony for the institute on Saturday. Undergraduate students will get lectures on counterterrorism strategies of China and other countries, along with lessons on religion and ethnic affairs. The institute will also introduce doctoral and master's degree programs in counterterrorism law. China is facing intensified terrorism problems as foreign terrorists and extremist groups have stepped up their efforts to target the country, and an increasing number of domestic attacks were found to have been plotted overseas via the Internet, authorities say. To cope with changes and trends in the fight against terrorism at home and abroad, China enacted its first counterterrorism law in 2015. Unlike counterterrorism institutes at the People's Public Security University of China, the Yunnan Police Officer Academy and Xinjiang Police College, the newly created institute will focus on law and policy studies rather than how to react to terrorist attacks. Graduates of the institute could be advisers on antiterrorism policy at several levels, including the front-line fight and in the central government, Jia said.

Naperville man tied to Chinese intelligence agency became U.S. citizen illegally
Chicago Tribune, Clifford Ward, 2016 01 15
Chicago— A **Naperville man who failed to disclose his past affiliation with the Chinese Communist Party and an alleged tie to the Chinese intelligence service** has been charged with unlawfully becoming a U.S. citizen, federal authorities said Friday. **Lu Lin**, 58, of the 4200 block of Colton Circle, is due to appear Thursday in federal court in Chicago to be arraigned on a charge of obtaining citizenship or naturalization illegally. Lin was indicted this past Thursday, according to the FBI. According to the indictment, Lin provided false information on paperwork he turned in during his process of becoming a naturalized U.S. citizen. In the documents, Lin said he had never been a member of or associated with the Chinese Communist Party and had never used any other names, according to the indictment.But authorities say Lin belonged to the Communist Party from 1987 to 1997. They also allege that he had received identification with his photo but under the name Yung Yeung. That identification belonged to China's Ministry of Public Security, which is that country's national police force and law enforcement agency, the FBI said. Federal authorities allege that Lin used the ID to enter Hong Kong and obtain information that he forwarded to **the Ministry of State Security**. The ministry is an intelligence agency responsible for counterintelligence, foreign intelligence and political security, the FBI said.

Xinjiang drafting 1st statute against religious extremism
China Daily, 2016 01 14
Beijing - **Lawmakers in the Xinjiang Uygur autonomous region will begin to draft a regulation against religious extremism this year, the top regional legislator said on Wednesday**. It will be China's first legislation targeting religious extremism, which has led to a

number of terrorist attacks in the country in recent years. "Drafting local regulations on anti-terrorism and eliminating religious extremism are the main focus of this year's legislative work, which will provide solid legal support for Xinjiang to combat terrorism and religious extremism," said Nayim Yassen, director of the Standing Committee of the Xinjiang Regional People's Congress. Nayim made the remarks on the sidelines of the annual session of the local people's congress in Urumqi, the regional capital. Local lawmakers will also start to draft the practices for implementing the counter terrorism law in Xinjiang this year. They had already begun to draft local anti-terrorism legislation before the National People's Congress passed China's first counter terrorism law in December.

Return to Table of Contents/ Retour à la table des matières

Russia/Russie

SBU says IS supporters recruiting new members in Ukraine
UNIAN (Ukraine), Staff report, 2016 01 18
Kiev - **In Ukraine, there are separate groups of IS ideology supporters, who are engaged in propaganda among people they know and in the recruitment of new members, the relocation of recruited persons**, including those from the Caucasus and Central Asia via Ukraine and Turkey to the Syrian-Iraqi zone for fighting for or against the ISIS. They also provide [recruits] with material and financial support, temporary accommodation and supply [them] with passports and travel documents," the **SBU Security Service** of Ukraine told Gordon. According to the SBU, the recruits include both immigrants from Muslim countries, permanently or temporarily residing in Ukraine, and Ukrainian citizens who do not belong to ethnic groups that practice Islam. "As of today, the SBU has identified 50 people from among residents of Crimea (Ukrainian citizens and foreigners residing in Crimean territory), who are involved in fighting in Syria and Iraq as part of the Islamic State, Al-Nusra Front and related organizations. In addition, the SBU revealed 63 IS supporters from among foreign nationals who have been brought to Turkey through our country," the security service reported. The SBU concludes that Ukraine is considered by IS agents mainly as a zone for supporting terrorists' activity in third countries. At the same time, the security agency does not rule out the possibility of IS terrorist attacks on Ukrainian-based representative offices, enterprises, institutions, organizations and individual citizens of the anti-terrorist coalition.

Ukraine says cyber attack on airport launched from Russia
Reuters, Staff report, 2016 01 18
Kiev - **A cyber attack on Kiev's main airport was launched from a server in Russia, Ukraine's military spokesman told Reuters on Monday, as the state-run Computer Emergency Response Team (CERT-UA) warned of the threat of further attacks**. Malware similar to that which attacked three Ukrainian power firms in late December was detected in a computer in the IT network of Kiev's main airport, Boryspil, last week. The network includes the airport's air traffic control. "The control center of the server, where the attacks originate, is in Russia," military spokesman Andriy Lysenko said by phone, adding the malware had been detected early in the airport's system and no damage had been done. A spokeswoman for the airport said Ukrainian authorities were investigating whether the malware was connected to a malicious software platform known as "BlackEnergy," which has been linked to other recent cyber attacks on Ukraine. There are some signs that the attacks are linked, she said.

America may be doomed to cooperate with Putin
Washington Post, David Ignatius, 2016 01 13
Column - **Russia is emerging as an essential diplomatic and security partner for the United States in Syria, despite the Obama administration's opposition to Moscow's support for President Bashar al- Assad**. Russian-American cooperation on Syria now includes regular diplomatic, **military and intelligence contacts**. Moscow and Washington have evolved a delicate process for "deconfliction" in the tight Syrian airspace, where accidents or miscommunication could be disastrous. Administration officials see working with Russia as the best of a bad set of options. An administration that has had trouble living with Russian President Vladimir Putin, especially after his actions in Ukraine, finds that it can't live without him in Syria. Washington's hope is that Putin will support U.S. efforts to negotiate a cease-fire because he concludes it's the only way to avoid a quagmire. "While we remain skeptical of Russian interests and intentions in Syria, we also believe that they will be an essential part of any political solution to this conflict," one senior administration official explained Tuesday.

Return to Table of Contents/ Retour à la table des matières

Europe

Detained Turkish reporters defiant over espionage claim
BBC News, Selin Girit, 2016 01 19
Istanbul - "We were kept in total isolation for 40 days. We were all alone in our prison cells. This punishment is the same a murderer of five people gets," writes Can Dundar, a prominent Turkish journalist currently behind bars in Istanbul. Mr Dundar, editor-in-chief of the opposition Cumhuriyet daily has been in pre-trial detention for almost two months now, along with his colleague Erdem Gul, the newspaper's Ankara bureau chief. In November, a court in Istanbul charged both journalists with espionage after their reports alleged Turkey's intelligence services were sending weapons and ammunition to Islamist rebels fighting the Syrian regime. Turkish security forces intercepted a convoy of lorries near the Syrian border in January 2014, and Cumhuriyet alleged these vehicles were linked to **Turkey's MIT intelligence organisation**. Alongside the newspaper report was video footage showing police discovering crates of weapons hidden beneath boxes of medicine. The government insisted that the lorries were not carrying weapons to the Islamist rebels as alleged, but bringing aid to Syria's Turkmen minority, a Turkic-speaking ethnic group.

Ex-police chief: MİT was aware of PKK stockpiling weapons in SE
Cihan News Agency (CNA), 2016 01 19
Istanbul - **Former Diyarbakır Police Chief İlyas Burunak has said the National Intelligence Organization (MİT) was aware that the terrorist Kurdistan Workers' Party (PKK) was piling up weapons in southeast Turkey during the settlement process launched in 2012 that aimed to end the country's long-standing Kurdish problem**. The process, launched by the government with the PKK's jailed leader, Abdullah Öcalan, in late 2012, came to an end in late July, with the revival of intense clashes in the region. During the settlement process, a de facto cease-fire was in place. The PKK has traditionally used an attack and leave" tactic. Today, however, PKK terrorists are challenging government forces in urban centers by digging trenches and using heavy weapons. The government has been harshly criticized for allegedly closing its eyes to the PKK's increasing activities in urban areas and the terrorist group's stockpiling of weapons in some tense, southeastern towns, such as Cizre, Silopi, Sur and Nusaybin, during the cease-fire period.

Découverte d'une hotline de l'État Islamique
Le Figaro, Journaliste maison, 2016 01 18
Paris - **La Direction Générale de la Sécurité Extérieure (DGSE) a expliqué dans une note confidentielle rédigée début décembre avoir fait la découverte d'une "cellule d'assistant informatique" de l'État Islamique, révèle RTL**. Cette hotline est disponible 24 heures sur 24 par des "experts informatiques titulaires de diplômes universitaires". Ils distillent des conseils sur la façon de crypter les messages et sécuriser les communications et possèdent un compte Twitter "islamiscate technical" qui forme à l'utilisation des messageries Telegram (Russie) et Threema (Suisse) et des blogs qui offrent des cours à distance. "Il faut être clair, à partir du moment où le cryptage est réalisé correctement de bout en bout, il n'y a pas de parade. Même avec les supers ordinateurs que les uns ou les autres peuvent avoir, on est aujourd'hui sur des logiciels qui utilisent des cryptages importants et le décryptage de ces messages s'avère impossible", l'expliquait ce matin François Paget, secrétaire adjoint du Club de la Sécurité de l'Information Français (CLUSIF) au micro de Damien Delseny, journaliste RTL.

German data surveillance includes Finland
Yle (Finland), Staff report, 2016 01 17
Helsinki - **At least 6 Finnish transit lines were monitored in the mid-2000s by German intelligence agency BND, according to leaked German intelligence documents**. The list was leaked to Austrian politician and member of parliament Peter Pilz, who published the first part the list in May 2015. According to Pilz, the leaked list was around 2005 and was part of the German and American surveillance operation Eikonal. "Operation Eikonal" gathered telephone and Internet data between 2004 and 2008, in co-operation with the American security agency, the **NSA**. The German surveillance list -- 256 foreign transit lines from 31 European countries were monitored -- was made public last October in Slovenia's investigative journalism programme Epilog. At that time, the list brought into light unknown details regarding Finland. According to the list, six transit lines were monitored: Helsinki- Paris, Brussels-Helsinki, Helsinki-Shanghai, Budapest-Helsinki, Helsinki- Luxembourg and Helsinki-Reims. Finnish Security Intelligence Service Supo said that generally speaking, it comes as no surprise if it Finnish lines had been monitored.

France Moves to Better Coordinate Its Antiterrorism Efforts; French intelligence agencies to share information and resources
The Wall Street Journal Online, Matthew Dalton, 2016 01 19
Paris - **France on Thursday said it is moving to increase cooperation between its domestic and overseas intelligence services, pushing to break down bureaucratic barriers that have hindered its efforts to prevent terrorist attacks**. The government has been seeking to bolster its antiterrorism infrastructure since Islamist militants killed 130 people in Paris in Novemberand another 17 a year ago. **A weak point, security analysts say, is the lack of coordination across the multitude of French intelligence agencies, including the police, the country's foreign intelligence service, its counterespionage agency and a military intelligence directorate**.The French government decided “to deepen coordination between interior and exterior intelligence services in France as well as overseas…particularly from transit zones and sanctuaries where terrorists gather who want to commit acts on our territory," President François Hollande's office said after the government's weekly cabinet meeting.France, like other Western governments, is scrambling to gather information on Islamic State's attack planning in Syria, where hundreds of French citizens are still fighting in the ranks of the militant group. France ramped up that effort even before Islamic State operatives from France and Belgium slipped into Europe to sow carnage on the streets of Paris on Nov. 13. That intelligence usually collected by France's main external intelligence agency, the **DGSE**, or by its military intelligence agency. But the information sometimes isn't shared with France's main

domestic intelligence service, the **DGSI**."Information collected overseas is not transmitted systematically and automatically to the DGSI," says Jean-Charles Brisard, president of the Center for Analysis of Terrorism, a French think tank.An investigation conducted by the French legislature in the aftermath of the January 2015 attacks, which left 17 people dead, including 12 at the satirical newspaper Charlie Hebdo, **called for better intelligence cooperation**, in particular between the DGSI and the intelligence service of the French police.

Portuguese court orders that former CIA officer be sent to Italy
Washington Post, Ian Shapiraw, 2016 01 16
Washington - **A Portuguese appeals court has ordered the extradition of a former CIA officer to Italy, where she was convicted in absentia for her role in the rendition of a terrorism suspect and faces four years in prison**. Sabrina De Sousa, a U.S. and Portuguese citizen, traveled in April to Lisbon, where she and her husband spend part of the year. But in October, when she went to the airport to travel to the Indian state of Goa to visit her ailing mother, De Sousa was arrested when authorities saw an alert that she was wanted in Italy. In an interview Friday morning, De Sousa said she was surprised by the court's decision this week and will appeal the ruling to Portugal's Supreme Court. If she loses there, she can tak e her case to the country's Constitutional Court. She will not be sent to Italy until she exhausts her judicial options, she said.

Renseignement antiterroriste : qui fait quoi de la DGSI et de la DGSE ?
L'Opinion, Journaliste maison, 2016 01 15
Paris - **A la suite du conseil national du renseignement (CNR), qui s'est tenu mercredi à l'Elysée, au cours duquel le « pilotage opérationnel quotidien » du renseignement sur le terrorisme visant le territoire national a été explicitement confié au ministre de l'Intérieur, nous pouvons apporter des précisions sur le fonctionnement de la lutte antiterroriste**. Tout d'abord, la **DGSE** ne passe pas sous la « tutelle » du ministère de l'Intérieur, mais le coeur du dispositif tient en une « coopération opérationnelle » entre la Direction générale de la sécurité intérieure et Direction générale de la sécurité extérieure. Les autres services de la communauté du renseignement, qui ont une mission dans le domaine de la lutte antiterroriste (LAT), s'organisent autour de ce « noyau ». Dans la pratique, il existe une « cellule » au sein du ministère de l'Intérieur, où sont présents tous les services du premier cercle (DGSI, DGSE, **DRM**, **DPSD**, **DNRED** et **Tracfin**). La **DGSI** est « le référent, le chef de file, le pilote » de la coordination de la lutte antiterroriste sur le sol national. La DGSE est chargée de la détection et de « l'entrave » de la menace à l'étranger. Dans le langage des services, l'entrave fait référence à l'action clandestine visant à empêcher la commission d'un acte hostile. Dans ce cadre, la DGSE vient en appui à la DGSI lorsque la menace contre le territoire national est détectée à l'étranger.

Dutch spy services unravel 'myth' of life with IS
Agence France-Presse, Staff report, 2016 01 14
The Hague - **Dutch secret services fear as many as 70 Dutch children may be growing up among Islamic State jihadists, warning in a bleak new report about life under such a "totalitarian" regime**. "Life among ISIS, unravelling the myth" was released late Tuesday by **the intelligence services, the AIVD**, in a bid to spell out to families, police and aid workers the true hardships and dangers facing those who travel to Iraq and Syria. It paints a stark picture of life under a regime where "violence is inherent", new male recruits to IS are interrogated for days to ensure they are not spies, and children are routinely taken to watch executions of those sentenced to death by harsh Sharia courts. Thousands of foreign fighters from Western Europe as well as Gulf countries have been attracted to IS ranks in the past two years wanting to

support its goal of establishing an Islamic caliphate stretching across Iraq and Syria and beyond. Among them are more than 200 Dutch nationals, including about 50 women.

L'agresseur de l'enseignant à Marseille se dit " très fier " de son acte
Le Monde, Soren Seelow, 2016 01 14
Marseille - **Le jeune lycéen turc d'origine kurde qui a agressé à Marseille un enseignant juif à l'aide d'une machette, lundi 11 janvier, devait être présenté dans la journée de mercredi à un juge antiterroriste en vue de sa mise en examen pour " tentative d'assassinat aggravée en raison de l'appartenance à une religion et en relation avec une entreprise terroriste "**. Sa garde à vue n'aura duré que quarante-huit heures, contre un maximum prévu de quatre-vingts heures en matière de terrorisme, en raison de son âge : il aura 16 ans dans quelques jours. Le parquet a requis son placement en détention provisoire dans un établissement pour mineurs. Durant sa garde à vue, ce lycéen scolarisé en 2de dans un lycée professionnel des quartiers est de Marseille s'est montré particulièrement vindicatif. " Il a revendiqué son acte, dont il s'est dit très fier , explique une source proche de l'enquête. Il tient des propos cohérents, particulièrement haineux à l'égard des juifs et des mécréants. Son seul regret est que sa victime ne soit pas morte. Il se présente comme un partisan de l'Etat islamique, qu'il a découvert sur Internet. " Le jeune homme, qui prétend avoir agi seul, aurait en outre évoqué son désir de partir en Syrie. L'enquête, confiée à la police judiciaire de Marseille, **à la sous-direction antiterroriste (SDAT) et à la direction générale de la sécurité intérieure (DGSI)**, devra déterminer s'il a effectivement tenté de rejoindre la Syrie.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Iranian Intelligence Ministry has thwarted terror acts abroad
Tehran Times, Political Desk, 2016 01 19
Tehran - **The Iranian Intelligence Ministry has thwarted plots of extremist groups against the Islamic Republic in operations abroad**, an MP has quoted Intelligence **Minister Mahmoud Alavi** as saying. "Alavi said the ministry has foiled plots of Takfiri groups hundreds of kilometers away from Iranian borders," Mehr news agency quoted MP Abdolreza Mesri as saying on Monday as he was reporting a closed session with the intelligence minister. During the session, the minister submitted a report to the country's parliament about the ministry's anti-terror activities, Mesri stated. The Intelligence Ministry also neutralized hundreds of anti-Iran operations planned by Takfiri groups at the country's borders, Mesri quoted Alavi as saying. According to the ministry, some reactionary countries in the region are providing financial, military and informational support to Takfiri groups, Mesri further said.

Israel faces no existential threats, says departing Mossad chief
Times of Israel, 2016 01 16
Jerusalem—**Israel is no longer facing any existential threats, Tamir Pardo, the outgoing head of Israel's Mossad intelligence agency**, said in an interview published Saturday. But he warned that the nature of the challenges that the Jewish state must meet has shifted dramatically in recent years. Everyone knows that Israel is a very strong nation. This is no longer a time when Israel, as a young state, is forced to deal with existential fears," Pardo told the Hebrew-language Maariv newspaper. The greatest challenge faced by every head of the organization is to adapt to reality," he said. This is a profoundly different reality to the one that

existed when I was drafted into the IDF in 1971. Then we dealt with entirely different issues, as the threats were different. Hezbollah was an entirely different entity, Iran has completely changed, and even Turkey and Saudi Arabia are not what they once were." Pardo was a Mossad officer who came up through the ranks. A political insider, he served as the radio operator for the late Yoni Netanyahu (the prime minister's brother) during the rescue mission in Entebbe in 1976.

How Gazan Hackers Are Targeting Israelis
Haaretz, Oded Yaron, 2016 01 15
Jerusalem - **The Molerats – a group of hackers from the Gaza Strip who have been targeting Israelis and Israeli websites since 2012 – have recently started using a piece of software that they developed themselves to spy on their targets, according to an Israeli cybersecurity company.** Thus far, ClearSky Consulting and Intelligence Services reported that the Gazan hackers have been using off-the-shelf malware. According to the report, this is the same group of hackers that was responsible for the now infamous Benny Gantz virus, which targeted several government officers in 2012 by using the name of the then-IDF chief of staff. ClearSky experts believe that the group has also been targeting other countries in the Middle East, has links to Hamas and that at least some of its members reside in the Gaza Strip. According to ClearSky, the hackers have been focusing on Israeli military industries, embassies, journalists, banks and public bodies – as well as software developers.

Return to Table of Contents/ Retour à la table des matières

Asia/Asie

Indonesia to Discuss Terror Law Revision at Special Cabinet Meeting
Jakarta Globe, 2016 01 19
Jakarta - **President Joko Widodo is mulling a revision of Indonesia's 2005 Anti-Terrorism Law in order to give law enforcers more authority to prevent attacks, following a bombing and shooting spree in Central Jakarta last week that left people eight, the State Palace said**. According to the Cabinet Secretariat, the president was scheduled to hold a closed-door meeting on Tuesday with senior law enforcement and security officials to discuss a possible revision of the law. Cabinet Secretary Pramono Anung said the meeting would hear suggestions and advice from the relevant agencies as well as discuss the human rights dimension of national security. "Since November, we had suspected, felt and detected extraordinary activities [of terrorists]. But the [Anti-Terrorism] Law, stipulates that there are some steps [in this process] where we are not able to take action," Pramono told reporters at the State Palace. After last week's attack, which was claimed by the Islamic State movement, people have pointed fingers at the **State Intelligence Agency (BIN),** saying it failed to detect the threat before it happened. In his defense, BIN chief Sutiyoso has said his people did detect the threat but lacked the legal authority to take act on it. Four of those killed in the attack were terrorists, the others civilians. Sutiyoso has proposed that intelligence officers also be given the authority to make arrests before an attack happens. Pramono, however, hinted that the president would likely turn down that request, saying that the National Counter-Terrorism Agency (BNPT) and the National Police would continue to lead the country's fight against terrorism. (full article)

Intelligence agent gunned down by motorcyclists in Nimroz
Pajhwok Afghan News, Ramin, 2016 01 19
Zaranj - **Unidentified gunmen have shot dead an agent of the intelligence service in southwestern Nimroz province**, a security official said on Tuesday. The official, who wished to

go unnamed, told Pajhwok Afghan News two motorcyclists opened fire on Mirajuddin late on Monday in the Shuhada Square of Zaranj, the provincial capital. Col. Abdul Hadi Aziz, the crime branch chief, confirmed the shooting and said the local spy network employee was on his way home when gunmen opened fire on him. The assailants managed to flee the scene, but police have launched a search for the killers. It was the third target killing incident in Zaranj in the past one week. (Full Report).

North Korea nuclear test paves way for rare party congress
Reuters, James Pearson and Ju-min Park, 2016 01 19
Seoul - **North Korean leader Kim Jong Un's recent nuclear weapon test was designed to boost his domestic legitimacy ahead of a rare ruling party conference in May that could formalise market-based economic experiments in the isolated country,** analysts say.The Workers' Party Congress, once a regular event, was last held in 1980.Although violent, the years since Kim took power following his father's death in late 2011 have moved the country towards increased stability and a return to a more "formal" way of running the country, said Michael Madden, an expert on the North Korean leadership,"North Korea needed a good result to celebrate at the congress and that was the hydrogen bomb test," **said Lee Cheol-woo, a member of South Korea's parliamentary intelligence committee, citing a briefing by the South's intelligence agency.**

Spy chief's role threatens hopes for Korea peace
London Times, Richard Lloyd Perry, 2016 01 19
Tokyo - **Kim Jong Un, the North Korean leader, has placed a hardline spy chief in charge of relations with South Korea,** in a setback for peace efforts on the peninsula. According to an intelligence report presented to South Korean MPs, Kim Yong Chol was appointed to the job after its previous occupant died in a car crash last month. As head of the general reconnaissance bureau, General Kim is held responsible by South Korea for acts of aggression that have brought the two sides close to war. In 2010 he ordered a submarine attack on a South Korean naval corvette, the Cheonan, which killed 46 sailors. General Kim, 70, was formerly a bodyguard of Kim Jong Un's father, Kim Jong Il. After several years moving up the bureau's hierarchy, he became its head in 2009, the year that other **intelligence agencies** were consolidated under its authority. Intelligence about General Kim's appointment was included in a report by the Yeouido Institute, a think tank affiliated with South Korea's ruling party, the contents of which were leaked to journalists in Seoul yesterday. (Full report).

Sri Lankan intelligence agencies on high alert on possibility of ISIS threat
Colombo Page, 2016 01 18
Colombo - **Following the recent attack in Jakarta by Islamic militants, Sri Lankan intelligence agencies are on high alert on the possibility of local groups having links with the extremist group Islamic State of Iraq and Syria (ISIS),** according to a report in Sunday Observer. Sri Lanka's Ministry of Defense earlier this month assured that the security forces and **all intelligence agencies were on full alert** on the possibility of any groups having links with the ISIS making their appearance in the country. When questioned about the presence of ISIS terrorists or links to sympathizer groups in Sri Lanka, Military Spokesman Brigadier Jayanath Jayaweera has said that the situation is no way a cause for panic or alarm. Brigadier Jayaweera however has declined to provide details saying that divulging vital and sensitive information could be counterproductive to the intelligence network established in the country and could jeopardize identifying the elements. Defense Secretary Karunasena Hettiarachchi recently said that security officials have received information that 36 Sri Lankan citizens have entered Syria secretly and some of them have joined the ISIS.

Rajnath meets intelligence, police officials over IS
Press Trust of India, 2016 01 18
New Delhi - **Top officials of central intelligence and investigative agencies and police of 13 States on Saturday held a meeting with Home Minister Rajnath Singh and discussed steps to check the growing influence of Islamic State (IS) among youngsters through social media and other sources**. Mr. Singh held the meeting to review the situation arising out of some Indian youths getting attracted towards IS and how to deal with the emerging challenge. "The issues that were discussed included misuse of social media, sources of impetus that attract persons, specially youth, to IS, the growth of IS influence in India's neighbourhood and the best possible law enforcement response," a Home Ministry spokesperson said.

Return to Table of Contents/ Retour à la table des matières

Africa/Afrique

Un homme lié aux attentats de Paris arrêté à Mohammedia
La Nouvelle Tribune (Maroc), Journaliste maison, 2016 01 18
Mohammedia, Maroc - **Le bureau central des investigations judiciaires (BCIJ) relevant de la Direction Générale de la Surveillance du Territoire (DGST) a réussi à arrêter, vendredi dernier à Mohammedia**, un ressortissant belge d'origine marocaine en relation directe avec certains auteurs des attentats terroristes perpétrés en novembre dernier à Paris. L'enquête en cours a révélé que le prévenu a voyagé en Syrie à partir de la Belgique en compagnie de l'un des kamikazes de Saint Denis (Paris) pour rejoindre, dans un premier temps, le » Front Al-Nosra » avant de rallier, par la suite, les rangs de l'organisation » Daech » où il a bénéficié d'entrainements militaires sur le maniement de différents types d'armes et sur les techniques de guérilla, avant d'être affecté sur l'un des fronts du conflit, indique un communiqué du ministère de l'Intérieur.

La Tunisie échappe aux opérations terroristes grâce à l'efficacité de son dispositif de renseignement
African Manager, Journaliste maison, 2016 01 12
Tunis - **La Tunisie vit, depuis quatre ans, sous haute menace de déstabilisation terroriste au point que la réactivation du système de renseignement, qui opère à l'abri de toute ingérence politique, est devenue une démarche impérieuse pour protéger le pays**. Il s'agit de l'une des solutions envisagées par plusieurs parties gouvernementales pour remodeler le rôle de l'appareil des renseignements en Tunisie, **s'inspirant en cela de l'expérience de l'Allemagne en matière de renseignements** garantissant à la fois la sauvegarde des droits de l'homme, l'autorité de la loi et la sécurité du pays. Le porte-parole du ministère de l'Intérieur Walid Loughini, a déclaré dans une interview accordée, lundi, à l'hebdomadaire « Assabah Ousboui, que grâce à la réactivation des systèmes de renseignement, la Tunisie a échappé à de nombreuses opérations terroristes.

Return to Table of Contents/ Retour à la table des matières

Americas/Amériques

Nisman's mysterious death: one year later, still more questions than answers
Buenos Aires Herald, 2016 01 17
Buenos Aires— A year later, the mystery remains. Tomorrow marks 12 months to the day when

Alberto Nisman shook the country's political world to its core after he was found in a pool of blood in his apartment, mere days after filing a criminal complaint against former president Cristina Fernández de Kirchner. But the death of the prosecutor in charge of investigating the country's worst-ever terrorist attack continues to be plagued with unanswered questions. The shock wave his death caused around the world continues to resonate at the Pink House. President Mauricio Macri has sent a message to make it clear that he wants to reactivate the investigation into the prosecutor's mysterious death and to thrust the former administration into the heart of the inquiry. On December 16, 2014, CFK shook up the **Intelligence Secretariat** (SI) in an attempt to reduce the power Antonio "Jaime" Stiuso yielded as Operations chief. The decision went largely unnoticed until January 14, when Nisman filed a criminal complaint accusing CFK and her Foreign minister, Héctor Timerman, of having signed the 2013 Memorandum of Understanding with Tehran to whitewash the alleged Iranian involvement in the 1994 attack on the AMIA Jewish community centre. The former administration immediately described the writ as a consequence of Stiuso's anger.

AFI to cooperate with Nisman probe
Buenos Aires Herald, 2016 01 17
Buenos Aires— **President Mauricio Macri yesterday gave the green light for the Federal Intelligence Agency (AFI) to fully cooperate with the criminal investigation into the mysterious death of former AMIA special prosecutor Alberto Nisman**. The move illustrates how the new government is making an effort to relaunch the Nisman probe ahead of the upcoming one-year anniversary of his death on January 18. AFI head Gustavo Arribas yesterday said members of the secret services were free to appear before Judge Fabiana Palmaghini. The agents will be free to provide information as to whether Nisman was being spied on before his death, as the magistrate requested on Wednesday. Palmaghini seems determined to reactivate the case in line with the claims of Nisman's ex-wife, San Isidro Federal Judge Sandra Arroyo Salgado, who has long said that Nisman was assassinated days after filing a criminal complaint against former president Cristina Fernández de Kirchner, accusing her of seeking to whitewash the alleged Iranian involvement in the 1994 attack on the AMIA Jewish community centre.

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

20 01 2016 to/au 26-01-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Mounties use cellphone data in bid to track architects of terrorist attack
Globe and Mail, Geoffrey York, 2016 01 25
Canadian investigators are analyzing cellphone data in an attempt to track down the masterminds of a terrorist attack that killed six Canadians, a senior Burkina Faso cabinet minister says. The comments by Foreign Minister Alpha Barry, in an interview with The Globe and Mail, are the first details of the Canadian role in hunting for the organizers of the brutal attack that killed six Quebec volunteers and 24 other people at a popular restaurant and hotel in Ouagadougou on Jan.15.. **RCMP** officers were swiftly dispatched to Burkina Faso after the attack, but the RCMP would not comment on exactly what the Canadian police are doing. Mr. Barry said the Canadian police are working with French and U.S. investigators and local police. Investigators in white protective suits and masks have been seen combing for clues at the site of the attack, for which a militant group affiliated with alQaeda claimed responsibility.

Télévirements internationaux: les autorités veulent abaisser le seuil de signalement
La Presse, Joel-Denis Bellavance, 2016 01 24
Ottawa - **Pour mieux débusquer les voyageurs à risque qui souhaitent grossir les rangs d'organisations terroristes à l'étranger comme le groupe armé État islamique, les autorités canadiennes jonglent avec l'idée de réduire le seuil à partir duquel les institutions bancaires doivent signaler les télévirements internationaux**. À l'heure actuelle, tous les télévirements internationaux de 10 000 $ et plus doivent obligatoirement être signalés au Centre d'analyse des opérations et déclarations financières du Canada, mieux connu dans les cercles d'enquête sous l'acronyme CANAFE. Mais selon le directeur de cet organisme de réglementation fédéral, Gérald Cossette, des voyageurs à risque peuvent se faufiler entre les mailles du filet en versant des sommes moindres vers l'étranger.

Latin America Takes Action to Control Hezbollah's Activities
Asharq alawsat, Staff Writer, 2016 01 25
Buenos Aries-- **Mexican intelligence, in cooperation with Canadian intelligence services, has recently revealed activities for the Lebanese Hezbollah under Iranian support being detected in Latin America, at Venezuela, Mexico, Nicaragua, Chile, Colombia, Bolivia, Ecuador, in addition to the zone between the Paraguay, Argentine, and Brazil border triad**. George Shea, expert in Middle Eastern affairs and lecturer at the Buenos Aires University, explained that Hezbollah, under Iranian sponsorship, now plans on further expansion following the Russian interference in Syria, in addition to the military Iranian presence that has reduced the need of Hezbollah ground troops in Syria. Authorities in Mexico had already arrested a Lebanese Hezbollah affiliate, on borders with the US, who was caught with fake identification papers and drugs. However, official authorities have yet not disclosed his name for further investigation on Hezbollah's activities there. The Lebanese detainee has confessed to being associated with the Iranian Army of the Guardians and that he was on a mission to collect data on foes of the Iranian government. Moreover, intelligence services in Mexico and **Canadian Security Intelligence Service** revealed that groups affiliated with Hezbollah have begun taking ground action, such as groups of the "Abbas al-Musawi unit" and the "Imad Mughniyah unit". Media pointed out that, during interrogations, the Lebanese detainee had confessed that the two groups' mission is to scout out any threats on Iran in a score of countries across the world and prepare for striking them.

Canadian Embassies Worry They Can't Deal With Earthquakes, Terrorists, and Hackers
Vice News Canada, Justin Ling, 2016 01 23
Ottawa - **Diplomats have told Justin Trudeau that Canada's embassies don't have the funding necessary to deal with terror or cyber attacks, according to memos provided to the incoming prime minister.** "Canadian missions abroad face significant and evolving risks at a time when security resources are diminishing," reads the classified note prepared for the new government. It continues that while the foreign affairs department will continue to look after overseas embassies and staff, "there is a direct correlation between resource investments and mission security." And those investments have simply dried up. The report prepared for Trudeau in October specifically singles out "civil unrest and terrorism" as threats to Canada's missions abroad, but it also warns of "violent criminality in large swaths of Latin America and Africa," the risk of "a range of hostile espionage activities" as well as earthquakes, typhoons, and hurricanes. A 2014 request for funding from the **Canadian Security Intelligence Services (CSIS**), leaked by a hacker who claimed to be part of the Anonymous hacker collective, purports to show that the intelligence agency was frustrated by outdated technology infrastructure in Canada's embassies, and was requesting some $20 million in upgrades.

B.C. judge rules against secret hearings for CSIS in terror probe
Canadian Jewish News, Geordon Omand, 2016 01 23
Vancouver - **Canada's spy agency has lost a bid to hold a secret hearing over its involvement in an investigation involving a couple who were later found guilty on terror charges in British Columbia**. B.C. Supreme Court Justice Catherine Bruce has ruled the media and the public will be allowed to attend the hearing that is considering if the RCMP manipulated the couple into carrying out the bomb plot. John Nuttall and Amanda Korody were found guilty for plotting to blow up the B.C. legislature on Canada Day 2013, but the convictions have been put on hold while their lawyers argue the pair was entrapped by police in an undercover sting. The **Canadian Security Intelligence Service** had asked the judge to allow a hearing to be held in camera, arguing that some of the information is so sensitive to national security that only lawyers for the service and the judge should hear it.

Lawyers attempt to pull curtain over terror plot trial
Vancouver Sun, Ian Mulgrew, 2016 01 22
Column - **Call him Bond, not James Bond, OO7, but Superintendent Daniel Bond -- one of B.C.'s top RCMP liaisons with the Canadian Security Intelligence Service**. He joked outside B.C. Supreme Court that he is ribbed about his name by those who know what he does but his involvement and the role of the country's national security apparatus has become the focus of the Canada Day terror plot trial. A poor Surrey couple, John Nuttall and Amanda Korody, were convicted last summer of terrorism offences for planting inert pressure-cooker bombs at the legislature on July 1, 2013. But their lawyers have asked Justice Catherine Bruce to stay the guilty verdicts and release the pair because of police misconduct. Recovering addicts and recent converts to Islam living in a Metro Vancouver basement suite, the common-law couple were entrapped by the **RCMP**, who preyed upon their vulnerabilities, which included daily doses of methadone, the lawyers say. In stunning testimony Wednesday, Bond testified Nuttall was targeted by **CSIS** in 2012 and the agency had an "investigative technique engaged" in early 2013 when they pointed the Mounties at him. "What was the investigative technique CSIS told you they had engaged with respect to Mr. Nuttall at this meeting on Feb. 1, 2013," lawyer Marilyn Sandford innocuously asked.

CSIS asks judge to keep B.C. terror probe details secret
Canadian Press, Geordon Omand, 2016 01 22

Vancouver - **Canada's spy agency is back in court asking that information about its involvement in a British Columbia terrorism probe be kept secret from the public**. For the second time in two weeks, the **Canadian Security Intelligence Service** asked Justice Catherine Bruce of the British Columbia Supreme Court to allow a closed-door hearing into whether the **RCMP** entrapped a couple found guilty in a terrorist bomb plot. John Nuttall and Amanda Korody were found guilty of planting pressure-cooker explosives at the B.C. legislature on Canada Day 2013. The convictions have been put on hold while their lawyers argue the pair was manipulated by police in an elaborate undercover sting. This time, a lawyer representing the Canadian Security Intelligence Service argued some of the information is sensitive enough to national security that part of the closed-door proceedings must also exclude both defence and Crown lawyers, with only intelligence agency lawyers and the judge present. CSIS's argument is that information might be revealed that would risk identifying this alleged human source, which would put both that person and the person's family in danger.

Canada hard-pressed to deliver on offer to aid intelligence in Iraq
Ottawa Citizen, David Pugliese, 2016 01 20
Ottawa - **Defence Minister Harjit Sajjan has been touting the potential for Canada's military to help gather intelligence in Iraq in the battle against Islamic extremists.** But with no recent history of meaningful involvement in Iraq or Syria, a scarcity of Arabic speakers, and a lack of intelligence-gathering equipment such as drones, how much of a contribution can Canada's military make? In late December, Sajjan told journalists that the Liberal government is considering contributing an intelligence capability to the war against the Islamic State, including helping improve the abilities of Iraqi security forces to target extremists. He suggested the Canadian Forces have technology to play this role, but didn't specify whether that would be equipment on the ground or in the air. In other interviews, the minister has said that Canada's intelligence capabilities are second to none and the government was looking at how to increase that in the Iraq war. "While the Canadian Armed Forces does maintain rosters of members with ability in languages other than English and French, we do not specifically track the number of Arabic speakers within the Intelligence Branch," **Defence Department spokesman Evan Koronewski** said in an email. But he added, "all intelligence officers and operators are highly trained and provide commanders with valuable support to decisionmaking, planning and operations." The federal government's electronic spy agency, the **Communications Security Establishment**, could play more of a role, but it is already monitoring phone calls and emails of Islamic extremists.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

How Petraeus avoided felony charges over leak
Washington Post, Adam Goldman, 2016 01 26
Washington - Inside a secure conference room on the sixth floor of the Justice Department in early 2014, top federal law enforcement officials gathered to hear what criminal charges prosecutors were contemplating against **David H. Petraeus**, the storied wartime general and former **CIA** director whose public career had ended about 15 months earlier over an extramarital affair. Attorney General Eric H. Holder Jr. and **FBI Director James B. Comey** listened as prosecutors did a mock run-through of the government's case, a preview of how they would present their evidence to Petraeus's lawyers in order, they hoped, to force a guilty plea. The presentation included felony charges: lying to the FBI and violating a section of the

Espionage Act. A conviction on either carried potentially years in prison. They were also considering bringing the same charges against Petraeus's biographer and former mistress, Paula Broadwell. The government would never file those charges. The plea agreement left some in the Justice Department angry, particularly at the FBI, and some agents have argued privately that it will hamper future efforts to secure prison terms in leak cases. But others in the government defended the deal as the only viable conclusion to a case in which a successful prosecution on the more serious charges was far from certain.

Government background checks still don't require review of social media profiles
Washington Times, Stephen Dinan, 2016 01 25
Washington - The **Obama administration has announced a new set of rules for government background checks -- but still doesn't require a review of applicants' social media profiles**, leaving the government well behind the private sector in vetting high-risk employees. After a series of high- profile bungles, the administration on Friday announced that it was changing the name of the background check investigations agency and revamping the office to which it reports. Key among those changes is giving the Defense Department, which has the biggest need for security clearances and makes up the majority of background checks, a leading role in setting up and running the National Background Investigations Bureau. But the Office of Personnel Management, which oversees background checks, said the bureau's investigators still don't have permission to delve through the social media accounts and profiles of applicants, forgoing a tool that all sides say is becoming more important in the 21st century. Samuel Schumach, an OPM spokesman, said they agree on the need to look at social media, but they haven't worked out how to do that while balancing privacy and accuracy.

U.S. Prisoner Who Stayed in Iran Was F.B.I. Consultant, Expatriate News Service Says (Canada)
New York Times, Rick Gladstone, 2016 01 24
Washington - **An American prisoner recently freed by Iran, but about whom little is known, is a former California-based carpet seller and F.B.I. consultant, a news service run by expatriate Iranian journalists reported on Saturday**. It said Iranian officials might have believed the man had links to the case of **Robert A. Levinson**, an American who went missing in Iran nearly nine years ago. The news service, **Iranwire**, also reported that the prisoner, **Nosratollah Khosravi**, whom it identified by an alternately used name, Nasrollah Khosravi-Roodsari, had left Iran. Mr. Khosravi was the only American prisoner who did not immediately depart the country after a deal to release prisoners was announced a week ago.. If confirmed, the **Iranwire report** would fill in some gaps in what is known about the prisoner release, in which five people, including four Iranian- American dual citizens, were released by Iran, and seven people, including six Iranian-American dual citizens, were released by the United States. Iranwire was created by Iranian journalists living outside the country, which exerts strict controls on the domestic news media. The founders include **Maziar Bahari, an Iranian-Canadian** who was himself a prisoner in Iran. It has maintained numerous contacts inside Iran.

Saudis, the C.I.A. and the Arming of Syrian Rebels
New York Times, Matt Apuzzo, 2016 01 24
Washington - **When President Obama secretly authorized the Central Intelligence Agency to begin arming Syria's embattled rebels in 2013, the spy agency knew it would have a willing partner to help pay for the covert operation**. It was the same partner the C.I.A. has relied on for decades for money and discretion in far-off conflicts: the Kingdom of Saudi Arabia. Since then, the C.I.A. and its Saudi counterpart have maintained an unusual arrangement for the rebel-training mission, which the Americans have code- named Timber Sycamore. Under

the deal, current and former administration officials said, the Saudis contribute both weapons and large sums of money, and the C.I.A takes the lead in training the rebels on AK-47 assault rifles and tank-destroying missiles.

Clues Emerge on Robert Levinson, C.I.A. Consultant Who Vanished in Iran
New York Times, Barry Meier, 2016 01 23
Washington - **When the United States and Iranswapped prisoners last week, nothing was said to resolve the mystery about another captive: Robert A. Levinson, a Central Intelligence Agency consultant who disappeared in Iran in 2007**. Iranian leaders have long said that they knew nothing about the missing American, and United States officials have said that he may no longer be in Iran -- or even still alive. Aside from a hostage video and photographs of him in an orange jumpsuit five years ago, there had been no public clues about his fate. But newly disclosed documents suggest that Iranian officials knew far more about Mr. Levinson.

Senators To Obama: The CIA Owes Us An Apology And You Know It
BuzzFeed News, Ali Watkins, 2016 01 21
Washington - **Three U.S. Senators are renewing their calls that CIA Director John Brennan cop to spying on Senate Intelligence Committee computers two years ago** -- and this time, they're going above the spy chief's head. In a letter sent to the White House Thursday, Democratic Sens. Martin Heinrich, Ron Wyden and Mazie Hirono, all members of the Senate Intelligence Committee, asked President Barack Obama to step in on the Senate's behalf and force the spy chief to, if not apologize, at least acknowledge that the search was wrong. "We believe it is necessary for you to address this matter directly, and to ensure that senior officials in your administration recognize the importance of adhering to the rule of law," the letter reads. "We ask that you instruct Director Brennan to acknowledge that the CIA's unauthorized search of Senate files was improper and will not be repeated."

NSA Chief Says U.S. at 'Tipping Point' on Cyberweapons
Wall Street Journal, Damian Paletta, 2016 01 21
Washington - **The U.S. military has spent five years developing advanced cyberweapon and digital capabilities and is likely to deploy them more publicly soon, the head of the Pentagon's U.S. Cyber Command said Thursday**. Adm. Mike Rogers, who is also director of the National Security Agency, said U.S. policy makers have largely agreed on rules of engagement for when cyberweapons can be used for defense. There is still an open discussion, however, about when cyberweapons should be used for "offense," such as carrying out attacks against a group or foreign country. "You can tell we are at the tipping point now," Adm. Rogers said. "The capacity and the capability are starting to come online [and] really starting to pay off in some really tangible capabilities that you will start to see us apply in a broader and broader way." Still, Adm. Rogers stopped short of specifying how exactly these cyberpowers could be deployed in coming months.

U.S. discloses zero-day exploitation practices
FCW.com (US), Chase Gunter, 2016 01 21
Washington - **The federal government has confirmed that it uses undisclosed software bugs not only in espionage and intelligence gathering, but also in the course of law enforcement activities.** In November 2015, the government released a redacted version of the Vulnerabilities Equities Process, the policy that lets agencies such as the **National Security Agency and FBI** decide whether to announce the flaws to vendors for patching. Just weeks ago, the government argued that acknowledging its exploitation of the software flaws, known as

zero-day vulnerabilities, would damage national security. Now the government has rescinded some of those redactions in its first official acknowledgment of "defensive, offensive and/or law enforcement-related [and] prosecutorial" uses of the vulnerabilities beyond counterterrorism efforts.

NSA Chief Stakes Out Pro-Encryption Position, in Contrast to FBI
The Intercept, Jenna McLaughlin, 2016 01 21
Washington - **National Security Agency Director Adm. Mike Rogers said Thursday that "encryption is foundational to the future," and arguing about it is a waste of time. Speaking to the Atlantic Council, a Washington**, D.C., think tank, Rogers stressed that the cybersecurity battles the U.S. is destined to fight call for more widespread use of encryption, not less. "What you saw at OPM, you're going to see a whole lot more of," he said, referring to the massive hack of the Office of Personnel Management involving the personal data about 20 million people who have gotten background checks. "So spending time arguing about 'hey, encryption is bad and we ought to do away with it' ... that's a waste of time to me," he said, shaking his head. "So what we've got to ask ourselves is, with that foundation, what's the best way for us to deal with it? And how do we meet those very legitimate concerns from multiple perspectives?"

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

MI5 and MI6: time to come clean on torture
The Guardian (London), Richard Norton-Taylor, 2016 01 26
London--A **British newspaper splashed a story saying a former MI5 officer wants to "present explosive new evidence"** that the Security Service knew inmates at Guantanamo Bay were being tortured. The unidentified officer wants to reveal his evidence to the parliamentary **Intelligence and Security Committee (ISC),** it said. We already know from documentary evidence that officers from **MI5** and from **MI6**, Britain's Secret Intelligence Service, were aware British residents and citizens, and other detainees and terror suspects, were being tortured in US jails in Afghanistan before being rendered to Guantánamo Bay. Security and intelligence officers privately discussed how to handle matters they knew would cause problems if disclosed. When did MI5 and MI6 chiefs - and the ministers to whom they are accountable - knew about the torture, and what steps did they take to stop it? The questions still await answers.

This is the KGB news: how the BBC fell for Soviet ring
Sunday Times (UK), 2016 01 24
London - **The BBC was fooled into giving a job to Guy Burgess, a member of the Cambridge Five ring of Soviet agents, at the request of MI5 -- with neither organisation realising that he used the position to betray Britain to the KGB,** writes Nicholas Hellen. His appointment was orchestrated by Anthony Blunt, another of the Cambridge Five and who worked for MI5 during the Second World War, according to newly discovered documents. It was just one example of how Burgess and other traitors ran rings around the BBC as well as the security services in the late 1930s and during the war. They went on to occupy key positions in the Foreign Office, MI5 and the Secret Intelligence Service, or MI6, which they exploited to pass information to the Russians. The revelations appear in Guy Burgess -- The Spy Who Knew

Everyone by Stewart Purvis and Jeff Hulbert which is to be published by Biteback on Wednesday.

The KGB's Dumbest Double Agent: Yevgeni Brik thought he could outsmart his Russian spy-masters. He was terribly wrong. (Canada)
The Daily Beast, Paddy Hayes, 2016 01 24
Analysis: Daphne Park was briefed personally by her Director (probably Shergold) in Wright's house, rather than in London Block, the center of British administration in the city, home also to SIS Berlin station with its hundred members of staff, where her presence might have been noticed. After the barest minimum of niceties he got right down to it. The Service, he said, had a potential source in Moscow and she was to be given the opportunity to handle him. **The source was Yevgeni Vladimirovich Brik**. Brik was a **KGB** illegal, originally from Kiev in the Ukraine, who had been sent to Canada by Moscow Centre in 1951. Aware that border controls between Canada and the U.S. were lax to the point of invisibility, the KGB plan was to use Canada as a staging post for the infiltration of its illegals into the United States, the 'Principal Adversary', Britain being reduced by this time to the status of 'Principal Ally'. The illegals (officers working under assumed identities) were to be used to handle U.S.- based KGB agents such as the 'atom spies'. Brik's life as a 'double' lasted for two years. His every move was monitored more closely than a laboratory mouse as the **RCMP** determined to learn everything possible about **KGB operations in Canada**. The monitoring led to the uncovering of several KGB sources but it was hard-earned: Brik 'the double' was at least as much trouble to his Canadian handlers as Brik 'the illegal' had been to his Soviet ones. Then Brik was recalled to Moscow. This was supposedly to attend a pre-arranged debriefing and to spend some time with his wife. Despite his concerns that he might have been compromised, Brik's hubris encouraged him to go ahead with the visit, convinced he could outwit the KGB's interrogators. **His RCMP controllers weren't so sure, but the opportunity to obtain a fuller picture of KGB operations from inside Russia swayed them**. However the Canadians were not set up to handle Brik while he was in Moscow, so they turned to [Britain's] SIS who had been briefed on Brik from the beginning. SIS had, in theory at least, the capacity to run an agent in the Russian capital and was happy to take over. (Note: Paddy Hayes is the author of Queen of Spies: Daphne Park, Britain's Cold War Spy Master, from which this excerpt was adapted. Copyright © 2016 by Paddy Hayes. Published in 2016 by The Overlook Press, Peter Mayer Publishers Inc. overlookpress.com.)

Russia's spying on Britain is back to Cold War level
London Times, Marc Bennetts, 2016 01 25
Moscow - **The number of Russian spies operating in Britain is comparable or higher than during the Cold War, according to Russia's leading expert on President Putin's security services.** Andrei Soldatov, a Moscow- based journalist and author, said that there were likely to be at least 30 agents in the United Kingdom. Some operate under diplomatic cover while others -- so-called "illegal" agents -- use false identities to pose as British citizens, Mr Soldatov said. A third group of agents are Russian nationals, often businessmen, living openly in Britain. "These people are usually recruited and trained by the Russian security services to gather intelligence," he said. Besides London, towns and cities close to Royal Navy bases are targets, he said. These include Clyde, home to the UK's nuclear deterrent as well as a new generation of hunter-killer submarines, and Devonport, in Plymouth, the largest naval base in western Europe. There are three Russian intelligence services with active agents in Britain: the GRU military intelligence agency, the SVR foreign intelligence service, and the FSB, the main successor agency to the **KGB**.

MI5 officer: I will expose torture secrets
Sunday Times (UK), Sean Rayment, 2016 01 24
London - **A former MI5 intelligence officer is to break ranks with the agency to present explosive new evidence the security service knew inmates at the Guantanamo Bay detention centre were being tortured**. The former senior officer is seeking to give evidence to a parliamentary inquiry about how **MI5** officials witnessed detainees being tortured at Camp X-Ray and Camp Delta -- two of the Guantanamo prisons -- in December 2002. Even though the former officer is trying to get official permission to give evidence, it is thought to be unprecedented for a former member of staff to defy the agency in this way. Senior security sources have told The Sunday Times that the testimony will prove for the first time that MI5 was fully aware detainees at Guantanamo were systematically abused and tortured. Details of the torture were disclosed during a series of toplevel meetings held at Thames House, MI5's London headquarters, when control of the organisation was passing from Stephen Lander, then director-general, to **Eliza Manningham- Buller**, according to intelligence sources. A source has revealed a significant number of highranking officials, including MI5's senior management board, lawyers and senior officers, held confidential "torture" meetings on several occasions during 2002. The former officer, who had access to the country's most important state secrets, is expected to tell the parliamen-tary intelligence and security committee (ISC) that the abuse was conducted by trained interrogators from America's intelligence agency, the CIA.

Litvinenko suspect mocks Britain on TV
London Times, Deborah Haynes, 2016 01 23
London -**The prime suspect in the murder of Alexander Litvinenko will use a television show to mock Britain by documenting the fate of Russian spies who, like his victim, worked for the UK. Andrei Lugovoy** showed no sign of concern hours after he was named as the main assassin by a British inquiry into the death of Litvinenko. The former Russian intelligence officer, who fled to Britain after falling out with his **FSB** bosses, was assassinated in London in 2006. Rather than preparing for a police interrogation as requested by Britain, Lugovoy was getting ready to front the latest series of his Russian television programme, Traitors. The presenter, who is also an MP, was asked if the chosen theme was deliberate. "That's what the series producers wanted me to focus on this time," he told the BBC. The showman gave a defiant response to the outcome of the inquiry, which found that he and Dmitri Kovtun, a former Russian army officer, killed Litvinenko using radioactive polonium-210, on the orders of the Russian state -- a mission that was probably sanctioned by President Putin. Litvinenko became a British citizen just weeks before he was killed at the age of 44 and was an outspoken critic of the Russian president and is believed to have worked for MI6.

FSB links make it highly unlikely Putin would be unaware about plot to assassinate former spy
The Independent (UK), Chris Green, 2016 01 22
London - **It was, the Litvinenko inquiry was told, "rule number one" of life in the KGB: cover your back.** According to former Russian spies and others familiar with the power nexus inside the Kremlin, this motto also explains why it is likely that even the head of the country's security agency would have turned to Vladimir Putin to sign off the decision to murder Alexander Litvinenko. At the time of his death, the head of the **KGB's** successor the **FSB** was Nikolai Patrushev, who served as Mr Putin's deputy at the intelligence agency before taking over when his superior left to become Prime Minister in August 1999. The operation to poison Mr Litvinenko's tea with polonium was probably approved by both men, who had remained close, according to Sir Robert Owen's report. Exactly how much Mr Putin knew about the FSB's day-to-day work at the time - and how much he was involved in dictating what it did - remains unclear, mainly because of the Russian president's obsession with collective solidarity and

confidentiality among his ministers and officials. According to Professor Robert Service, a former professor of Russian history at the University of Oxford who submitted a lengthy report on the Kremlin power structure to the inquiry, Mr Putin has presided over a "severe constriction" in the type of information released about his activities since coming to power. However, some Kremlin observers have claimed that an incident which took place shortly after Mr Putin left the FSB for politics illustrates his willingness to interfere with the agency's often murky work through his friend and former colleague Mr Patrushev.

Snoopers and scrutiny
The Economist, Editorial Board, 2016 01 21
Editorial - **A lot is riding on Britain's attempt to update the law governing the domestic activities of its spy agencies**. The draft bill will make explicit how the electronic-intelligence agency, **GCHQ**, may (with a warrant) plant bugs on computers and other devices, collect and analyse bulk information (such as mobile-phone activity and web-browsing records) and read private messages. Get the details right, and Britain can provide a model of how to balance security and freedom; get them wrong, and centuries of freedom might shrivel. The bill's biggest success is its self-restraint. It does not require firms to weaken the encryption they sell to customers, as politicians in several countries, including Britain, would like. If people want security on the internet, they have no alternative to strong encryption. The agencies have other means of collecting data, including bugging phones and computers. The draft bill is also right to require companies to retain, at least for a time, data about mobile-phone and internet activity that may, subject to a warrant, be of use to future investigations. Intelligence agencies need to be able to look back at the history of a suspected terrorist's contacts and movements. Elsewhere, however, the bill could be better. It rightly strengthens **GCHQ's** powers to pursue terrorists, gangsters and foreign spies.

Of warrants and watchers
The Economist, Staff report, 2016 01 22
Commentary - **Britain's laws on bugging and snooping are out of date. Written in a pre-internet era, they give sweeping powers to the home secretary to authorise the interception and collection of electronic information, and the planting of bugs (in spookspeak, "equipment interference").** Without a stronger legal basis, these powers could fall foul of European judges on human-rights and data-protection grounds. Moreover, until the revelations by Edward Snowden, a fugitive American intelligence contractor now living in Moscow, most people had no idea of the reach of Britain's digital spy agency, **the Government Communications Headquarters (GCHQ)**, and how close its ties are with America's **National Security Agency**. The Snowden revelations infuriated digital-privacy advocates and also alarmed the technology industry, which feels squeezed between government demands and its customers' expectations. The draft bill on investigatory powers going through Parliament attempts to sort out this mess. It follows the failure two years ago of a previous bill, dubbed the "snoopers' charter", and the hurried passage of a stopgap bill that expires this summer. The bill is under scrutiny by a joint committee of peers and MPs, which will report on February 11th. The biggest divide is not over the technicalities of intelligence oversight, but in attitudes to what spies do. Some believe the agencies to be overmighty, beguiling politicians with tales of derring-do and lobbying zealously for their cause in the media.

Litvinenko murder suspect dismisses inquiry as 'nonsense'
The Guardian (London), Luke Harding, Esther Addley, 2016 01 22
London - **The former Russian spy Andrei Lugovoi has denounced the British inquiry that said he was one of the state-directed murderers of dissident Alexander Litvinenko**,

describing it as "**nonsense**". Speaking to the BBC, the former **KGB** bodyguard and **FSB** secret service agent dismissed the findings of Sir Robert Owen, chairman of the inquiry that said President Vladimir Putin "probably" approved the assassination of Litvinenko in London in 2006. Lugovoi said: "I've seen the nonsense conclusions of your judge who has clearly gone mad. I saw nothing new there. I am very sorry that 10 years on nothing new has been presented, only invention, supposition, rumours. "And the fact that such words as 'possibly' and 'probably' were used in the report means there is no proof, nothing concrete against us."

GCHQ spies quashed this phone encryption because it was too good against snoopers
The Register (UK), Kieren McCarthy, 2016 01 22
London - The researcher who discovered that the UK government's phone encryption standard has a huge backdoor installed has made another discovery: **GCHQ's rejection of a better encryption standard because it didn't allow for undetectable spying**. **Dr Steven Murdoch** has updated his original post on the MIKEY-SAKKE standard, developed by UK listening post GCHQ, to include a document from the 3GPP standardization group that was responsible for the 3G mobile phone standard and which also developed the 4G and LTE standards (i.e., what your phone currently uses). That document stems from a meeting back in 2010 and outlines how a representative from the National Technical Assistance Centre (NTAC) - GCHQ's decryption and data analysis arm - worked to reject the MIKEY-IBAKE standard because it could produce a slight delay in people's phone calls when they were being intercepted.

Accused Claims MI6 Offered To Recruit Him, Suspects He Was Also Exposed To Polonium
International Business Times, Sneha Shankar, 2016 01 22
London - **Andrei Lugovoi, one of the men accused of poisoning former Russian KGB agent Alexander Litvinenko in 2006, said in an interview Thursday that British intelligence agency MI6 offered to recruit him before Litvinenko's death**. He said he suspected he was also exposed to polonium- 210, the radioactive poison that killed Litvinenko. The U.K. public inquiry concluded Thursday that Litvinenko was killed by Lugovoi and another KGB agent, Dmitry Kovtun, "probably" on the personal orders of Russian President Vladimir Putin. The inquiry said Litvinenko drank a cup of tea with Lugovoi and Kovtun that was laced with polonium-210, adding that the two agents could have been working on behalf of the **Russian Federal Security Service (FSB). "**Litvinenko died in November 2006, in March-April I was openly offered cooperation [by MI6] and in order to motivate me somehow, I was denied a visa, that was in May 2006. And after I called Litvinenko - I've said this multiple times - I was granted a visa all of a sudden. I have always connected these two events," Lugovoi said during an interview to Rossiya1 network, according to Sputnik News, adding: "They [UK] always gave me visas, and did it with great pleasure before May 2006, when I was denied a visa after the British intelligence MI6 tried recruiting me." In another report by Sputnik News, Lugovoi was cited suspecting that he had also been exposed to polonium-210. "I can suspect that I got it [polonium exposure] together with Litvinenko. But I lived in British hotel, took British flights, met with representatives of the British establishment and only God knows who could have given it to me," Lugovoi said, according to Sputnik News.

Alan Turing, James Bond and London Spy: how MI5 became Britain's most inclusive employer
The Guardian (London), Richard Norton-Taylor, 2016 01 19
Column - **If you had walked past MI5's headquarters in central London earlier today, you might have noticed the rainbow flag flying above the building. It is not the first time - it flew there on the day of London's Pride festival last summer**. But this time it was raised to

mark the accolade of Stonewall's employer of the year: Britain's Security Service came top in the annual Stonewall Workplace Equality Index. The index measures an organisation's work in tackling discrimination and creating an inclusive workplace for lesbian, gay, bi and trans people. MI5 in particular, it might be argued, needs to be inclusive. Much of its work, as it director general Andrew Parker, said, "goes on by necessity out of view". Its employees cannot talk about their work with outsiders. They need a workplace that is tolerant and welcoming, and an esprit de corps that encourages diversity. MI5 now has a LGBT "champion" to promote diversity, an 80-plus-strong LGBT network, and a "reverse mentoring" scheme for staff who want to develop their understanding of diversity. Staff are offered "unconscious bias training". Meanwhile MI6, Bond's employer, uses Stonewall's logo on recruitment ads appealing for people who are "able to get on with diverse groups".

For fsck's SAKKE: GCHQ-built phone voice encryption has massive backdoor - researcher
The Register (UK), Kieren McCarthy, 2016 01 20
London - **The UK government's official voice encryption protocol, around which it is hoping to build an ecosystem of products, has a massive backdoor that would enable the security services to intercept and listen to all past and present calls, a researcher has discovered**. Dr Steven Murdoch of University College London has posted an extensive blog post digging into the MIKEY-SAKKE spec in which he concludes that it has been specifically designed to "allow undetectable and unauditable mass surveillance." He notes that in the "vast majority of cases" the protocol would be "actively harmful for security." Murdoch uses the EFF's scorecard as a way of measuring the security of MIKEY-SAKKE, and concludes that it only manages to meet one of the four key elements for protocol design, namely that it provides end-to- end encryption.

Return to Table of Contents/ Retour à la table des matières

Australia/ Australie

Indonesian government 'using Sydney server for surveillance program'
ABC (Australia), Conor Duffy, 2016 01 26
Sydney - **An Indonesian government agency is using a Sydney-based proxy server to run the notorious spyware FinFisher, according to technology researchers**. The notorious spyware FinFisher, used to infect mobile phones and computers to place targets under surveillance, has been found in a Sydney data centre. A proxy server inside the Global Switch data centre in Ultimo, Sydney is being used to obscure the real user of the spyware, in this case an Indonesian government agency, according to a group of technology researchers. A proxy server acts as an intermediary which protects the identity of its real user. The intrusive spyware developed by Munich-based is sold exclusively to government agencies as a way to "help identify, locate and convict serious criminals". However, there are also well documented cases in which governments have abused the highly invasive spyware by targeting political opponents within their borders and overseas. According to Privacy International FinFisher was recently used by the Ugandan government to gather "hordes of information" on political opponents and "control the media houses". In Bahrain, authorities are accused of using the technology to place three young activists under surveillance whilst they were living in the UK. The trio say as a result of the surveillance they were relentlessly pursued and tortured at the hands of Bahraini authorities. Once deployed, FinFisher is able to remotely control any computer or mobile phone it infects, copy files, intercept Skype calls, and activate a microphone or webcam. It is not clear

which Indonesian government agency is responsible for the proxy server at Ultimo. The ABC approached **ASIO** and the **Department of Defence**, which declined to comment. The ABC also approached Damon Reid, the executive director of the Global Switch data centre, to ask if the company was aware of the FinFisher server.

Digital age makes old-style spying vital
The Australian, Paul Maley, 2016 01 23
Canberra - **Australia's intelligence agencies are increasingly reliant on dangerous forms of intelligence collection, such as the use of informants and physically infiltrating terror cells, as the rise of freely available encrypted messaging apps makes electronic eaves-dropping more difficult**. Police and intelligence agencies are relying more heavily on "humint", or human intelligence, as commercial-grade encryption technology moves into the mainstream and electronic communication becomes harder to find, buried amid ever greater quantities of digital data. Encryption technology has been embraced wholeheartedly by jihadists, in both Australia and in Syria, prompting US **FBI director James Comey** to demand last year that developers of such apps be required to provide a "back door" into the system so that police and intelligence agencies could access them with a warrant. A spokeswoman for Attorney-General George Brandis confirmed that it had become a major problem in Australia. "(Islamic State) and other terrorist organisations are increasingly using encrypted communications and closed networks to spread their propaganda, recruit new members and plan terrorist attacks here in Australia and overseas," she said.

Return to Table of Contents/ Retour à la table des matières

New Zealand/Nouvelle-Zélande

Light coverage/couverture légère.

Return to Table of Contents/ Retour à la table des matières

International

China/Chine

Digital attacks on China critics intensify, says cybersecurity firm
Christian Science Monitor, Jaikumar Vijayan,, 2016 01 26
Washington - **A shadowy hacker group with suspected ties to the Chinese government has increased its attacks on human rights groups and is even targeting the Russian spy agency**, according to a report released Monday. The cybersecurity company Palo Alto Networks noticed a recent upswing in activity in a four-year-old malware campaign dubbed "Scarlet Mimic," a reference to the program attackers use to imitate legitimate software, designed to steal location data and sensitive communications from targeted computers. While the attackers mostly target organizations that support the rights of Tibetan and Uyghur minorities, the unknown group behind the campaign appears to be targeting the **Russian Federal Security Service** and Indian government organizations with targeted phishing attacks. "We do believe there is a government behind this," says Ryan Olson, director of threat intelligence at Palo Alto's Unit 42 research team. "But we don't have any evidence linking China" directly to Scarlet Mimic, he said.

Return to Table of Contents/ Retour à la table des matières

Russia/Russie

Putin's Spokesman Calls Litvinenko Inquiry a 'Quasi- Investigation'
Moscow Times, Staff report, 2016 01 21
Moscow - **Putin's spokesman Dmitry Peskov called the British inquiry into the murder of Alexander Litvinenko -- a former Federal Security Service (FSB) agent poisoned in London in 2006 -- a "quasi-investigation" and said it may "poison" bilateral relations between Russia and the U.K.,** the Interfax news agency reported Thursday. A report into Litvinenko's death based on a public inquiry was published earlier on Thursday. It alleged that Litvinenko was poisoned with highly toxic isotope polonium 210 by two Russians -- current State Duma deputy Andrei Lugovoi and entrepreneur Dmitry Kovtun - that were "probably" acting under the instructions of the FSB, which were "probably" approved by President Vladimir Putin. Russia's Foreign Ministry deemed the inquiry "politically motivated." The Kremlin will not take the inquiry seriously, because it is based on "probabilities" and uses the word "probably," according to Peskov. "Such terms are not allowed in our legal proceedings, or the legal proceedings of other countries, and we can't perceive it as a court's verdict," he was quoted by Interfax as saying. "Russia was hoping for cooperation with the British in investigating this case. Unfortunately, the British froze not only the cooperation, but the dialogue in other spheres, too," Peskov added.

Kremlin does not perceive Litvinenko death investigation results as verdict
ITAR-TASS World Service, Staff report, 2016 01 21
Moscow - **The Kremlin does not perceive as verdict any part of the results of investigation into the death of Russian Federal Security Service (FSB) defector Alexander Litvinenko, Russian presidential spokesman Dmitry Peskov said Thursday**. "Why am I saying 'quasi-investigation' and why can't we perceive that as an investigation?" Peskov told journalists. "Because the talk is about some judgments based on probability, on the use of words 'possibly', 'probably'." He said "such terminology is not allowed in Russian judicial practice; nor is it allowed in court practices of other countries, and it certainly can't be perceived by us as a verdict in any part [of the investigation's results]." According to Peskov, the results of the investigation may be ironically "referred to subtle British humor."

Return to Table of Contents/ Retour à la table des matières

Europe

Prêt à frapper, Daech s'européanise
Le Figaro, Jean-Jacques Mével, 2016 01 26
Paris **- Le groupe État islamique a développé « une nouvelle capacité de combat pour effectuer une campagne d'attaques d'ampleur » concentrée sur l'Europe, et en particulier sur la France, avertit l'agence Europol**. TERRORISME La menace terroriste est immédiate - particulièrement pour l'Hexagone - mais d'un coup, elle paraît aussi bien plus proche. Daech est parvenu à « européaniser » le recrutement de ses tueurs, leur entraînement et peut-être même leur commandement, d'après un rapport rendu public par Europol, l'agence policière qui ambitionne de devenir le **FBI** du Vieux Continent. L'État islamique a développé « une nouvelle capacité de combat pour effectuer une campagne d'attaques de grande ampleur » centrée sur l'Europe « et en particulier contre la France » , explique Rob Wainwright, directeur de l'agence

et ancien du **MI5** britannique. Le terrorisme islamique « peut frapper presque toutes les cibles où il veut, quand il veut » dans des opérations complexes et bien coordonnées. Depuis les attaques du 13 novembre à Paris, rares sont ceux qui peuvent encore en douter. Europol rajoute à l'alarme en évoquant la possibilité d'autres attentats « dans un avenir proche » .

Prominent intelligence officer Gohar Vardanyan celebrates 90th birthday anniversary
Armenpress, 2016 01 25
Yerevan, Armenia—**Prominent intelligence officer, veteran of Russian Foreign Intelligence Service Gohar Vardanyan, who made a big contribution in acquisition of the needed information for the country's national interests and safety, celebrates her 90th birthday** jubilee on January 25, "Armenpress" reports. Gohar Vardanyan was born on January 25, 1926 in Leninakan (Gyumri) city. In the early 1930s, her family moved to Iran. At age 16, she entered her future husband and comrade-in-arms Gevorg Vardanyan's anti-fascist group along with which she lead an active intelligence work.

France: Hollande veut prolonger l'état d'urgence de trois mois
Radio France Internationale, 2016 01 23
Paris - **Le président François Hollande veut prolonger l'état d'urgence de trois mois, jusqu'à fin mai.** L'annonce a été faite par l'Elysée ce vendredi en fin de journée après les entretiens du chef de l'Etat avec les responsables des partis politiques représentés au Parlement et avec qui il a évoqué la question de la révision constitutionnelle. Décrété le 13 novembre au soir après les attentats à Paris et à Saint-Denis qui ont fait 130 morts, l'état d'urgence devait arriver à terme le 26 février prochain. François Hollande souhaite le prolonger de trois mois. Un projet de loi sera donc présenté le 3 février en Conseil des ministres. La décision du chef de l'Etat de solliciter sa prolongation au Parlement a été dévoilée avant la publication du communiqué par le leader du Parti communiste français Pierre Laurent à la sortie de son entretien avec le président de la République.

Les services belges infiltrés par un indic ?
Marianne, Philippe Engels, 2016 01 22
Bruxelles - **Enorme malaise dans le procès d'une filière syrienne : un Marocain en contact régulier avec les renseignements belges accompagnait les candidats au djihad jusqu'au pied même de l'avion.** Aujourd'hui, il s'est évaporé dans la nature... La voiture qui le conduisait à l'aéroport de Bruxelles-National le 20 novembre 2013 s'est arrêtée au dépose-minute. Etape suivante : Istanbul. Muni d'un simple sac et d'un téléphone portable, Murat D. est parti faire le djihad sans trop y croire. Aux flics qui l'ont cueilli à son retour quelques semaines plus tard, à la veille de ses 19 ans, ce jeune Belge d'origine turque a avoué qu'il avait hésité à chaque pas, ou presque, jusqu'au comptoir d'embarquement. Il a donné aux enquêteurs le nom de son convoyeur, le Marocain Abdelkader el-Farssaoui, dont on est sans nouvelles aujourd'hui

Security researcher: Ukraine power grid facing new wave of cyberattacks
The Hill, Katie Bo Williams, 2016 01 22
Washington - **Ukrainian power plants are still facing an onslaught of cyberattacks in the wake of a malware-caused blackout in December, according to a U.S. security firm. "[On January 19th],** we discovered a new wave of these attacks, where a number of electricity distribution companies in Ukraine were targeted again following the power outages in December," malware researcher Robert Lipovsky wrote in a post on the blog We Live Security. But the kind of malware used in this latest wave of attacks is not the same code that left 80,000 people in the western regions of Ukraine without power last month, Lipovsky notes. "What's particularly interesting is that the malware that was used this time is not BlackEnergy, which poses further questions about the perpetrators behind the ongoing operation," he wrote.

NATO, EU poised to assist Ukraine in security service reform
Kyiv Post, Staff report, 2016 01 21
Kyiv - **Security Service of Ukraine (SBU) Head Vasyl Hrytsak and representatives of the NATO Communication Office in Ukraine and the EU Advisory Mission for Civilian Security Sector Reform Ukraine, have agreed during their meeting to create a permanent international advisory group on the SBU reform**. Representatives of the EU Advisory Mission for Civilian Security Sector Reform Ukraine, foreign advisors at the NATO Communication Office in Ukraine, employees of the NATO Centre for information and documentation in Ukraine, and other international organizations will join the group, as well as leading foreign and Ukrainian experts in this field, the SBU press service said in a report. "The main goal is [to organize] expert support of the process of the Security Service reforming by way of holding permanent consultations on improvement of legal regulation, development of an advanced SBU model with consideration of the best political and legal practices of EU member states and NATO, and to lay out an agreed package of proposals (a plan) with regard to stages of the reform," the report says.

Norwegian intelligence chief says Muslim, other immigrants causing challenges
BBC News—via Norwegian news agency NTB, 2016 01 21
Oslo— **PST [Norwegian Police Security Service] chief Benedicte Bjornland fears that increased immigration, especially from Muslim countries, may provide a breeding ground for radicalization, increased conflict in society and bigger right-wing extremist communities.** The warning came at the national conference of Society and Defence in Sweden on 11 January, where the PST chief was one of the openers. "Sharply increasing immigration, especially from Muslim countries, may also bring other challenges with it in the long term. When a large number of asylum seekers come to local communities, this can have unfortunate consequences," Bjornland said from the rostrum, according to TV 2 [commercial television station]. She warned of an increased conflict level, acts of violence and the emergence of right-wing extremist communities.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

You'd be surprised how many animals are arrested for being Israeli spies
Al-Bawaba News, 2016 01 26
Jerusalem— On Tuesday morning, **residents in the southern Lebanese town of Bint Jbeil captured what they claimed was an Israeli spy vulture**. They thought the bird was carrying Israeli spy equipment, but it was released after authorities determined it was not carrying anything dangerous. This is not the first time an animal has been arrested for espionage. There have been numerous incidents in which creatures ranging from rats to Zionist spy ducks" have been detained for their alleged undercover operations. Israel is often the target of these accusations, allegedly using animals to spy on various countries in the Islamic world, including Saudi Arabia and Sudan.

Foreign Ministry Rejects US Media Claims on Presence of Levinson in Iran
Fars News Agency, 2016 01 22
Tehran - **An informed source in the Iranian foreign ministry dismissed media reports claiming that the US retired FBI agent, Robert Levinson, is in Iran**. The source rejected the CNN news channel's claim that Levinson is being held in Iran, and said, "Different US officials,

the latest of whom the White House spokesman, have many times underlined in their remarks that this person has been traced out of Iran." "The Islamic Republic of Iran has done any possible cooperation to help clarify this person's fate based on a humanitarian attitude," the source told FNA on Thursday. CNN quoted US officials who were briefed on the investigation as claiming that FBI investigators believe Robert Levinson, if he is still alive, is being held in Iran despite public statements from US officials in other agencies indicating he may be elsewhere.

Palestinian Intelligence Chief: We Foiled 200 Attacks Against Israelis
Haaretz, Jack Khoury, 2016 01 21
Jerusalem - **The Palestinian Authority has foiled 200 attacks against Israelis in the upsurge in violence that began in October and it will continue its security coordination with Israel, Palestinian intelligence chief Majid Faraj said** in an interview this week with Defense News. Faraj, who is considered very close to Palestinian President Mahmoud Abbas, rarely makes public statements. He told the U.S.-based publication that Palestinian security and intelligence forces also confiscated weapons and arrested about 100 Palestinians during this period. He said was important to keep the Islamic State organization from establishing a base in the West Bank in bringing about the PA's collapse.

Terror Prince: Hezbollah leader's son led terror cell in West Bank, says Shin Bet
Jerusalem Post, Yaakov Lappin, 2016 01 20
Jerusalem - **Security forces announced on Wednesday the foiling of a terrorist suicide bombing and shooting cell based in Tulkarm in the West Bank that was under the command of Hezbollah, and which was set up by the son of Hezbollah chief Hassan Nasrallah**. A total of five Palestinians are in custody on suspicion of joining the Hezbollah terrorist cell, and they were close to launching attacks, according to the **Shin Bet**. The Shin Bet intelligence agency said its investigation found that Juad Nasrallah, the son of Hezbollah chairman Hassan Nasrallah, used online social media networks to recruit Mahmoud Za'alul, a Palestinian resident of Tulkarm, who in turn received instructions on how to recruit other members into the cell. Za'alul, aged 32, acting under Hezbollah instructions received from his handler, a man named only as 'Fadi,' set up an email account through which he received instructions on how to recruit other members of the cell, gather field intelligence, and select targets.

Foreign intelligent services trigger unrest on Iran, Pakistan borders
Islamic Republic News Agency, 2016 01 20
Tehran - **Pakistan Army Chief General Raheel Sharif conferred on Tuesday with the Secretary of the Supreme National Security Council Ali Shamkhani on expansion of border cooperation in dealing with bandits and armed groups**. In the meeting, Shamkhani said such insecurities have roots in the activities of the **intelligent services** of the alien countries. They seek to promote unrest in the region to prevent expansion of economic, commercial and cultural relations and cooperation between the two countries, he said. To seriously deal with the threat imposed by terrorist groups in the region requires collective contribution of the countries in the region, Shamkhani said.

Return to Table of Contents/ Retour à la table des matières

Asia/Asie

Rajnath Singh reviews security situation with NSA, intelligence agencies
India Blooms News Service, Staff Writer, 2016 01 25

New Delhi- **On the eve of the Republic Day, Union Home Minister Rajnath Singh met National Security Advisor Ajit Doval, intelligence bureau and RAW chiefs to review the security preparedness,** reports said. The meeting came just a day after a car of an army officer was stolen from a south Delhi area, sounding an alarm ahead of the Republic Day parade which will be attended by French President Francois Hollande and top Indian leaders. **Intelligence agencies** had already received inputs about the presence of members of terror outfits. The alert has been intensified especially keeping in mind the kind of attack Pakistani terrorists carried out in the Pathankot air base early this month.

Kim Jong-un's father wanted to end hereditary rule, top spy reveals
London Telegraph, Julian Ryall, 2016 01 23
Tokyo—**Kim Jong-il, the former leader of North Korea, planned to end the hereditary system of rule that handed power to his son Kim Jong-un,** a new book by a **top South Korean spy** has revealed. In a move that could have put the hermit nation on a radically different course, the elder Kim planned instead to create a 10 strong-committee that would run the country instead, according to **Ra Jong-yil**, the **former head of South Korea's national intelligence service**."Those close to Kim Jong-il suggested that he should name one of his children as his successor, but he brushed those suggestions aside." In an interview with The Telegraph, Ra Jong-yil, who also served as ambassador to both London and Tokyo, said Kim Jong-il's plans to end the sole system of hereditary succession in the communist world was thwarted by a combination of his sudden death in December 2011, jostling for influence among the 10 chosen members of his committee - and the brazen determination of Kim Jong-un to seize ultimate power.

Govt to focus on terrorism prevention
The Jakarta Post, 2016 01 21
Jakarta— The **government is currently considering several options that may be included in possible revisions to the current antiterror laws**, including one that would prevent jihadists who have fought with the Islamic State (IS) movement abroad from returning to Indonesia. **President Joko "Jokowi" Widodo** said on Wednesday that a provision that would allow authorities to strip the citizenship of Indonesian nationals fighting in foreign lands, would be part of a draft of new policies that aimed to improve terrorism prevention. **National Counterterrorism Agency (BNPT) chief Comr. Gen. Saud Usman Nasution** said that an amendment to the 2003 Terrorism Law would have at least four provisions, including a change in the definition of "treason" that would allow authorities to criminalize individuals who joined radical groups or declared "caliphates" abroad. Jakarta Police chief Insp. Gen. Tito Karnavian backed the proposal, saying that intelligence information should be included as a legitimate form of evidence. Jakarta Police chief Insp. Gen. Tito Karnavian backed the proposal, saying that intelligence information should be included as a legitimate form of evidence. Tito, however, rejected any proposal that would allow the **National Intelligence Agency (BIN)** or the Indonesian military (TNI) to arrest and detain terrorism suspects.

BIN Requests for Broader Authorities
Tempo (Indonesia), 2016 01 21
Jakarta— **Intelligence Agency (BIN) chief Sutiyoso said that he will deliver a proposal requesting broader authority for the Agency to President Joko Widodo, Vice President Jusuf Kalla and cabinet ministers.** "Yes, I will present it," said Sutiyoso on Thursday, January 21, 2016. Sutiyoso requested that BIN should be allowed to detain suspected terrorists. Sutiyoso argued that one of the reasons why terrorists are difficult to eradicate was because BIN has limited authorities. "That's been our weakness all this time," Sutiyoso said. The prohibition for BIN to arrest suspected terrorists is regulated in Law No. 17/2011 on State

Intelligence. BIN is however, allowed to tap communications, inspect flow of funds and gather information about its targets.

Gov't calls for parliamentary endorsement of anti-terrorism bills
Yonhap News Agency, 2016 01 20
Seoul— **The government renewed its call on Wednesday for the parliamentary approval of anti-terrorism bills to protect the lives of South Koreans**, citing growing threats of terrorism both at home and abroad. In addition to the first bill proposed by the government in 2011 following the 9/11 attacks, a number of anti-terrorism bills are currently pending in the National Assembly. However, the bills have not yet been put to a full floor vote due to strong dissent from the opposition party on concerns about giving more authority to the **National Intelligence Service (NIS),** South Korea's top spy agency. "There have been needless battles at the National Assembly for the past 15 years," said Kim Soo-min, a senior NIS official who participated in the government-ruling party meeting. "The anti-terrorism bills are designed to protect the lives of the people and should not be the subject of a bargaining tool."

Book shows regime's darkest side
Korea JoongAng Daily, 2016 01 18
Seoul—**Former North Korean leader Kim Jong-il did not initially plan to pass on his authority to his third son**, Kim Jong-un, according to a book containing accounts by experts with special knowledge of the country. In the book, the author, **former intelligence official Ra Jong-yil**, depicts North Korea's founding father Kim Il Sung as a cold-blooded dictator, who once ordered his confidants to kill his son, Jong-il, if he veered from the country's official ideological line. Ra, 75, previously served as the **former deputy director of the North Korea bureau inside the National Intelligence Service** as well as the national security adviser to the late President Kim Dae-jung. His book, tentatively titled, "The Path Taken by Jang Song-thaek: A Rebellious Outsider," is due to be released by the end of the month. According to copies of its transcript obtained by the Monthly JoongAng, Kim Jong-il, who died in December 2011, told his aides that the power succession would end with him.

Seoul announces new counterterrorism effort
Korea JoongAng Daily, 2016 01 18
Seoul—Authorities in Seoul announced Friday **plans to create a consolidated network involving the police, the military and firefighting forces to boost counterterrorism measures**. The three agencies will "freely share" information on terrorism and enhance communication channels among one another via official liaisons, the Seoul Metropolitan Fire & Disaster Headquarters said. Authorities will also design an instruction manual outlining the roles of each department in case of a terror attack, and a combined practice drill will take place annually on Jan. 21. The first combined drill was scheduled to take place Friday afternoon at a training area for the SWAT team in Seodaemun District, central Seoul. Earlier this week, the **National Intelligence Service (NIS)** announced that 51 people had been deported over the past five years over terrorism allegations, including ties to ISIS.

Return to Table of Contents/ Retour à la table des matières

Africa/Afrique

Athmane Tartag coordinateur des Services de renseignement
El Watan, Mokrane Ait Ouarabi, 2016 01 25
Alger - **Le DRS est renommé Direction des affaires de sécurité**. Le nouveau service, rattaché à la présidence de la République, quitte l'enceinte du MDN pour s'installer dans

l'ancien ministère des Affaires étrangères. La restructuration des services de renseignement passe à une nouvelle étape. Le **Département du renseignement et de la sécurité** (DRS), qui a eu un nouveau chef en septembre dernier, vient d'avoir une nouvelle dénomination. Selon les informations rapportées hier par plusieurs médias électroniques et confirmés par nos sources, un décret non publiable, signé le 20 janvier courant, met ainsi fin à ce sigle qui a accompagné l'Etat algérien pendant 25 ans. Ce service est donc renommé Direction des affaires de sécurité. Le successeur du général de corps d'armée Mohamed Mediène à la tête du DRS, le général-major à la retraite Athmane Tartag en l'occurrence, est maintenu à la tête de cette nouvelle structure sécuritaire qui est également mise sous la tutelle de la présidence de la République comme l'a toujours été le DRS.

Algeria's Bouteflika dissolves DRS spy unit, creates new agency – sources
Reuters, 2016 01 25
Algiers— **Algerian President Abdelaziz Bouteflika has dissolved the long-standing military spy directorate known as the DRS**, creating a new agency under the control of the presidency in another step to ease the military out of politics, security sources said. Bouteflika, rarely been seen in public since he suffered a stroke in 2013, began curbing the military's influence before his re-election in April 2014, in what analysts said was preparation for his eventual departure after more than 15 years in power. But the decree to shut the Department of Intelligence and Security, or DRS by its French initials, and replace it with the Direction of Security Services is a significant move to restructure the intelligence apparatus.

Ultime phase de restructuration des services de renseignement Bouteflika dissout le DRS
L'Expression (Algérie), Brahim Takheroubt, 2016 01 25
Alger - **Le président de la République, chef suprême des armées Les enjeux du moment, la nature des conflits imposent une réadaptation des services de renseignement. L'Algérie veut redonner à la justice, aux droits de l'homme et aux libertés individuelles le rôle et la place majeure qui leur siéent**. Comme attendu par les observateurs avertis, les services de renseignement algériens changent de nom avec l'ultime phase de restructuration. Désormais, Département du renseignement et de la sécurité, le **DRS**, s'appellera la **«Direction des services de sécurité» (DSS)** chapeautée par le général Bachir Tartag. Ce décret qui renomme le DRS en DSS institue ainsi, le poste de Coordinateur des services de sécurité et lui redonne de larges prérogatives. C'est ce que rapportent plusieurs sites électroniques ainsi que les télévisions privées. L'information a été confirmée par des sources sécuritaires crédibles. Ces sources indiquent que la nouvelle structure dont le siège est sis au Golf (celui de l'ancien ministère des Affaires étrangères) sera composée de trois départements chargés respectivement de la «sécurité intérieure, de la sécurité extérieure et d'une direction technique», ajoutant que la DSS, travaillerait en coordination avec la Gendarmerie nationale et la police.

Algérie/Bye Bye le DRS !
Algérie Focus, Abdou Semmar avec Essaïd Wakli, 2016 01 24
Alger - **Comme nous l'avons rapporté il y a de cela plusieurs mois, le DRS est dissout et les services secrets algériens changent d'appellation comme le dicte la restructuration de cet appareil sécuritaire décidée par Abdelaziz Bouteflika**. Une restructuration menée depuis pratiquement fin 2011 et dont les prémices remontent jusqu'à 2008. L'Algérie enterre donc le DRS pour donner naissance à un nouveau service de renseignement dénommé le **Département des Affaires sécuritaires (DAS)**, qui se chargera désormais de centraliser tous les départements chargés du renseignement dans le pays. Athmane Tartag, ancien chef du DRS, a été nommé comme ministre-conseiller chargé du renseignement. C'est lui qui se

chargera désormais de coordonner toutes les actions du renseignement, que cela vienne de l'ancien DRS, de la police ou de la gendarmerie.

Attentats terroristes - Le gouvernement rassure le corps diplomatique (Canada)
All Africa, Journaliste maison, 2016 01 20
Ouagadougou - **Sur instruction du président du Faso et du Premier ministre, des ministres du gouvernement ont rencontré les membres du corps diplomatique présents au Burkina Faso ainsi que les organisations internationales afin d'échanger sur la situation qui prévaut au pays**, avec notamment l'attentat terroriste qu'il a enduré le 15 janvier dernier, l'attaque d'un convoi de gendarmerie dans l'Oudalan et la prise en otage d'un couple d'Australiens survenue à Djibo. Alpha Barry a, par ailleurs, souligné que des mesures urgentes (voir encadré) ont été prises pour assurer la sécurité du Burkina Faso, de ses amis et de ses partenaires. Il a également salué les **Forces de défense et de sécurité (FDS**) burkinabè, les Forces spéciales françaises, les Forces américaines et les **Canadiens** qui sont présents au Burkina Faso pour l'identification des corps.

Return to Table of Contents/ Retour à la table des matières

Americas/Amériques

Let's Change leaders show up at Nisman rally
Buenos Aires Herald, 2016 01 19
Buenos Aires— Thousands of people, including the top ranks of the Let's Change administration, attended a demonstration in Palermo yesterday to commemorate the **one-year anniversary of AMIA special prosecutor Alberto Nisman's death.** The gathering took place at Plaza Alemania, in the Buenos Aires City neighbourhood of Palermo, where participants marked precisely one year since Nisman was found dead in his apartment in Puerto Madero from a single gunshot wound to the head, though speculation since remains rife as to how the man formerly tasked with investigating the 1994 AMIA bombing — the deadliest terror attack in Argentine history — met his end. "Forty million Argentines want to know how did the gun (that killed Nisman) go off and who did it," Ariel Cohen Sabban, the head of the DAIA Jewish organization, said amid strong applause from those in attendance. "How is it possible that after one year of investigations we're nowhere near (the truth)?" the DAIA leader went on. **"We hope statements from intelligence agents may shed some light on this unfair** death. We don't want Nisman to become the 86th victim of the AMIA attack."

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

24-02-2016 to/au 1-03-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

La sécurité doit être une priorité pour Ottawa
Agence QMI, Guillaume Saint-Pierre, 2016 03 01
Ottawa - **Deux anciens hauts fonctionnaires canadiens demandent au gouvernement Trudeau de moderniser la structure du renseignement et de la sécurité afin de mieux protéger les Canadiens de la menace terroriste**. Après avoir essuyé des compressions sous le précédent gouvernement conservateur, les agences de renseignement doivent être à nouveau mieux financées, estiment l'ancien patron de **l'Agence des services frontaliers du Canada (ASFC), Luc Portelance, et un ex-agent du Service canadien du renseignement de sécurité (CSIS), Ray Boisvert.** «Les Canadiens ont besoin d'être rassurés», affirment-ils conjointement dans une publication rédigée pour le compte de l'Institut MacDonald-Laurier et rendue publique lundi. En plus d'injecter des fonds dans les agences existantes, MM. Portance et Boisvert croient qu'il est temps de créer de nouveaux organismes de surveillance. Selon eux, le Canada doit se doter d'un service de renseignement responsable d'épier ce qui se passe à l'étranger, afin qu'il soit moins dépendant du travail de ses alliés. La mise en place d'une agence centrale qui coordonnerait tous les efforts de surveillance canadiens devrait aussi être une priorité, disent-ils.

Money transfer called a 'pre-meditated plan'
Ottawa Citizen, James Bagnall, 2016 03 01
Ottawa - After nearly four years of criminal proceedings against former construction boss **Roland Eid,** the Crown on Monday presented its final submissions. Federal prosecutor Moray Welch said nothing about **Eid's activities as an informant for the Canadian Security and Intelligence Service**, concentrating instead on the financial drama that unfolded in Ottawa's construction industry early in 2008. That's when Eid's firm - ICI Construction - went bankrupt, leaving dozens of creditors on the hook for millions owed. The circumstances, well known by now, still seem bizarre.. Eid has suggested, in interviews conducted before the trial, that the government pushed ICI into bankruptcy at the behest of CSIS, which he claims was upset that he refused to perform a high- risk assignment in Lebanon.

Bewildering case of former spy to hear final arguments
Ottawa Citizen, James Bagnall, 2016 02 27
Ottawa - It's difficult to imagine a stranger set of circumstances and evidence facing an Ontario Superior Court Justice. **Judge Timothy Ray, starting Monday, will hear final arguments from Crown and defence lawyers in a bewildering fraud trial involving Roland Eid - a former spy with the Canadian Security Intelligence Service**. The criminal proceeding, a judge- only affair, began nearly a year ago but has taken several breaks, including a lengthy one to accommodate a key witness with health issues. Eid was charged in 2012 with multiple counts of fraud and forgery in connection with the transfer of $1.7 million from his firm, ICI Construction, to his personal account in Lebanon. Shortly after the cash arrived in his Beirut bank late in 2007, ICI Construction filed for bankruptcy, leaving dozens of creditors on the hook. Evidence at the criminal trial to date has focused on how the money flowed. Witnesses from a variety of financial intermediaries unique to the construction industry offered perspective. But here's the problem facing Ray: So many of the facts in the case are simply unknowable - or involve potential witnesses, including Eid, who were not called upon to testify. Eid has never

denied that the $1.7 million was transferred. At trial, it emerged that he was planning to use the money as startup capital for building projects in Syria.

Sixty linked to terror back in Canada
Agence France-Presse, Staff reporter, 2016 02 25
Sixty Canadians have returned home after travelling abroad to join banned terror groups, while another 180 are still engaged with these organizations, Canada's spy master told a local newspaper. "The total number of people overseas involved in threat-related activities, and I'm not just talking about Iraq and Syria, is probably around 180," **Canadian Security Intelligence Service director Michel Coulombe told the Globe and Mail newspaper**. "In Iraq and Syria, we are probably talking close to 100," he added. An agency official was not immediately available to confirm the figures, which represent a significant jump in the number of Canadians reported to be involved in "terrorist" activities. A 2014 national security report said 130 Canadians overseas were being tracked by CSIS. They are said to be involved in fighting, training, fundraising to support attacks, promoting extremist views and planning attacks. Federal police chief Bob Paulson said the Royal Canadian Mounted Police is keeping tabs on those who have returned to Canada, some of them around the clock. (Full report)

Bring our spies to heel
Toronto Star, 2016 02 25
Editorial: **Just how many Canadians had their personal information handed over to the Americans and other allies when Ottawa's electronic spies dropped the ball a few years ago and unlawfully passed along metadata to foreign security services without scrubbing it first? Was it hundreds, thousands, millions? Jean-Pierre Plouffe**, the commissioner-watchdog for the **Communications Security Establishment**, can't say. Because he doesn't know. "It's impossible to know the exact figure," he told the Senate's national security committee a few days ago. We can only wonder. How long did the **CSE** security breach go on before it was noticed? Was it a year? Two? More? Again, Plouffe is in the dark. CSE "didn't know for how long the problem existed," he told the committee. And just what personal information ended up in the hands of Canada's "Five Eyes" allies, the United States, Britain, Australia and New Zealand? There's no prize for guessing that, either. Plouffe doesn't know. "After a certain time, data disappears," he said. But rest assured, CSE said in a press release after Plouffe addressed the committee, "the privacy impact is assessed as low." Really? CSE, which reports to Defence Minister Harjit Sajjan, is barred by law from targeting Canadians. Yet it passed on a torrent of so-called metadata information and now wants to wave off the breach as small potatoes. If anyone needed more evidence that our security agencies ought to be more transparent and accountable for their activities, this is it.

Une soixantaine de Canadiens liés à des groupes extrémistes de retour chez eux
Agence France-Presse, Journaliste maison, 2016 02 24
Ottawa - Une soixantaine de Canadiens sont revenus dans leur pays après avoir rejoint à l'étranger les rangs d'organisations classées "terroristes" par Ottawa, et 180 autres y sont toujours engagés, surtout en Irak et en Syrie, a indiqué le patron du service du renseignement. "Le nombre total de personnes impliquées à l'étranger dans des activités menaçantes --et je ne parle pas uniquement de l'Irak et de la Syrie-- est probablement autour de 180", a déclaré **Michel Coulombe**, directeur du **Service canadien de renseignement de sécurité (SCRS)**, dans un entretien au quotidien le Globe and Mail de mercredi.

CSIS using new powers to disrupt terrorists since Bill C-51 became law
CBC News, Peter Zimonjic, 2016 02 24

Ottawa - **Michel Coulombe, director of the Canadian Security Intelligence Service, told a Commons committee today that Canada's spy agency has used new disruption powers it was granted when Bill C-51 became law this past summer**. This marks the first time CSIS has publicly acknowledged the use of its new powers under the Anti-terrorism Act to disrupt suspected plots rather than just relay information about those plots to the federal government and the RCMP As an intelligence agency, CSIS does not have powers to enforce the law. Its role has been to relay intelligence to other branches of government. That changed when Bill C-51 became law, giving the spy agency power to actively interfere with suspected terrorists if it has reasonable grounds to think a security threat exists. The disruption powers allow CSIS to interfere with, telephone calls, travel plans and bank or financial transactions. The agency can also disrupt radical websites and Twitter accounts of groups or people inside and outside of Canada. This provision in the act has garnered criticism from the outset, because there is no clear definition of what "disrupt" means in the legislation, causing some to be concerned the power would be abused by police and intelligence services.

Canada's spies expecting a budget boost
Toronto Star, Alex Boutilier, 2016 02 24
Ottawa - **Canada's spies are expecting a budget boost when the Liberals table their first fiscal plan next month, documents released Tuesday show. The Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE) have estimated an additional $95 million for intelligence and cyber defence operations next year**. The figures were released in the government's main estimates document, a best-guess scenario for departments and agencies released a month before the Liberals table their first budget. CSIS expects an additional $35.5 million "in support of Canada's national security and the safety of Canadians." A breakdown of CSIS budget -- grouped vaguely into "intelligence" and "security screening" -- shows most of the increase will go to intelligence operations. CSE, the electronic spying and cyber defence agency, is expecting a net increase of $59.5 million "in support" of its mandate. Specifically, CSE expects to spend the money to increase its "capacity to address cyber threats and advancements in technology." Together, the two spy agencies estimate they'll spend $1.2 billion in 2016-17, a slight increase compared to the 2015-16 estimates of $1.075 billion. CSE spokesperson **Lauri Sullivan** said in a statementthat the funding will go to addressing several "key vulnerabilities" in government networks, as well as moving forward with the national Cyber Security Strategy.

180 Canadiens environ partis faire le djihad
Agence QMI, Journaliste maison, 2016 02 24
Ottawa - **Près de 180 Canadiens ont quitté le pays pour aller combattre en Irak et en Syrie, selon le Service canadien du renseignement de sécurité (SCRS) et la Gendarmerie royale du Canada (GRC)**. Dans un point de presse commun tenu hier matin, à Ottawa, les services de renseignement ont précisé qu'une centaine de ces individus sont allés grossir les rangs du groupe armé État islamique (ÉI). Les directeurs du SCRS et de la GRC ont dit qu'ils utilisaient les outils mis à leur disposition par la loi antiterroriste (C-51) entrée en vigueur en juin dernier. «Est-ce que nous avons utilisé les nouveaux pouvoirs que nous donne la loi C-51? La réponse est oui, a fait savoir le commissaire de la GRC, Bob Paulson. Dans certains cas, nous faisons de la surveillance 24 heures sur 24, sept jours sur sept. Dans d'autres cas, nous travaillons avec des groupes communautaires pour essayer de réintégrer ces jeunes à la société canadienne.»

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

In New York, Apple wins a battle in its legal war with the U.S.
Washington Post, Ellen Nakashima, 2016 03 01
Washington - **A federal judge in New York ruled in favor of Apple on Monday, saying that an obscure Colonial-era law did not authorize him to force the firm to lift data from an iPhone at the government's request**. The ruling is not binding in any other court, but it takes on an outsize importance as the U.S. government battles Apple in a separate case in California over whether the tech firm should help unlock a phone used by one of the shooters in the San Bernardino terrorist attack in December. The two cases involve different versions of iPhone's operating system and vastly different requests for technical help, but they both turn on whether a law from 1789 known as the All Writs Act can be applied to cases in which the government cannot get at encrypted data stored on suspects' devices.

Un nouvel accord recadre l'espionnage américain
Le Temps (Suisse), Ram Etwareea, 2016 03 01
Bruxelles - **Protection de données Les citoyens européens obtiennent de nombreuses garanties et diverses possibilités pour faire recours s'ils s'estiment lésés par des services de renseignement ou des entreprises américains « Safe Harbour »,** le règlement transatlantique en matière de transmission et de protection des données, est mort. Vive « Privacy Shield », qui entrera en vigueur dès qu'il aura obtenu le feu vert des vingthuit Etats membres de l'Union européenne (UE) ainsi que celui du Parlement européen. En gros, les Etats-Unis promettent de moins espionner les citoyens européens. « Notre objectif est d'assurer la protection des droits fondamentaux de nos citoyens et d'apporter une sécurité juridique à nos entreprises », a expliqué lundi un haut fonctionnaire européen. Du côté des Etats-Unis, le président Barack Obama a signé la semaine dernière le Judicial Redress Act qui accorde aux Européens les mêmes droits qu'aux Américains en matière de protection des données. Programme américain d'espionnage à grande échelle ,

Last Batch of Clinton Emails Is Released
New York Times, Steven Lee Myers, Julie Hirschfeld Davis, 2016 03 01
Washington - The **State Department on Monday released the last set of emails from the 30,000 messages on Hillary Clinton's private computer server**, including an email about North Korea that remains a point of dispute between the department and one of the nation's spy agencies over the secrecy of information that passed through the server. That email -- written on July 3, 2009, after a North Korean ballistic missile test -- was one of four that prompted intensified scrutiny of the emails for classified information and a referral last year to the F.B.I. for a review of the handling of classified information by Mrs. Clinton, her aides and other State Department officials while she was secretary of state. It was released as part of a chain of five replies and forwards on Monday with portions blocked out on the grounds that they **contained information now classified "secret," though not "top secret**," the higher classification that the spy agency, the National Geospatial-Intelligence Agency, had cited last summer.

28. Washington; 2002 Letter on Eavesdropping Is Made Public
New York Times, Charlie Savage, Eric Lichtblau, 2016 03 01
Washington - The **Obama administration on Monday made public a previously classified letter from 2002 about the Bush administration's secret program that allowed the National Security Agency to eavesdrop on Americans' international communications without court orders**. The release of the 22-page letter, written by John Yoo, then a top lawyer in the Justice Department's Office of Legal Counsel, adds to the historical record of one of the

most controversial pieces of the Bush administration's response to the terrorist attacks of Sept. 11, 2001: The surveillance and bulk data collection program known by the code name Stellarwind.

Apple's congressional testimony: 'Dangerous precedent' would weaken all iPhones
Washington Post, Andrea Peterson, 2016 02 29
Washington - **Apple's general counsel plans to argue Tuesday on Capitol Hill that the FBI's request to unlock the smartphone used by one of the San Bernardino, Calif. terrorists would set "a dangerous precedent" of the federal government ordering a company to weaken the security of its own products, according to a copy of his testimony obtained by The Washington Post.** Bruce Sewell, the general counsel, plans to say that Apple has "no sympathy for terrorists." But he will argue that once the iPhone is weakened in this way, hackers and cyber criminals could wreak havoc on the personal safety and privacy of the hundreds of millions of people who own an Apple device. "They are asking for a backdoor into the iPhone," Sewell's testimony states. "Building that software tool would not affect just one iPhone. It would weaken the security for all of them.... We can all agree this is not about access to just one iPhone." Sewell's testimony also states that FBI **Director James Comey** has acknowledged that the FBI would likely use the precedent in other cases involving iPhones.

Pentagon chief to appeal to Silicon Valley for help with cybersecurity
Los Angeles Times, W.J. Hennigan, 2016 02 29
Los Angeles - **Defense Secretary Ashton Carter will visit a crucial front this week in the war the Pentagon considers its greatest potential threat: cyberspace. Carter will visit a Pentagon outpost in the heart of Silicon Valley, speak at a cybersecurity conference in San Francisco and go to Microsoft and Amazon headquarters in Seattle to highlight the risks of cyberattacks and the need for greater digital cooperation with the Pentagon**. His visit to the West Coast -- his third in less than a year, more than he's made to Kabul or Baghdad -- marks the latest effort by the Obama administration to recruit telecommunications, social media and other technology companies as partners in national security operations despite deep suspicion in Silicon Valley about government surveillance. "One hand of the government is reaching out to the valley, while another is poking them in the eye," said Peter W. Singer, a fellow at the nonprofit New America Foundation in Washington and coauthor of the book **"Cybersecurity and Cyberwar."**

Apple-FBI battle renews push for encryption bill
Washington Post, Karoun Demirjian, 2016 02 29
Washington - **The controversy over whether Apple should help federal investigators access the iPhone of one of the San Bernardino shooters is putting renewed urgency behind legislative efforts to settle the contentious issue of when tech companies should comply with government requests for help accessing their customers' secure information**. **FBI Director James B. Comey** strongly hinted to lawmakers last week that it's time for Congress to begin a serious debate about encryption as Apple and the government battle it out in court with a California judge ruling recently that the tech giant should comply with investigators' demands. "Whatever the judge's decision is in California - I'm sure it will be appealed no matter how it ends up - will be instructive for other courts," Comey said Thursday during a House Intelligence Committee hearing. "But I do think the larger question is not going to be answered in the courts, and it shouldn't be, because it's really about who do we want to be and how do we want to govern ourselves." The heated atmosphere is focusing attention on the anticipated release of a bill being drafted by Senate Intelligence Committee Chairman Richard

Burr (R-N.C.) and Sen. Dianne Feinstein of California, the panel's top Democrat, that would compel companies to override encryption technology when presented with a warrant.

NSA deploys game-changer against U.S. enemies
WTOP Radio (Washington), J.J. Green, 2016 02 29
Washington - **U.S. intelligence has hard proof that almost 1,000 foreign intelligence targets, including terrorists tracked by the U.S., have changed their communications methods because they were tipped off by Edward Snowden's leaks**. Those targets, according to Rick Ledgett, deputy director of the National Security Agency, include a group of terrorists that were actively plotting to attack the U.S. In an exclusive interview with WTOP, Ledgett described as "significant" the continuing damage caused by the leaks. He also detailed a new program to recapture the advantage over U.S. adversaries. "The information that Snowden leaked caused immediate risk and long-term risk to the safety of Americans around the world, and our friends and allies," said Ledgett. High-level foreign intelligence targets of the U.S. government, that number "in the high hundreds," he said, have altered the way they communicate because of the Snowden leaks.

CIA director: Armed forces would ignore Trump
Politico.com, Nick Gass, 2016 02 28
Washington - **Former CIA Director Michael Hayden blasted Donald Trump's rhetoric in a recent interview, saying that the U.S. military would refuse orders from him, even as commander-in-chief, to kill the families of terrorists, as Trump has pledged to do**. Appearing on HBO's "Real Time with Bill Maher" to promote his latest book, Hayden expressed concern about Trump's language, including the Manhattan real-estate magnate's vow to bring back waterboarding and worse because "they deserve it." "I would be incredibly concerned if a President Trump governed in a way that was consistent with the way that candidate Trump expressed during the campaign," Hayden said. Maher brought up Trump's pledge to kill family members of Islamic State terrorists. "That never even occurred to you, right?" Maher deadpanned. "God, no!" Hayden exclaimed. "Let me give you a punchline: If he were to order that once in government, the American armed forces would refuse to act."

FBI vs. Apple Establishes a New Phase of the Crypto Wars
The Intercept, Dan Froomkin & Jenna McLaughlin, 2016 02 27
Washington - **For over two decades, the battle between privacy- minded technologists and the U.S. government has primarily been over encryption. In the 1990s, in what became known as the Crypto Wars, the U.S. tried to limit powerful encryption** -- calling it as dangerous to export as sophisticated munitions -- and eventually lost. After the 2013 Snowden revelations, as mainstream technology companies started spreading encryption by putting it in popular consumer products, the wars erupted again. Law enforcement officials, led by **FBI** Director James Comey, loudly insisted that U.S. companies should build backdoors to break the encryption just for them. That won't happen because what these law enforcement officials are asking for isn't possible (any backdoor can be used by hackers, too) and wouldn't be effective (because encryption is widely available globally now). They've succeeded in slowing the spread of unbreakable encryption by intimidating tech companies that might otherwise be rolling it out faster, but not much else. Indeed, as almost everyone else acknowledges, unbreakable encryption is here to stay.

U.S. government concludes cyber attack caused Ukraine power outage
Reuters, Staff report, 2016 02 26
Washington - **A December power outage in Ukraine affecting 225,000 customers was the result of a cyber attack, the U.S. Department of Homeland Security said Thursday, marking the first time the U.S. government officially recognized the blackout as caused**

by a malicious hack. Security experts had already widely concluded that the downing of utilities in western Ukraine on December 23 was due to an attack, which is believed to be the first known successful cyber intrusion to knock a power grid offline. The published alert from DHS's Industrial Control Systems Cyber Emergency Response Team does not confirm attribution of the attack. But U.S. cyber intelligence firm iSight Partners and other security researchers have linked the incident to a Russian hacking group known as "Sandworm." DHS said its assessment was based on interviews with six Ukrainian organizations affected by the blackout and said its investigators were not able to independently review technical evidence.

U.S. Asks Tech and Entertainment Industries to Aid Antiterror Efforts
New York Times, Cecilia Kang, Matt Apuzzo, 2016 02 25
Washington - **Obama administration officials met with executives of major technology and entertainment companies in Washington on Wednesday to discuss combating the activities of violent extremists online, according to industry and government officials**. The meeting was called by the White House, according to a person who attended and who spoke on the condition of anonymity. The session began with government officials admitting their shortcomings in tackling the explosion of activity by terrorist groups online. John P. Carlin, assistant attorney general for national security, started the meeting by saying that federal law enforcement had struggled to reach audiences that were responding to recruitment by violent extremists, according to the participant. Nick Rasmussen, director of the national counterterrorism center, lauded some social media platforms for aggressively taking down accounts of suspected terrorists. **The hourslong meeting, which took place at the Justice Department, also included speeches by Megan Smith, the national chief technology officer; and Jen Easterly, the senior director for counterterrorism**. The subject of encryption and Apple's resistance to being ordered to break through its encrypted software for law enforcement was not on the agenda.

As it defies U.S., Apple complies with China
Los Angeles Times, David Pierson, 2016 02 26
Los Angeles - **Apple Inc. has come out swinging in its pitched battle with the government on its home turf. But when it comes to its second-largest market, China, the Cupertino, Calif., company has been far more accommodating**. Since the iPhone was officially introduced in China seven years ago, Apple has overcome a national security backlash there and has censored apps that wouldn't pass muster with Chinese authorities. It has moved local user data onto servers operated by the state-owned China Telecom and submits to security audits by Chinese authorities. The approach contrasts with Apple's defiant stance against the **FBI**, which is heaping pressure on the company to decrypt an iPhone that belonged to San Bernardino shooter Syed Rizwan Farook.

Ex-CIA, NSA chief Michael Hayden: 2016 rhetoric 'scares me'
CNN.com, Tal Kopan, 2016 02 26
Washington - **Former CIA and National Security Agency Director Gen. Michael Hayden says the rhetoric from the GOP candidates in the presidential race is scary -- and he suspects the rest of the world is concerned, too**. Hayden was responding Thursday to a question from CNN's Michael Holmes about the rhetoric on the campaign trail, with Holmes mentioning Texas Sen. Ted Cruz's promise of carpet bombing ISIS and GOP front-runner Donald Trump's praise for waterboarding and harsher interrogation techniques as well as a proposed temporary ban on foreign Muslims. "We have taken ... very complicated, serious issues and we've pushed them down to the level of bumper stickers," Hayden said. "That scares me and I'm sure it scares a lot of the rest of the world."

Apple challenges FBI's iPhone demand as 'oppressive'
Washington Post, Ellen Nakashima, Mark Berman, 2016 02 26
Washington - **Apple on Thursday asked a court to quash a judicial order that would force the company to help the Justice Department unlock an iPhone used by one of the San Bernardino attackers, arguing that the order imposed an "unprecedented and oppressive" burden on the tech giant**. The motion to vacate was the latest step in a high-stakes legal battle that could stretch out for months and possibly wind up at the Supreme Court. The filing comes as Apple and the U.S. government are engaging in a public back- and-forth that in the coming weeks will extend to an appearance before Congress and a court hearing. While the debate centers on a locked iPhone 5C, it has far-reaching consequences about the way a digital society balances privacy and civil liberties with law enforcement. "This is not a case about one isolated iPhone," Apple wrote in its motion, filed in the U.S. District Court for the Central District of California. "Rather, this case is about the Department of Justice and the **FBI** seeking through the courts a dangerous power that Congress and the American people have withheld: the ability to force companies like Apple to undermine the basic security and privacy interests of hundreds of millions of individuals around the globe." The company argues that the government is attempting to cut off a debate about the privacy issues in this case and that asking Apple to create a back door would expose personal information "to hackers, identity thieves, hostile foreign agents, and unwarranted government surveillance."

Homeland secretary tells Congress DHS won't squander cyber funds
Federal Times, Aaron Boyd, 2016 02 26
Washington - **Homeland Security Secretary Jeh Johnson is asking for an extra $200 million for cybersecurity in next year's budget but promised legislators the department won't be squandering those funds**. Johnson presented the DHS 2017 budget request to the House and Senate appropriations committees on Feb. 24, laying out the department's priorities, **including cybersecurity.** The department's plans for 2017 go beyond technology, putting DHS at the center of the government's cybersecurity operations and proposing a reorganization of operations within the department.

Homeland Security Is Spilling a Lot of Secrets
Bloomberg View, Josh Rogin, 2016 02 26
Column - **The Department of Homeland Security suffered over 100 "spills" of classified information last year, 40 percent of which came from one office, according to a leaked internal document I obtained**. Officials and lawmakers told me that until the Department imposes stricter policies and sounder practices to better protect sensitive intelligence, the vulnerabilities there could be exploited. Not only does this raise the threat that hostile actors could get their hands on classified information, but may lead to other U.S. agencies keeping DHS out of the loop on major security issues. There were 119 of these classified spills reported throughout the Homeland Security Department in fiscal year 2015, according to the internal document, which itself is unclassified. The section with the most spills by far was the Office of Intelligence and Analysis, headquartered at building 19 of the Nebraska Avenue Complex in Washington, led by retired General Francis Taylor. This office is composed mostly of intelligence analysts assigned to produce and review classified reports that are often the **work of other intelligence agencies, including the Central Intelligence Agency and the Office of the Director of National Intelligence.**

U.S. Set to Expand Sharing of Intercepted Calls and Email
New York Times, Charlie Savage, 2016 02 26
Washington - **The Obama administration is on the verge of permitting the NationalSecurity Agency to share more of the private communications it intercepts with other American**

intelligence agencies without first applying any privacy protections to them, according to officials familiar with the deliberations. The change would relax longstanding restrictions on access to the contents of the phone calls and email the security agency vacuums up around the world, including bulk collection of satellite transmissions, communications between foreigners as they cross network switches in the United States, and messages acquired overseas or provided by allies. **The idea is to let more experts across American intelligence gain direct access to unprocessed information, increasing the chances that they will recognize any possible nuggets of value.** That also means more officials will be looking at private messages -- not only foreigners' phone calls and emails that have not yet had irrelevant personal information screened out, but also communications to, from, or about Americans that the N.S.A.'s foreign intelligence programs swept in incidentally. Civil liberties advocates criticized the change, arguing that it will weaken privacy protections. They said the government should disclose how much American content the N.S.A. collects incidentally -- which agency officials have said is hard to measure -- and let the public debate what the rules should be for handling that information. "Before we allow them to spread that information further in the government, we need to have a serious conversation about how to protect Americans' information," said Alexander Abdo, an American Civil Liberties Union lawyer.

Apple enhancing its iPhone security
Washington Post, Ellen Nakashima, Todd C. Frenkel, 2016 02 25
Washington - **Fearing that the government may be able to order it to bypass security features in newer-model phones, Apple has begun working on enhancements that would prevent the company from updating the software of an iPhone without knowing a user's password**, according to individuals familiar with the effort. These security improvements would make it impossible for Apple to help the government unlock newer iPhones in the manner authorities want the company to do so now. The move would force those authorities to find a new technical solution even if they gain the legal authority to force the company to unlock the phones of suspects. Security experts hailed Apple's move. "They've never thought before that they might be forced by the government to break into its own products and reverse security procedures," said Jonathan Zdziarski, a security researcher who has proposed about a dozen solutions to the problem to Apple. "Now that they've been forced into this mode of thinking, a lot of the security updates in the future will be not just to keep the hackers out, but to keep themselves out until the user authorizes the update."

U.S. spy chiefs expect continuing problems in Libya, Ukraine
Reuters, Mark Hosenball, 2016 02 25
Washington - **U.S. spy agencies expect continuing upheaval in Libya and Ukraine, top intelligence officials told Congress on Thursday.** James Clapper, the U.S. Director of National Intelligence, told a **House of Representatives Intelligence Committee** hearing that the United States had "great hope" that a new government of national accord will soon be formed in Libya. But at the same hearing, **CIA chief John Brennan** acknowledged that the United States in practice was pursuing a two-track policy in Libya, in which it was engaged both in a diplomatic effort to knit together two competing, regionally based self-proclaimed Libyan governments while also conducting "counter terrorism" operations against a growing contingent of Islamic State militants. U.S. officials now estimate that up to 4,000 foreign fighters have traveled to Libya to base themselves in Islamic State training camps that have sprouted up around the country, where they have joined up with hundreds if not thousands of local Libyans who have joined the movement.

U.S. Power Producers Seeking to Stem Grid Cybersecurity Threats
Bloomberg News, Harry Weber, Meenal Vamburkar, 2016 02 25

New York - **Exelon Corp. and other major U.S. power producers are in discussions with regulators and stakeholders on a detailed plan for preventing and responding to cyberattacks designed to disrupt the country's electric system**. Unresolved questions in the talks include who is in charge and would substations that are hit be considered a crime scene, said Exelon Chief Executive Officer Christopher Crane during a Thursday panel discussion at IHS CERAWeek in Houston. "Think about the civil unrest in Philadelphia and Baltimore and some of the communities we serve if you have multiple days of power not flowing," Crane said. The debate comes as U.S. power grids are upgraded from an analog to a digital system, raising the potential that the systems that manage the flow of electricity to millions of Americans could be shut down by a cyberattack. Among the challenges are differences in security requirements across the country and the world, how the grids share power in times of high demand and the massive task of bringing together industry, government and the technology community to find solutions.

Top Intel Officials: U.S. Faces Highest Terror Threat Level Since 9/11
Washington Free Beacon, Adam Kredo, 2016 02 25
Washington - **Top intelligence community officials warned Thursday that the United States faces the highest terrorist threat level since the 9/11 terror attacks, citing a record-breaking increase in the flow of foreign fighters to Syria and Iraq, as well as joint Iranian-North Korean plans to boost "attack capabilities"** and other efforts by leading terror groups to increase their offensive capabilities. As Iran "continues to be the foremost sponsor of terror" across the globe, ISIS has emerged as the "preeminent global terrorist threat," with its combined strength now exceeding al Qaeda's, **according to Director of National Intelligence James Clapper**, who warned lawmakers on the House Permanent Select Committee on Intelligence that "unpredictable instability has become the new normal." The United States has never dealt with this type of threat landscape and struggles to ensure it can continue gathering intelligence on these terror groups, which have shown unprecedented proficiency at obfuscating their actions. Violent extremists now operate in 40 countries, Clapper said. Another seven countries have collapsing governments, and 14 are in danger of falling due to violent instability. An additional 59 countries have been marked as facing "significant risk of instability through 2016," Clapper said.

Spy head: 'Jury's out' on whether China quit hacking after deal
The Hill, Cory Bennett, 2016 02 25
Washington - **The Obama administration still can't assess whether China is adhering to a September pledge to stop hacking private American companies, Director of National Intelligence James Clapper told lawmakers on Thursday**. "I think the jury's out," Clapper said in a rare open House Intelligence Committee hearing. "We have seen some reduction, but I don't think we're in a position to say at this point whether they're in strict compliance," he added in response to the question from Rep. Jim Himes (D- Conn.).

FBI Chief: Apple Issues Are Hardest He's Seen in Government
Associated Press, Staff report, 2016 02 25
Washington - **The policy issues raised in the Justice Department's dispute with Apple Inc. over a locked iPhone represent the "hardest question I've seen in government, and it's going to require negotiation and conversation," FBI Director James Comey said Thursday in defending the government's demand for the tech company to help access the device**. "I do think the larger question is not going to be answered in in the courts, and it shouldn't be. Because it's really about who do we want to be as a country, and how do we want to govern ourselves," Comey told the House Intelligence Committee. Days after making his first public statement on the matter in an Internet blog post, Comey appeared determined to tamp

down the tension that has flared publicly between the government and the company in the week since the judge's order.

FBI's Tor hack shows the risk of subpoenas to security researchers
Threat Level (Wired), Andy Greenberg, 2016 02 25
New York - **Computer security researchers who expose hackable vulnerabilities in digital products face plenty of occupational hazards: They can have their work censored by threats of lawsuits from the companies whose products they hack, or they can even be criminally indicted if their white-hat hacking runs afoul of the Computer Fraud and Abuse Act.** But one still-mysterious encounter between security researchers and the law points to a newer, equally troubling possibility: They can have their work subpoenaed in a criminal investigation and used as a law enforcement tool. A judicial ruling released yesterday in the case of Brian Farrell, an alleged staffer of the defunct Dark Web drug site Silk Road 2, confirmed what many who followed that black market's downfall have suspected for months: That the FBI was able to bypass the anonymity software Tor--the central tool used by the Silk Road 2 and its buyers and sellers to evade the cops--with information they obtained from a subpoena to Tor-focused security researchers at Carnegie Mellon University's Software Engineering Institute.

Apple's top lawyer to testify before Congress over encryption fight with FBI
The Guardian (London), Spencer Ackerman, 2016 02 25
Washington - **Apple's top lawyer will testify before a congressional panel next week about the company's escalating battle with the FBI over smartphone privacy, Washington sources have confirmed.** The hearing, scheduled for 1 March before the House judiciary committee, will be Congress's first opportunity to quiz an Apple representative, vice-president and general counsel Bruce Sewell, over the company's rejection of a court order demanding the company unlock the iPhone belonging to one of the terrorists who killed 14 people in San Bernardino, California, in December. **FBI director James Comey**, who conceded to a different House panel on Thursday that the resolution of the case will likely set a legal precedent, will also testify - but not alongside Sewell. Comey will speak first and without other witnesses, something aides said was typical for government witnesses, and Sewell will follow.

400 Intel Pros Warn: ISIS Info Flawed
The Daily Beast, Shane Harris, Nancy A. Youssef, 2016 02 25
Washington - **Forty percent of analysts working at the U.S. military's Central Command, which is running the war against ISIS, think there are problems with "analytic integrity" in their work, a top congressman said on Thursday**. Rep. Devin Nunes, chairman of the **House Intelligence Committee**, asked senior intelligence officials about the figure, which was discovered in a recent survey of analysts by the country's top intelligence office. The survey was first reported by The Daily Beast this month. "To me, it seems like if 40 percent of analysts are concerned at **CENTCOM**, that's just something that can't be ignored," Nunes told top intelligence officials testifying before the committee, including **Director of National Intelligence James Clapper and CIA Director John Brennan.** "I would consider that unusually high," Lt. Gen. Vincent Stewart, the director of the Defense Intelligence Agency, said of the 40 percent figure. "We've already had requests where there's been a dispute at CENTCOM where we've sent out an ombudsman there to look at the analytic rigor."

Spy agencies say Clinton emails closely matched top secret documents: sources
Reuters, Mark Hosenball, 2016 02 25
Washington - **U.S. spy agencies have told Congress that Hillary Clinton's home computer server contained some emails that should have been treated as "top secret" because their wording matched sections of some of the government's most highly classified**

documents, four sources familiar with the agency reports said. The two reports are the first formal declarations by **U.S. spy agencies** detailing how they believe Clinton violated government rules when highly classified information in at least 22 email messages passed through her unsecured home server. **The State Department has already acknowledged that the emails contained top secret intelligence**, though it says they were not marked that way. It has not previously been clear if the emails contained full classified documents or only some information from them. The agencies did not find any top secret documents that passed through Clinton's server in their full version, the sources from Congress and the government's executive branch said. However, the agency reports found some emails included passages that closely tracked or mirrored communications marked "top secret," according to the sources, who all requested anonymity. In some cases, additional classification markings meant access was supposed to be limited to small groups of specially cleared officials.

Apple CEO Tim Cook Says iPhone-Cracking Software 'Equivalent of Cancer'
ABC News, Enjoli Francis, 2016 02 25
New York - **In an exclusive interview with ABC News today, Apple CEO Tim Cook told "World News Tonight" anchor David Muir that what the U.S. government was asking of the tech giant -- to essentially create software enabling the FBI to unlock an iPhone used by one of the San Bernardino, California, shooters** -- amounted to the "software equivalent of cancer." "The only way to get information -- at least currently, the only way we know -- would be to write a piece of software that we view as sort of the equivalent of cancer. We think it's bad news to write. We would never write it. We have never written it -- and that is what is at stake here," he said. "We believe that is a very dangerous operating system." The FBI has called on Apple to help crack into the iPhone of Syed Farook, who along with wife Tashfeen Malik killed 14 and injured 22 at a training session and holiday party in December. The FBI attempted to crack the pass code but failed because Apple phone systems have a function that automatically erases the access key and renders the phone "permanently inaccessible" after 10 failed attempts. Last week, at the request of the Justice Department, a federal judge told Apple to assist law enforcement.

NPR's Interview With CIA Director John Brennan
NPR, Mary Louise Kelly, 2016 02 24
Interview: MARY LOUISE KELLY: **Let me start with this week's news with cyber and the legal showdown unfolding between Apple and the FBI over this San Bernardino iPhone. Should Apple be forced to help the FBI unlock this phone? CIA DIRECTOR JOHN BRENNAN:** Well, on that particular case, it is being worked now through the courts. But from the standpoint of the government's responsibility to keep its citizenry safe, I think there needs to be a very healthy debate and discussion about what the government should be able to do and access when it comes to electronic communications. You know, for many years, I think there has been a fairly well-established principle that the government, when it has the appropriate basis, or a court order, will be able to have access to information that is important to determine guilt-innocence, or what needs to be done in order to protect the citizens. So for example, when I think about electronic communications, it is sort of a unique environment. But at the same time, what would people say if a bank had a safe-deposit box, or a storage company had a storage bin, that individuals could use and access and store things, but the government was not going to be able to have any access to those environments? And so criminals, terrorists, whatever, could use it. So what is it about electronic communications that makes it unique in terms of it not being allowed to be accessed by the government when, again, the law, the courts, say that the government should have access to it? So these are things that need to be worked through.
KELLY: Is that a yes, that you think Apple should be forced to help the FBI in this case?
BRENNAN: I think that the FBI clearly has a legitimate basis to try to understand what is on a

phone that is part of a very active investigation; again, consistent with what their responsibilities and authorities are. So, again, this is being worked out through the courts. But I do believe that electronic communications, like other means of communication, or means of storage, should have the opportunity for the government, when there is a legitimate basis, to access it.

Feds secretly tracked 6,000 phones
USA Today, Brad Heath, 2016 02 24
Washington - **Federal marshals have secretly used powerful cellphone surveillance tools to hunt nearly 6,000 suspects throughout the USA, according to newly disclosed records in which the agency inadvertently identified itself as the nation's most prolific known user of phone-tracking devices**. The fact that the U.S. Marshals Service uses cellphone trackers, commonly known as stingrays, has long been among law enforcement's worst- kept secrets, though the agency refuses to acknowledge it. The Marshals Service confirmed its use of the devices to USA TODAY only in the process of trying to keep it secret, rejecting a Freedom of Information Act request for a copy of its log of cases in which agents used stingrays. The Marshals Service's response to that request included an almost totally censored spreadsheet listing its stingray cases. Information about the cases was stripped out line by line, which made it possible to count the number of entries the agency had made on its log of stingray uses.

Bill Gates 'Disappointed' by Reports He Backs FBI Over Apple
Bloomberg News, Jing Cao, 2016 02 24
New York - **Bill Gates is "disappointed" with a recent report suggesting that he supports the U.S. government in its clash with Apple Inc. over unlocking an iPhone, saying it doesn't accurately reflect his opinion on the matter**. "That doesn't state my view on this," he said in an interview on "Bloomberg Go." "The extreme view that government always gets everything, nobody supports that. Having the government be blind, people don't support that." The Financial Times reported that Gates sided with the U.S. government, saying that a court order requiring Apple to help unlock the phone of a terrorist involved in a December attack was a one-time request and "no different" from accessing bank and telephone records. It's important to strike the right balance between the government getting to see everything versus nothing, Gates said on "Bloomberg Go."

House Committee Looks at Possible T.S.A. Lapses and Mistreatment
New York Times, Ron Nixon, 2016 02 24
Washington - **A congressional committee is investigating allegations that the agency in charge of airport security retaliated against employees who reported security lapses and awarded bonuses to supervisors who ignored their warnings**. The agency, the **Transportation Security Administration**, has until March 4 to provide the House Oversight Committee with documents detailing how it awards bonuses to top agency officials. The investigation comes after Andrew Rhoades, an assistant federal security director at Minneapolis-St. Paul International Airport, sent documents to the committee that he said indicated that the top supervisors who ignored warnings about security lapses were awarded bonuses. One top official in charge of security for the agency received more than $70,000 in bonuses in a three-year period despite a leaked audit that showed screeners failed to detect investigators with fake weapons and bombs going through security lines. The audit showed that screeners failed to detect the weapons 95 percent of the time.

Encryption's tight grip
Los Angeles Times, Paresh Dave, 2016 02 24
Los Angeles - **The FBI hasn't made any headway in its standoff with Apple Inc., and the bitter feud isn't changing minds at competitors either. Several tech executives have**

voiced their support for Apple and are forging ahead with their plans for greater privacy, arguing that what consumers want is more control over their devices and no backdoors for governments. That's bad news for the FBI, and signals that even as it battles Apple, pushback will persist from other tech companies, including social media giants, hardware makers and online storage providers. The government has shown no signs of backing down, though. But where the government wants reasonable paths into phones and databases for criminal investigations, it is instead being met with stiffer barriers. "As much as they try to play up terrorism and child pornography and make an emotional play, we are going to see more encryption," said John Adams, director of security at San Francisco payments processing start-up Bolt and a former head of security at Twitter Inc. "They try to use the horrors of the world to erode civil liberties and privacy, but the greater good -- having encryption, more privacy for more people -- is always going to trump small isolated incidents."

Donald Trump's national security policy would look like a high school UN
Foreign Policy, Peter Feaver, 2016 02 23
Comment - **What kind of national security policy would a President Donald Trump conduct? Since the fall, there have been some heroic attempts by serious analysts to identify a method to the madness of Trump's positions**. George Mason's Colin Dueck thinks he is a traditional American nationalist. Walter Russell Mead at Bard claims Trump has recreated a "nihilistic populism." The National Review's Rich Lowry borrows from Mead's own framework to suggest that Trump is a "Jacksonian" populist. Thomas Wright, writing in Politico, asserts that Trump has had a consistent foreign policy framework, albeit one drawn from the populism and isolationism of the pre-World War II era. Each of these analyses has some merit to it in the sense that sometimes Trump's positions coincide with some of the tenets of these worldviews. And while many of his foreign policy positions bounce around erratically -- he now claims he always opposed the Iraq war when, in fact, he was an early supporter of it -- there are some areas where he does hold a consistent position. For instance, Trump has consistently opposed free trade. **And Trump has consistently believed that our security treaty allies are ripping us off --** perhaps because he is apparently unaware that our allies actually subsidize the cost of U.S. troops stationed. Yet, none of this adds up to the kind of coherent foreign policy framework that would allow us to make the plausible predictions that are possible with a normal candidate.

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

Home Office to publish revised draft of snooper's charter
The Guardian (London), Alan Travis, 2016 03 01
London - The home secretary, **Theresa May, has revised some elements of her controversial "snooper's charter" legislation in an attempt to address criticism by MPs and peers of the surveillance powers it confers**. Home Office sources say the revised bill, to be published on Tuesday, will reflect a majority of the 129 recommendations made by three parliamentary committees in reports published over the last three weeks. The committees called for a fundamental rewrite of the draft investigatory powers bill, for privacy safeguards to be made the backbone of the legislation and for safeguards to be created against new powers to track everyone's web browsing histories - known as internet connection records. The bill will not meet demands that the most intrusive snooping operations should be authorised by a judge - and not by a minister as is the case at present.

May using campaign sneak in snoopers charter
Mail On sunday, Glen Owen, 2016 02 28
London - **Home Secretary Theresa May was last night accused of rushing her so-called snoopers charter into the Commons while MPs are distracted by the EU referendum campaign. Tory rebels joined forces with Labour to criticise the Home Secretary for hastily putting the Draft Investigatory Powers Bill to a Commons vote next week, despite warnings from MPs that it did not sufficiently address concerns about the intrusive spying powers of the intelligence agencies**. Mrs May has called for **MI5**, **MI6** and **GCHQ** to be allowed to access the web browsing histories of UK citizens for up to 12 months, among other new snooping measures designed to combat the terror threat. The powerful Intelligence and Security Committee, chaired by former Tory Attorney General Dominic Grieve, was one of three committees to complain that the new powers did not appear to have been fully thought through. Tory rebels also expected the House of Lords to force the Government to insert more protections for civil liberties into the legislation.Shadow Home Secretary Andy Burnham said: For Labours support, Ministers must show they have listened to our calls for greater transparency, stronger safeguards and protection of peoples privacy.

Keep calm and earn a big pay rise
Sunday Times (UK), Staff Writer, 2016 02 28
London - **MI5 is trying to poach bomb disposal experts from the army to help handle terrorist attacks in Britain, writes Sean Rayment**. The security service wants to recruit members of the Armed Forces Explosive Ordnance Disposal to join its **weapons intelligence unit -- and is offering pay rises of about £19,000. Successful applicants will earn up to £56,000**, far higher than the average £37,000 salary for an armed forces bomb disposal operator or an ammunition technical officer. The work will involve analysing intelligence from a range of sources and providing expert advice and support to members of MI5 and the wider intelligence and military communities. An advert on the MI5 website reads: "To join our Weapons Intelligence Group you'll need to make rapid, informed technical assessments, often based on incomplete information. An ability to remain calm and objective under pressure is vital for this role."

'GCHQ spy who raped us is still working there because police didn't take us seriously'
The Daily Mirror, Nick Dorman, 2016 02 28
London - **A spy accused of rape by two women is still working at the heart of Britain's security services after police ignored their claims**. The spook's first alleged victim, who met him through a dating website, today say detectives TWICE failed to act over her accusations - even after the second woman, who worked with him at the top secret **GCHQ** base, had come forward. The man was never even arrested. And in a further twist the intelligence expert was SACKED by his spy bosses after child porn was found on his computer. But he was reinstated three months later - after police again dropped the case. These shocking details have only emerged because the first alleged victim, who has a child by the spy, had a dramatic confrontation with him in a civil court. She has also complained to the Independent Police Complaints ¬Commission over her dealings with officers in Gloucestershire, where the Government's top secret listening post is based. She told the Sunday Mirror: "It seems like this man is untouchable because he works for GCHQ. I don't feel any of the claims against him have ever been properly investigated by the police. "There must be a full enquiry, and I am intending to sue the police over the damage this has caused." The Gloucestershire force has confirmed the women's disturbing claims are being investigated.

Provo's nephew in legal move to stop MI5 'harassment'
Beirut Daily Star, Alan Erwin, 2016 02 27

London - **A west Belfast taxi driver has begun legal moves to stop alleged repeated approaches by MI5 agents, it has emerged**. Christopher Catney has instructed his lawyer to explore seeking a High Court injunction amid claims he is being harassed by the security services. He alleges contact was made during a holiday in the Canary Islands and on his return to Belfast International Airport. Mr Catney, the nephew of former IRA man Tony Catney, said he fears others in his community will suspect him of being an informant. He stressed he had no links to any political group or organisation, and attributed the alleged targeting to his family name. In a statement prepared as an initial stage in the legal process, Mr Catney claimed he had come under increased attention from **MI5 and the PSNI**. He alleged that officers called at his ex-partner's home looking for him, and that unmarked cars followed his taxi. The level of attention increased following an approach by MI5 agents while on holiday last November, according to his account.

Spooky London: how Britain's spy agencies are using new and unexpected methods to recruit the next generation
The Evening Standard, Samuel Fishwick, 2016 02 25
London - **Gone are the days when a tap on the shoulder from an Oxbridge don was the only way into British intelligence services. Now you're more likely to be recruited when playing video games (this is no exaggeration: GCHQ adverts have been found on Xbox Live online game networks, where pixelated posters for 'gchq-careers.co.uk' are pasted on the simulated street corners of titles such as racing game Need for Speed: Carbon).** In October, Mumsnet users noticed banner ads for **MI6 intelligence officer** roles popping up as they browsed Dorset holiday destinations, while East London's GCHQ graffiti campaign recently took social media by storm. The approach may sound bizarre, but it seems to be working. John was browsing discussion forums when he stumbled upon canyoucrackit.co.uk, a website set up by GCHQ to recruit code breakers. 'I spent a bit of time just staring at the webpage and had a flash of understanding when I saw a pattern I recognised,' says John, 24. 'From that point I was hooked.' Online forums lit up with would-be spooks swapping ideas on how to break through. 'The air of mystery was what most got to me,' he admits. 'What kind of challenges would an organisation like GCHQ be designing for people to attempt to break? Was it possible for mere mortals to do so?'

Singing star Katherine Jenkins comes to GCHQ and sings to staff as thanks for their work
Gloucestershire Echo, Staff report, 2016 02 26
Cheltenham - **GCHQ staff took a break from their top secret work to listen to international opera and classical singing star Katherine Jenkins this afternoon**. The singer visited the Doughnut in Cheltenham and sang at a 45 minute concerts as a thank you to staff for their work in keeping Britain safe, and to raise money for charity The Welsh singing star, who performed for free, said: "I'm delighted to have been asked to sing here to show my support for all those keeping our country safe, as I am aware how hard they work. I have also kindly been shown around the headquarters which has been very interesting. I would like to wish them my on-going thanks for all that they do for our country."

Return to Table of Contents/ Retour à la table des matières

Australia/ Australie

Cybercriminals increasingly targeting Australia as a launch pad for cybercrime
ABC (Australia), Mohamed Taha, 2016 02 26
Canberra - **A Threat Intelligence Brief report finds Australian- based cyber threats -- including malicious IP addresses, suspicious URLs and phishing sites -- more than doubled in 2015. A published on Wednesday by one of the largest internet security companies in the US, Webroot, has found Australia is a lucrative market for cybercriminals.** The report found Australian-based cyber threats -- including malicious IP addresses, suspicious URLs and phishing sites -- more than doubled in 2015. It was found that in 2015 2,000 new harmful IP addresses were created every day. The data used for the Webroot report was captured, analysed and correlated by a data security platform, which reviewed 27 billion URLs, 600 million domains, 4 billion IP addresses, 20 million mobile apps from 10 million connected sensors. Although Australia only accounted for 2 per cent of global attacks, it featured in the top 10 global hosts for cyber threats.

Hi-tech upgrade to cost billion
The Australian, Joe Kelly, 2016 02 26
Canberra - **The defence white paper has poured hundreds of billions of dollars into delivering strategic planners a series of hi-tech acquisitions, including long-range spy planes, 12 new submarines, new- generation armoured vehicles and electronic attack aircraft**. Across the next 10 years, Defence will invest nearly $49 billion in its maritime and anti-submarine assets including 12 submarines, nine anti-submarine frigates and 12 offshore patrol vessels. The submarine fleet will cost at least $50bn from 2018 to 2057, doubling its size from six to 12. The weapons system is estimated to cost $5bn to $6bn over 2018-45. The government did not put a sustainment cost on the fleet but Defence Force chief Mark Binskin previously has put the upkeep at twice the value of the initial acquisition, suggesting a total expense of about $150bn.

White paper reveals broad range of threats
Sydney Morning Herald, David Wroe, 2016 02 25
Sydney - **Tensions in the South China Sea, the rise of the Islamic State group and the danger of crippling cyber attacks mean the Turnbull government's defence blueprint will tackle "a broader range of threats" than Australia has faced before, a senior Defence official has said**. The Defence white paper, to be released on Thursday, will unveil what government sources said would be a $29.9 billion increase in defence spending over the next 10 years. This boost will help pay for what sources say will be the most powerful and capable defence force the nation has had, in particular a modernised navy in recognition of the growing strategic uncertainty in Asia. "It's fair to say that this white paper has had to take account of a broader range of threats than any previous white paper," the defence official with close knowledge of the document told Fairfax Media. "

Return to Table of Contents/ Retour à la table des matières

New Zealand/Nouvelle-Zélande

Kiwi Big Brother is watching you
New Zealand Herald, 2016 02 27
Wellington - **In the US, Apple is fighting the FBI's court order to unlock a dead terrorist's iPhone. The terrorist, with his wife, massacred 14 people in San Bernardino last year. It's a tough case. There is not a lot of sympathy for murdering terrorists, but Apple says**

complying with the FBI's warrant would set a precedent for all Apple users. Meanwhile, in New Zealand our companies fall over themselves to give private information when a Government department asks for it. The Government mostly needs no warrant and companies hand over information even if not legally obligated to do so. The Government asks, companies provide. The Privacy Commissioner reports the big three that ask for information are the Inland Revenue, the Ministry of Social Development and police. These three departments issued 11,333 information requests to just 10 companies - two telcos, seven financial services companies and one utility.

Terrorists win if our privacy is lost
New Zealand Herald, David Rutherford, 2016 02 24
Op-ed: **The Independent Review of Intelligence and Security Services is due to deliver its recommendations to the Government on Monday. The questions Sir Michael Cullen and Dame Patsy Reddy have been tasked with reviewing sit at the heart of the Human Rights Commission's remit so we await the review's findings and the Government's response with immense interest.** In the frame is whether the **Government Communications Security Bureau (GCSB) and the Security Intelligence Service (SIS)** are well placed to protect New Zealand's national security needs, while protecting individual rights, and whether the current oversight arrangements are sufficiently robust to ensure they act within the law. In particular, the reviewers must consider whether the powers conferred by the anti-terrorism legislation brought in on December 12, 2014, as part of the UN-co-ordinated reply to the Isis (Islamic State) threat should be extended beyond their expiry date of April 1, 2017. We would have liked the information-collecting and surveillance functions of the police to have been included in the inquiry but note that this gap may now be filled as Justice Minister Amy Adams has asked the Law Commission to examine the Search and Surveillance Act 2012, including the impact of modern technology on the ability of the police and other authorities to prevent and investigate crime.

Return to Table of Contents/ Retour à la table des matières

International

China/Chine

China stealing military information from Norway
The Local (Norway), 2016 02 29
Oslo— In its annual threat assessment, **the Norwegian Intelligence Service (Etterretningstjenesten - NIS) said that both Russia and China present security challenges to Norway** and that the latter has most likely stolen military intelligence from Norwegian companies. While much of the NIS report – like that of the threat assessment released by the Norwegian Police Security Service (PST) earlier this month – focused on the dangers posed by Russian spies, it also revealed that China has stolen information from Norwegian weapons companies. See also: Russian spying can 'damage' Norway: PST "We believe that they [China, ed.] have succeeded in extracting information that they are using in their own weapons technology," NIS head Morten Haga Lunde told TV2.

China collecting personal data through Android apps: report
Globe and Mail, Nathan Vanderklippe, 2016 02 25
Hundreds of millions of Android smartphone users have downloaded photo-collage, karaoke and video-chat apps that send location data and other identifying details back to

servers in China, a new report has found. The information is collected by Chinese search and advertising engine giant Baidu, which collects users' GPS co-ordinates, names of nearby wireless networks and a unique device number that can be used to identify a person's phone, according to findings contained in a new report from The Citizen Lab at the University of Toronto's Munk School of Global Affairs. That information is stored on Baidu servers. The company says it gives Chinese authorities access to its data in accordance with local laws. But placing such material in government hands could provide a detailed picture of a person's movements and contacts, potentially threatening those who anger the Chinese state, such as human-rights campaigners or democracy activists, said **Ronald Deibert**, the lab's director. "That is obviously the ultimate and most serious risk," he said. "The collection of all that finegrained, detailed information is either poor engineering choices, or this is surveillance by design," he said. And, he added, "don't forget - none of that data disappears."

Chinese tech execs backing Apple
Los Angeles Times, Jonathan Kaiman, Samantha Masunaga, 2016 02 25
Beijing - Chinese technology executives are weighing in on the standoff between Apple Inc. and the FBI -- and they're taking Apple's side. Chinese Internet companies operate in one of the world's most restrictive online environments, in which bowing to official censorship and surveillance demands is a necessity of doing business. Services that don't comply, including Facebook, Twitter, YouTube, Google and Instagram, are summarily blocked. So it might seem counterintuitive that this week two prominent chief executives of Chinese technology firms threw their support behind Apple Chief Executive Tim Cook's refusal to create software that would help the U.S. government break into the encrypted iPhone used by one of the shooters in the deadly San Bernardino terrorist attack. But these public statements may have less to do with potential business advantages than they do with global politics, said James Lewis, senior fellow at the Center for Strategic and International Studies in Washington. "China has decided, as a matter of policy, to become very critical of the United States," he said. "We don't know what [the executives'] motives are ... but since you see this whole spate of Chinese articles saying the U.S. is corrupt and its democracy is flawed, this is another example of that."

Return to Table of Contents/ Retour à la table des matières

Russia/Russie

Snowden's Russian Improves After Over 2 Years of Living in Russia
Sputnik (Russia), Staff report, 2016 02 25
Moscow - **Former US National Security Agency (NSA) contractor Edward Snowden, currently residing in Russia, has learned a reasonable amount of Russian, the whistleblower's lawyer, Anatoly Kucherena, said Wednesday**. Kucherena has represented Snowden since 2013, continuing to do so without charge. "Edward is fine. He is working and learning Russian. We can already talk with him on certain issues, which is positive," Kucherena told RIA Novosti.

Moscow dispatches FSB hitmen to Donetsk city to eliminate some separatist leaders - intelligence
Ukrinform (Ukraine), Staff report, 2016 02 24
Kyiv - **In order to eliminate uncontrolled individual commanders of rebels a detachment comprising special operations teams of the Russia GRU of the General Staff of the Armed Forces and the FSB have arrived in Donetsk city**. Ukraine defense ministry

intelligence reported on it site. "In order to kill some commanders of illegal armed formations uncontrolled by the command of the Russian occupation troops 150-servicemen detachment comprising special operations teams of the Russia GRU of the General Staff of the Armed Forces and the FSB have arrived in Donetsk city," a statement said.

Return to Table of Contents/ Retour à la table des matières

Europe

Germans spied on our Brussels baroness
Sunday Times (UK), James Lyons, 2016 02 28
London - **Germany's secret service spied on the EU's British foreign policy chief and the US secretary of state, it emerged yesterday. The BND, Germany's equivalent of MI6, placed Baroness Ashton of Upholland under electronic surveillance when she was EU high representative on foreign affairs and security**. It also tried to tap the mobile and office phones of John Kerry, the secretary of state, according to Der Spiegel magazine. The attempt to listen in to Kerry's mobile conversations failed because a bungling spy used an African country code by mistake. His other phones, including one at the US State Department, were successfully tapped. The revelations are deeply embarrassing for Angela Merkel, who criticised the US over allegations that the **National Security Agency** monitored the chancellor's phone as part of a mass surveillance programme that included snooping on allies. At the time, Merkel told President Obama that "spying on friends is not acceptable". Ashton, 59, who was given a peerage by Tony Blair, was targeted by the BND when she became Europe's de facto foreign secretary in 2009.

Surveillance des frères Kouachi : autopsie d'un échec
Le Monde.fr, journaliste maison, 2016 02 27
Paris - **Si la DGSI ne manquait pas d'informations sur les tueurs de « Charlie Hebdo », elle n'a pas su les analyser. Chaque nouvel attentat souligne les défaillances des services de renseignement et fournit l'occasion d'octroyer plus de moyens à la Direction générale de la sécurité intérieure (DGSI, ex-DCRI).** La réflexion sur l'organisation du renseignement français, elle, est sans cesse repoussée. A la mi-novembre2015, quarante et une notes de la Direction centrale du renseignement intérieur (DCRI) - devenue la DGSI en mai2014 - sur les frères Kouachi et Amedy Coulibaly ont été déclassifiées à la demande de la justice, comme l'a révélé Le Monde le 4janvier. Leur examen retrace de manière très précise le travail effectué entre 2010 et 2013 sur les futurs auteurs des attentats de janvier2015. Il permet surtout de mieux cerner la nature des failles dans ce dossier. Premier enseignement: la DCRI n'a pas manqué de moyens.

Après trois mois d'état d'urgence, un bilan contesté et mitigé
Le Monde, Julia Pascual, 2016 02 26
Paris - **Sur les 274 assignations à résidence, moins de 100 devaient être renouvelées. La LDH porte plainte contre ces mesures " arbitraires " Vendredi 26 février, à minuit, l'état d'urgence voté par le Parlement après les attentats de Paris et Saint-Denis touche à sa fin**. Ainsi s'achève ce régime d'exception dans lequel les pouvoirs de police administrative sont décuplés. En réalité, il va être aussitôt renouvelé, jusqu'au 26 mai prochain, ainsi que l'a voté, le 16 février, l'Assemblée nationale. La menace terroriste " est plus élevée que jamais " , avait alors affirmé le ministre de l'intérieur, Bernard Cazeneuve, devant les députés. Le bilan de l'état d'urgence est pourtant diversement apprécié. Mercredi 24 février, dans son rapport annuel, Amnesty International s'en est pris à la réponse " liberticide " de la France aux attentats

terroristes de 2015. L'ONG juge l'état d'urgence disproportionné et estime que sa mise en oeuvre a donné lieu à des " dérives " .

Équipés de moyens pointus d'interception, les services de renseignements resserrent leur filet
Le Figaro, Christophe Cornevin, 2016 02 26
Paris - **Équipés de moyens pointus d'interception, les services de renseignements resserrent leur filet en campagne Volontiers brandi comme un funeste symbole, Maxime Hauchard est l'archétype du péril terroriste qui pousse en germe dans nos campagnes**. Bourreau de Daech paradant en novembre 2014 dans une vidéo de décapitations collectives, celui qui s'est fait appeler Abou Abdallah al-Faransi avait grandi à Bosc-Roger-en-Roumois, commune de 3 200 âmes proche de Rouen. Issa K., un Tchétchène de 27 ans, décrit comme « profondément radicalisé » ,neutralisé mi-décembre dernier en Indre-et-Loire, est quant à lui venu allonger cette galerie d'épouvantails qui mettent les services territoriaux sur les dents. Ayant prêté allégeance à Deach, ce Tourangeau venait d'enregistrer une vidéo testamentaire avant d'être intercepté par la **DGSI**. Il ne se déroule guère une semaine sans que les services ne déjouent une équipée djihadiste loin de Paris. Le 26 janvier dernier encore, quatre présumés combattants volontaires francais, deux mineurs et deux majeurs, ont été surpris, selon nos informations, près de l'étang de Berre (Bouches-du-Rhône) alors qu'ils s'apprêtaient à rejoindre la Syrie.

Lithuania: verdict in spying paramedic's case due next week
Baltic News Service, 2016 02 25
Vilnius— **Vilnius Regional Court on Thursday finished hearing the case of a former army paramedic accused of spying for Belarus**, and the verdict is due on March 4. Former army paramedic Andrej Osurkov was on Thursday given the right to address the court for the last time. The hearing was held behind closed doors. Osurkov, who formerly served at the Lithuanian Grand Duke Algirdas Mechanized Infantry Battalion, was arrested in January, 2014. In December of 2014, the **State Security Department** said it had established Osurkov had been recruited by the **Chief Intelligence Board** of the Belarusian Armed Forces' General Staff in Belarus to later infiltrate him in the Lithuanian army for special tasks. He is suspected to have provided Belarus with data for five years, receiving cash in return. Osurkov pleaded guilty.

Jailed journalists' rights breached, Turkish court rules
Anadolu News Agency, Staff report, 2016 02 25
Ankara - Two Turkish journalists accused of espionage and trying to overthrow the government suffered rights violations, Turkey's highest court has ruled. Can Dundar, editor-in-chief of the newspaper Cumhuriyet, and the daily's Ankara bureau chief Erdem Gul were arrested on Nov. 26 over the publication of photographs and video footage purportedly showing shells and ammunition loaded **on Syria-bound trucks belonging to Turkey's National Intelligence Organization (MIT).** .

En Libye, la guerre secrète de la France
Le Monde, Nathalie Guibert, 2016 02 25
Paris - **Pour lutter contre l'Etat islamique, l'armée française a recours aux forces spéciales et aux actions clandestines Plusieurs sources ont indiqué au Monde que la lutte contre les terroristes pouvait couvrir des opérations clandestines, menées par le service action de la Direction générale de la sécurité extérieure (DGSE).** Les premières engagent la France car leurs soldats, même très discrets, agissent sous l'uniforme. Les secondes sont aussi assurées par des militaires mais restent invisibles. Forces spéciales et clandestines sont considérées dans la doctrine militaire comme des " précurseurs ", des outils

classiques en l'absence de cadre disponible pour une guerre ouverte. Ces moyens, dits " d'ouverture de théâtre ", ne préjugent toutefois pas d'une future opération en bonne et due forme.

Les services de renseignement allemands pourront utiliser des logiciels espions
Le Monde, Journaliste maison, 2016 02 24
Berlin - **Le gouvernement a officiellement donné son feu vert à l'utilisation du Bundestrojaner, le « cheval de Troie fédéral ».** Le gouvernement allemand a officiellement donné son feu vert à l'utilisation d'un logiciel espion de type «cheval de Troie», par les services de renseignement du pays. Une fois installés sur un ordinateur, ces programmes créent une porte dérobée, invisible pour l'utilisateur, qui permet à un tiers de se connecter à la machine pour y dérober des informations. Le logiciel, surnommé par la presse allemande «Bundestrtojaner» («cheval de Troie fédéral»), a été conçu par la police fédérale et testé pour éviter tout abus, a affirmé le ministère de l'intérieur.

Les grandes oreilles de la NSA vont jusqu'à Genève
Le Temps (Suisse), Simon Petite, 2016 02 24
Genève - **Les Etats-Unis sont notamment accusés par WikiLeaks d'avoir espionné un fonctionnaire du Haut-Commissariat pour les réfugiés (HCR) nommé représentant en Iran Les Etats-Unis ont placé sur écoute plusieurs lignes téléphoniques à Genève. Voici les dernières révélations du site WikiLeaks**. La **National Security Agency (NSA)** est accusée d'avoir espionné de hauts responsables de l'Organisation mondiale du commerce (OMC) et du Haut-Commissariat pour les réfugiés (HCR). Les deux institutions n'avaient pas réagi mardi. « Il sera intéressant de voir la réaction de l'ONU, car les Etats-Unis avaient promis qu'ils ne l'espionneraient pas », a estimé Julian Assange depuis l'ambassade équatorienne à Londres, où le fondateur de Wiki-Leaks est toujours bloqué. La Suisse s'était émue par le passé des activités d'espionnage de la mission américaine à Genève. Un autre célèbre lanceur d'alerte, Edward Snowden, y avait travaillé entre 2007 et 2009 pour le compte de la CIA avant de révéler des années plus tard l'ampleur de la surveillance de la NSA.

La guerre secrète de la France en Libye
Le Monde, Journaliste maison, 2016 02 24
Paris - **Forces spéciales et opérations clandestines sont engagées en Libye par les autorités françaises pour lutter contre l'expansion de l'Etat islamique**. Des frappes ponctuelles très ciblées, préparées par des actions discrètes voire secrètes: en Libye, telle est la ligne de conduite de la France face à la menace de l'organisation Etat islamique (EI). Un haut responsable de la défense française confirme au Monde que «la dernière chose à faire serait d'intervenir en Libye. Il faut éviter tout engagement militaire ouvert, il faut agir discrètement.» Dans ce pays où la France scrute depuis des mois la menace de l'EI, l'objectif n'est pas de gagner une guerre mais de frapper l'encadrement du groupe terroriste, dans l'idée de freiner sa montée en puissance. Une action menée de concert par Washington, Londres et Paris, comme l'a de nouveau illustré le raid américain du 19février contre un cadre tunisien de l'EI à Sabratha. Moyens d'« ouverture de théâtre » La ligne fixée par le président François Hollande repose pour l'heure sur des actions militaires non officielles. Elles s'appuient sur des forces spéciales - leur présence, dont Le Monde a eu connaissance, a été repérée dans l'est de la Libye depuis mi-février par des blogueurs spécialisés. Ce n'est pas tout. Plusieurs sources ont indiqué au Monde que la lutte contre les terroristes pouvait couvrir des opérations clandestines, menées par le service action de la **Direction générale de la sécurité extérieure (DGSE).**

L'Italie condamnée pour l'enlèvement par la CIA en 2003 d'un imam à Milan
La Nouvelle Tribune (Maroc), Journaliste maison, 2016 02 23

Strasbourg - **L'Italie était au courant de l'enlèvement par la CIA d'un imam égyptien à Milan en 2003 et a abusivement invoqué le secret d'Etat pour assurer l'impunité aux responsables, a tranché mardi la Cour européenne des droits de l'Homme (CEDH**). Les juges de Strasbourg ont estimé que l'Italie s'était rendue coupable de nombreuses violations des droits de l'Homme dans cette affaire, notamment l'interdiction de la torture et le droit au respect de la vie familiale. La Cour « tient pour établi que les autorités italiennes savaient » que l'imam Abou Omar - alors soupçonné de liens avec le terrorisme, et depuis condamné en Italie par contumace pour association de malfaiteurs à des fins de terrorisme international- était victime d'une opération d'enlèvement montée par des agents américains.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

FM, NATO chief discuss regional, int'l issues
Kuwait News Agency, 2016 02 29
Kuwait— First Deputy Prime Minister and Foreign Minister Sheikh Sabah Khaled Al-Hamad Al-Sabah met with Secretary General of the North Atlantic Treaty Organization (NATO) Jens Stoltenberg, where they shed light on regional and international issues of common interest. **National Security Bureau Chief Sheikh Thamer Ali Sabah Al-Salem Al-Sabah was present at the meeting,** that was held at the Foreign Ministry's Headquarters on Monday. Sheikh Sabah Al-Khaled reiterated Kuwait's unwavering support to the NATO since it joined NATO's Istanbul Cooperation Initiative in 2004; an initiative that aims to contribute to long-term global and regional security by offering countries of the broader Middle East region practical bilateral security cooperation with NATO.

Intelligence Minister: Security Forces Acting on Leader's Recommendations on Foreign Influence
Fars News Agency, 2016 02 26
Tehran - **Intelligence Minister Seyed Mahmoud Alavi said Iran's security forces are working round the clock to ensure the full implementation of the Supreme Leader's recommendations as regards protecting the country against foreign influence**. "Supreme Leader of the Islamic Revolution (Ayatollah Seyed Ali Khamenei) said foreign influence is a threat, the strategy has to be derailing such influence, and the security and intelligence authorities should be highly sensitive to it," Alavi said Friday after casting his votes for the Parliamentary and Assembly of Experts elections in Tehran. He said the intelligence ministry and security forces are acting on the Leader's recommendations accordingly. Alavi also lauded the high turnout at the Friday vote. Iranian voters queued up at the polling stations in hotly-contested elections on Friday to choose their legislators for the next four years.

Nuclear physicist part of Iran spy ring
Saudi Gazette, Mansour Al-Shihri, 2016 02 25
Riyadh - **More and more skeletons are tumbling out of the closet everyday during the trial of 32 people accused of spying for Iran. A Saudi defendant on trial at the Criminal Court in Riyadh on Tuesday turned out to be a nuclear physicist**. The spy ring consists of 30 Saudis, an Afghan national who worked as a cook at a Bukhari rice restaurant and an Iranian who speaks fluent Arabic. Another Saudi defendant was a senior bank official. But neither his name nor the bank where he worked has been revealed. On Tuesday, the third day of the court sessions, eight of the defendants stood before the court. They consisted of six Saudis, the

Iranian and the Afghan whom the court provided with an interpreter. The nuclear physicist told the judge that he had worked in China for six years. The Iranian suspect refused a lawyer and said he would defend himself.

Shin Bet: Number of Terror Victims in 2015 Highest in Seven Years
Haaretz, Gili Cohen, 2016 02 24
Jerusalem - **The number of terror attack victims in 2015 was the highest since 2008, Shin Bet data published on Tuesday said. According to the Shin Bet, 28 people were killed last year in terror attacks, most of them civilians - two were foreigners, one was Palestinian, three were members of the security services, and the rest were Israeli civilians. The Shin Bet** noted that in 2015 there was a slight decline in the number of terror attacks in the West Bank compared to the previous year, but the attacks that happened were more severe. In Jerusalem, the Shin Bet noted, the number of attacks rose: 92 percent of the attacks were firebomb throwing incidents, and only a small fraction of the attacks involved firearms. The Shin Bet said that the assailants in the ongoing terror wave are mostly youngsters, with no group affiliation. However, the Shin Bet said that Hamas poses the central threat in the West Bank due to its efforts to rebuild its militant command posts.

NGOs charge Shin Bet with outsourcing torture to PA, state denies
Jerusalem Post, Yonah Jeremy Bob, 2016 02 24
Jerusalem **- The NGOs B'Tselem and Hamoked on Wednesday accused the Shin Bet (Israel Security Agency) of outsourcing torturing Palestinian detainees to the PA as well as other direct abuses of detainee rights**. The allegations were also directed at the IDF, the police and the Prisons Service, though the Shin Bet got the lion's share of the criticism, with the main focus on the Shin Bet's Shikma Prison in the South. The Justice Ministry denied the claims in the NGOs' report, saying they "distort the existing reality" of detainee treatment, which it said complies with all legal requirements. Focusing mainly on affidavits and witness accounts provided by 116 Palestinians held for security reasons and interrogated at the Shikma facility, the period covered by the report is August 2013-March 2014 and comes in the aftermath of a firestorm over alleged recent torture of right-wing Jewish detainees.

Iran spy network includes professor, student
Saudi Gazette, Mansour Al-Shihri, 2016 02 24
Riyadh **- A cell of 32 people accused of spying for Iran includes a professor at King Saud University in Riyadh and a student at Imam Muhammad Bin Saud Islamic University, court sources have said**. They did not disclose the names but said the suspects also included an academician who held the job of "development researcher" at the Ministry of Education for more than 25 years. The Criminal Court in Riyadh began its sessions on Sunday to try the suspects and has so far listened to the charges against 16 of them. The list of charges against the accused was presented by the attorney general who accused them of high treason and called for capital punishment. The court sources said one of the defendants was assigned three lawyers to defend him while another gave power of attorney to eight members of his own family. The suspects also included an Afghan national and an Iranian who appeared before the court of Tuesday.

Return to Table of Contents/ Retour à la table des matières

Asia/Asie

Telegram founder expresses concern over anti-terror bill

The Korea Times, 2016 02 28
Barcelona— **Pavel Durov, the founder and CEO of secure messaging app Telegram, has expressed concern over the South Korean government's push for an anti-terrorism bill**, citing possible infringements of privacy and potential abuses of surveillance by the authorities. The Park Geun-hye administration and the main opposition Minjoo Party of Korea (MPK) have been clashing over a bill that, if passed in the National Assembly, will grant the **National Intelligence Service (NIS)** greater authority to investigate individuals and organizations and collect information on the private communications of citizens. President Park and the governing Saenuri Party are calling for the Assembly to approve the bill in order to establish powers, they say, which can help counter threats from North Korea and militant organizations such as the Islamic State group.

Official renews call for parliamentary approval of anti-terrorism bill
Yonhap News Agency, 2016 02 26
Seoul— The presidential office on Friday asked the parliament to endorse an **anti-terrorism bill** in the latest push to try to **better protect South Korea from any possible terror attacks**. Presidential spokesman Jeong Yeon-guk expressed hope that the National Assembly "would take into account public safety exposed to terror threats." Opposition lawmakers staged a marathon filibuster for the third straight day Friday, dimming prospects of any bipartisan breakthrough on the bill. The rival parties have been at odds over how much power the **National Intelligence Service,** South Korea's spy agency, should be given in pursing suspected terrorists. The main opposition Minjoo Party is concerned about giving far-reaching authority to the spy agency, citing possible power abuse by the agency.

Defense Minister inspects readiness of military's counter-terror units
Yonhap News Agency, 2016 02 25
Seoul - **Defense Minister Han Min-koo inspected the combat readiness of the military's special counter-terror units Thursday as the government recently warned of possible terror attacks by North Korea.** Han visited the Special Warfare Command's counter-terror unit and a special chemical warfare battalion to check the forces' battle preparedness earlier in the day, the ministry said in a statement. The defense chief instructed the troops to maintain a "thorough readiness position" against possible terrorist attacks from North Korea, the statement said. Han is "aware of the seriousness of the current state where North Korea's terror threats are increasing after (leader) Kim Jong-un ordered increased terrorist forces against South Korea," the statement also noted. Last week, President Park Geun-hye warned of possible terror or cyberattacks by North Korea. "New types of threats such as terror (attacks), cyberattacks or biological weapons could occur anywhere," Park said in a meeting with mayors and governors. On Tuesday, North Korea threatened to launch a "pre-emptive strike" on the presidential office Cheong Wa Dae and the United States mainland in a statement by the Supreme Command of the (North) Korean People's Army as it denounced joint military exercises between Seoul and Washington, slated to start early March. (full article)

Africa/Afrique

Dans les geôles de Bujumbura
Le Monde, Jean-Philippe Rémy, 2016 03 01
Bujumbura, **Burundi - Burundi, au pays de la peur 1|2 Depuis les manifestations d'avril 2015 contre le troisième mandat de Pierre Nkurunziza, la police ratisse la capitale. Des centaines de personnes sont jetées dans les prisons secrètes de la ville pour y être interrogées et souvent torturées.** Parfois même, elles en disparaissent On est ici en plein

coeur de Bujumbura, la capitale du Burundi. La cathédrale Regina Mundi est à deux pas. Le silence qui règne dans le **service national de renseignement (SNR)** n'en est que plus étrange. Tous les bruits - sons de cloche, conversations, circulation - sont étouffés par les nombreux murs. Le monde extérieur semble tenu à distance. Le SNR, qu'on appelle aussi de son ancien nom, " la Documentation ", est une planète en soi, avec ses règles. Et ses secrets.

Le Maroc et l'Allemagne conviennent de signer un « nouvel accord en matière de sécurité globale »
La Nouvelle Tribune (Maroc), Journaliste maison, 2016 02 29
Rabat, Maroc - **Le Maroc et l'Allemagne se sont mis d'accord sur la signature d'un nouvel accord en matière de sécurité globale devant couvrir toutes les formes de criminalité, particulièrement contre le terrorisme**, a affirmé, lundi à Rabat, le ministre de l'Intérieur, M. **Mohamed Hassad**. « Nous avons convenu de signer rapidement un nouvel accord en matière de sécurité globale qui englobe toutes les formes de criminalité, particulièrement contre le phénomène du terrorisme », a souligné M. Hassad dans une déclaration à la presse, à l'issue d'un entretien avec son homologue allemand **Thomas de Maizière**.

Why Algeria dissolved its powerful spy agency
Al Jazeera, Richard Nield, 2016 02 26
Algiers - **Algerian President Abdelaziz Bouteflika last month dissolved the Department of Intelligence and Security (DRS), the powerful state security service long seen as the nexus of political power in the country** - a move that has raised questions about the extent of power wielded by the country's intelligence apparatus. The dissolution of the DRS followed the removal of its long-standing chief, Mohamed Mediene, last September. Mediene, more commonly known as Toufik, had been head of the organisation for 25 years and was believed by many to be the real power behind the president. Senior figures in the DRS and the army were instrumental in propelling Bouteflika to the presidency in 1999. DRS support was also crucial to Bouteflika's successful re-election campaigns in 2004, 2009 and 2014. Now, the DRS will be replaced by the **Department of Surveillance and Security (DSS)** which, unlike its predecessor, will report directly to the presidency.

'Police algèrienne : Création d'une nouvelle unité antiterroriste
El Watan, Mohamed Fawzi Gaïdi, 2016 02 25
Alger - **La police algérienne aura bientôt son unité d'élite de choc. Selon des sources policières, une première promotion sortira dans quelques jours où elle est actuellement en fin de cycle de formation, dispensée par des experts spécialisés de la gendarmerie et de la police**. GOSP (Groupement opérationnel spécial de la police) est l'acronyme, illustré d'une tête de lion, qu'arborera l'uniforme noir de ses éléments encagoulés. Le quartier général de ce nouveau service sera basé à Boumerdès, l'épicentre d'une région où le terrorisme active toujours. Placé sous l'autorité directe du directeur général de la **Sûreté nationale (DGSN),** «le GOSP est appelé à intervenir dans des situations extrêmes, notamment le terrorisme urbain et le grand banditisme. Des événements de crise où il est nécessaire d'utiliser des techniques et des moyens spécifiques pour neutraliser des individus dangereux, soit par la négociation sinon l'intervention armée, assistée de snipers.

La nouvelle guerre qui ne dit pas son nom
All Africa, Journaliste maison, 2016 02 24
Paris - **Le quotidien Le Monde a fait état, mercredi 24 février, de la présence de forces spéciales** et d'agents secrets français en Libye. Selon le quotidien du soir, des forces spéciales sont présentes dans ce pays, où le service action de la Direction générale de la sécurité extérieure (DGSE) mène aussi « des opérations clandestines » contre des cadres du groupe

Etat islamique (EI). Début décembre, l'Elysée révélait que des avions de combat Rafale, embarqués à bord du porte-avion Charles-de-Gaulle, avaient mené des missions de reconnaissance les 20 et 21 novembre dans une zone située entre Syrte (bastion de l'EI) et Tobrouk. Depuis, de mystérieux vols d'avions ravitailleurs C135FR français ont été relevés au large de la Libye par le site spécialisé Flight Radar 24 sur Internet. Enfin, il y a eu le raid américain sur la base de l'organisation à Sabratha le 19 février. Raid dans lequel une cinquantaine de jihadistes a été tuée. Comme l'a révélé RFI, Sabratha était un camp d'entrainement de l'organisation de l'Etat islamique. C'est par ce camp que seraient passés les auteurs des attaques des hôtels de Sousse et du musée du Bardo en Tunisie.

Return to Table of Contents/ Retour à la table des matières

Americas/Amériques

Ex-spymaster Stiuso testifies befote Judie Palmaghini
Buenos Aires Herald, 2016 02 29
Buenos Aires— **Former Intelligence Secretariat (SI) Operations chief Antonio "Jaime" Stiuso** was testifying today for the second time in the investigation into the mysterious death of former AMIA special prosecutor **Alberto Nisman**, the case that thrust the spymaster out of the shadows and into the light. Stiuso appeared this morning before prosecutor Viviana Fein and Judge Fabiana Palmaghini, who were angered last week by a writ filed by prosecutor Ricardo Sáenz before the Buenos Aires City Appeals Court claiming that Nisman had been murdered. They fear today's testimony could be part of a manoeuvre to take the case to a federal court, a friendlier arena for San Isidro Federal Judge Sandra Arroyo Salgado, Nisman's ex-wife.

Palmaghini wants AFI to access Nisman's e-mails
Buenos Aires Herald, 2016 02 27
Buenos Aires— Agency hasn't responded to **judge's petition so far Judge Fabiana Palmaghini is seeking to involve the Federal Intelligence Agency (AFI) in the investigation into former AMIA special prosecutor Alberto Nisman's mysterious death**. The magistrate requested that the secret services intervene after the United States turned down a request for access to Nisman's e-mail accounts. The AFI is expected to tell Palmaghini — who took charge of the probe on December 17 — whether it has the necessary equipment to access two e-mail accounts, anisman@yahoo.com and algarfun@hotmail.com — which were reportedly used by Nisman to monitor the unregistered account he had in an US bank. Earlier this week, the judge also added a new e-mail account that was provided by former secret agent Carlos "Moro" Rodríguez, who appeared before Palmaghini and prosecutor Viviana Fein on February 15. Rodríguez told Fein and Palmaghini that the former AMIA special prosecutor used another e-mail account.

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

20-04-2016 to/au 26-04-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Could Brussels happen in Canada?
The Hill Times, Phil Gurski, 2016 04 25
Commentary: In the wake of the horrendous **attacks in Brussels, there has been a cascade of stories, op-ed pieces, and analyses of the event, ranging from why Belgian security services did not prevent it to whether more are on their way.** Political scientists, sociologists, and even a few former spies have weighed in, and the verdict is generally not kind to Belgium. Others have referred to the terrorist attacks as a watershed or a harbinger of worse to come. Are these dire prognoses correct? We here in Canada are also asking ourselves whether what occurred at the airport and metro station could happen here and whether the government should raise the threat level or take other action. It may be illustrative to examine what went wrong in Belgium and ask whether we are in a different situation here. First and foremost, many have called the attack a failure of intelligence. **There is no question that there are challenges in sharing information across the EU and even within Belgium itself. Security intelligence and law enforcement agencies should do a better job of coordination**, but this will be difficult in a union of 28 member states with wide ranging levels of experience and competence in counter terrorism. The story here **in Canada is markedly better. Information sharing at the federal level, especially between CSIS and the RCMP is very good**, and there are mechanisms to talk among federal, provincial, territorial and municipal partners. Relationships can always improve, but we are working from a solid base. Note: Phil Gurski worked for over 30 years as an intelligence analyst in Canada, including 15 at CSIS. He is the author of The Threat from Within: Recognizing Al Qaeda- inspired Radicalization and Terrorism in the West.

Social Media Emerges as a Valuable Terrorist Fundraising Tool
Investigative Project on Terrorism (via Breitbart News), Abha Shankar, 2016 04 21
Analysis - **Social media has emerged as a valuable and effective fundraising tool for terrorist groups.** The Internet's easy access and relative anonymity allows terrorist groups to solicit online donations from both supporters and unsuspecting donors who believe they are supporting a humanitarian or charitable activity. Terrorist groups have also been known to use crowdfunding websites to raise money by setting up a fundraising page ostensibly for charitable and humanitarian activities while collecting donations to bankroll their jihadi activities. "Terrorism financing continues to manifest itself in so many different ways with more recent developments coming in the form of the use of largely unregulated space of social media by terrorist groups such as ISIL [Islamic State of Syria and the Levant] for crowdfunding," Paul Jevtovic, head of Australia's financial intelligence unit, AUSTRAC (Australian Transaction Reports and Analysis Centre), said during a November regional security summit in Sydney. **In testimony before Canada's Standing Committee on National Security and Defense, Michael Peirce, a senior official with the Canadian Security Intelligence Service (CSIS), also highlighted the use of crowdfunding websites by terrorists to raise funds. "**The Internet age has given us the ability for people to go and put a public message seeking funds. They won't necessarily direct the full purpose of raising the funds. Again, they might do it under the cover of humanitarian aid,

but crowd share. 'I want to go carry out humanitarian aid in Somalia, please share funds,' and they set up a website, and funding flows through. It's quite a troubling development from the Internet."

The Troubling Questions After Terror Trial
Vancouver Sun, Ian Mulgrew, 2016 04 21
Column: The **Canada Day terror plot** trial has wrapped up, except for final submissions on whether the RCMP entrapped the hapless Surrey drug addicts convicted of the murderous 2013 scheme. **John Nuttall and Amanda Korody** will have been imprisoned for three years by the time B.C. Justice Catherine Bruce retires to deliberate this summer. Convicted by a jury last June of conspiracy to commit murder and possession of an explosive substance for terrorism, the pair faces life imprisonment. The verdict has been on hold, though, while the judge considered defence allegations that someone associated with the **Canadian Security Intelligence Service may have helped radicalize the couple in 2012** and set them up to be victimized by a sophisticated RCMP sting marred by misconduct. There is much that is troubling about this case. During the several months they were under surveillance by police and CSIS from late 2012 until their arrest on July 1, 2013, Nuttall and Korody were obviously vulnerable and challenged individuals.

Canada's spies closely watching quantum tech developments
Toronto Star, Alex Boutilier, 2016 04 20
Ottawa - **Canada's electronic spies are working on ways to defend government systems from the "impending threat" of quantum computing**, a document obtained by the Star shows. The **Communications Security Establishment warned chief Greta Bossenmaier that emerging quantum technology could "easily break" today's strongest methods of protecting electronic information**. "A new class of technologies that operates at quantum speeds is beginning to move from the domain of academic curiosity into the world of commercial technological reality," the memo, heavily censored and stamped secret, reads. "Quantum computing poses an impending threat to widely-deployed public-key cryptography (PKC) and therefore has a significant impact on any information being protected with PKC." Governments, journalists, activists and hackers have increasingly turned to public-key encryption to protect information. Journalists protect sources, activists and hackers protect themselves and the people they communicate with, and governments protect classified or sensitive information from theft or eavesdropping. When implemented correctly, it is very difficult for malicious actors -- even with serious resources and expertise -- to crack the code. But quantum technology greatly increases the power and speed of computer functions, allowing computers to break today's strongest encryption methods.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

ISIS Growing in Europe, U.S. Spy Chief Warns
New York Times, Eric Schmitt, Alissa J. Rubin, 2016 04 26
Washington - The **Islamic State is operating clandestine terrorist cells in Britain, Germany and Italy, similar to the groups that carried out the attacks in Paris and Brussels, the top-ranking American intelligence official said** on Monday. When asked if the Islamic State was

engaging in secret activities in those nations, the official, **James R. Clapper Jr.**, the **director of national intelligence**, said: "Yes, they do. That is a concern, obviously, of ours and our European allies." He then added, "We continue to see evidence of plotting on the part of ISIL in the countries you named." ISIL is another name for the Islamic State. Mr. Clapper, speaking to reporters at a breakfast meeting organized by The Christian Science Monitor, became one of the most senior Western officials to publicly acknowledge the Islamic State's extensive reach into Europe, which has set off growing fears among American and European spy services and policy makers. The Islamic State has vowed to conduct attacks in those three European countries. Western experts, however, emphasize that it is impossible to know where the next attack might take place.

CIA, torture and secrecy; Victims' lawsuit is aided by landmark Senate report on agency's tactics
Los Angeles Times, Rick Anderson, 2016 04 25
Los Angeles - It's the type of legal case that usually gets tossed out once the government claims national security is at stake. But something surprising happened in a federal courtroom here last week -- **a judge ruled that a potentially embarrassing lawsuit against the CIA could go forward**. And even more surprising, the Justice Department agreed to go along. This isn't to suggest the federal government is throwing in the towel in the suit filed by three alleged torture victims against two **CIA psychologists**. The government will continue to fight. But its approach to the case is different from similar suits in the past, and the shift can be traced in part to a landmark report on the CIA in 2014. The report, partially released by the Senate Select Committee on Intelligence, exposed the dark depths of the U.S. rendition and torture programs overseas, including waterboarding, beatings, mind-bending experiments and rectal feedings intended to provoke reluctant detainees to talk. Committee Chairwoman Sen. Dianne Feinstein (D-Calif.) urged Americans not to let such history be "forgotten and grievous past mistakes to be repeated." History, for example, like Suleiman Abdullah's. He is the lead plaintiff suing the psychologists.

The 'October Surprise' was real hints legendary spymaster in his final interview
Column: Newsweek, Nicholas Schou, 2016 04 25
Last spring, I spent a week in Washington, D.C., **hoping to interview national security reporters and former CIA officers for my upcoming book, Spooked: How the CIA Manipulates the Press and Hoodwinks Hollywood,** and one of the people I contacted was **Duane Clarridge**, who died from cancer on April 9. Known as much for his love of safari suits and cigars as for his spy-craft, **"Dewey" was the CIA's former Latin America director and the founding leader of the agency's counterterrorism center during the 1980s**. He also was one of the most high-profile culprits of the Iran-Contra scandal, in which Reagan administration officials illegally sold missiles to Tehran to help raise cash for anti-Communist rebels in Central America. In 1991, Clarridge was indicted for lying to Congress about his role in Iran-Contra, but President George H.W. Bush pardoned him the following year, along with five other intelligence officials. On April Fools' Day last year, I arrived at Clarridge's retirement community in northern Virginia. Looking relaxed in a red track suit and tennis shoes, he was waiting for me at a small wooden table at the clubhouse, where we began what would prove to be his last major sit-down interview.

Encryption hindering efforts to stop Islamic State, intelligence director says
Christian Science Monitor, Anna Mulrine, 2016 04 25
Washington - The **Edward Snowden leaks have accelerated the sophistication of encryption technologies by "about seven years," Director of National Intelligence James Clapper told reporters** this morning. And that is not a development to be celebrated, he added

in remarks at a breakfast hosted by The Christian Science Monitor. "From our standpoint, it's not a good thing." New, commercially available encryption software "had and is having major, profound effects on **our ability" to collect intelligence**, "particularly against terrorists," he warned. Clapper warned Monday that (Isis) has clandestine cells that are plotting more terrorist attacks in Germany, Italy, and England. To this end, the United States is stepping up efforts to promote more intelligence sharing. In the meantime, since the recent IS attacks on Paris and Brussels, US intelligence officials have learned some things about the terrorist group, he said. For starters, they are "very op-sec conscious," Clapper said. A former Air Force lieutenant general, he was using military parlance for "operational security."

Spy Chief Complains That Edward Snowden Sped Up Spread of Encryption by 7 Years
The Intercept, Jenna McLaughlin, 2016 04 25
Washington - The **Director of National Intelligence on Monday blamed NSA whistleblower Edward Snowden for advancing the development of user-friendly, widely available strong encryption.** "As a result of the Snowden revelations, the onset of commercial encryption has accelerated by seven years," James Clapper said during a breakfast for journalists hosted by the Christian Science Monitor. The shortened timeline has had "a profound effect on our ability to collect, particularly against terrorists," he said. When pressed by The Intercept to explain his figure, Clapper said it came from the National Security Agency. "The projected growth maturation and installation of commercially available encryption -- what they had forecasted for seven years ahead, three years ago, was accelerated to now, because of the revelation of the leaks."

Ex-CIA Agent Loses Appeal Against Extradition to Italy
Associated Press, Staff report, 2016 04 26
Lisbon - An **official says Portugal's Constitutional Court has rejected a former CIA operative's appeal against her extradition to Italy to serve a six-year sentence for her part in the U.S. extraordinary renditions program**. The court official has told The Associated Press that a judge ruled there were no constitutional grounds to reverse a decision by a lower court and the Supreme Court to send **Sabrina de Sousa** back to Italy. The official spoke on condition of anonymity Tuesday in accordance with court rules. De Sousa was among 26 Americans convicted in absentia for the 2003 kidnapping in Milan of suspect Osama Moustafa Hassan Nasr. The Constitutional Court was De Sousa's only remaining recourse after her arrest last October. Her Italian lawyer says he is hopeful of obtaining clemency from Italy's president.

U.S. Says Apple's Help No Longer Needed
The Wall Street Journal, Devlin Barrett, 2016 04 23
Washington - The **Justice Department on Friday night dropped a court case trying to force Apple Inc. to help authorities open a locked iPhone**, adding new uncertainty to the government's standoff with the technology company over encryption.In a one-page letter filed with a Brooklyn federal court Friday night, the government said an individual had recently come forward to offer the passcode to the long-locked phone. Accordingly, **the government no longer needs Apple's assistance to unlock the iPhone, and withdraws its application**."Apple declined to comment. Last week, Apple had asked U.S. District Judge Margo Brodie to drop the case, saying the government had failed to demonstrate that it had exhausted all other options before demanding the company's help.

On Encryption Battle , Apple Has Advocates in Ex-National Security Officials
The New York Times, Eric Lichtblau, 2016 04 23
Washington - In their years together as top national security officials, **Michael V. Hayden and Michael Chertoff were fierce advocates of using the government's spying powers to pry**

into sensitive intelligence data. Mr. Hayden directed a secret domestic eavesdropping program at the National Security Agency that captured billions of phone records after the attacks of Sept. 11, 2001. Mr. Chertoff pushed for additional wiretapping and surveillance powers from Congress both as a top prosecutor and as Homeland Security secretary.**But today, their jobs have changed, and so, apparently, have their views on privacy. Both former officials now work with technology companies like Apple at a corporate consulting firm that Mr. Chertoff founded, and both are now backing Apple — and not the F.B.I., with which they once worked — in its fight to keep its iPhones encrypted and private.**They are among more than a half-dozen prominent former national security officials who, to varying degrees, have supported Apple and the idea of impenetrable "end-to-end encryption" during a furious national debate over the balance between privacy and security in the digital age.In white papers, op-ed articles, conferences, newspaper and television interviews and elsewhere, the former officials have made their support for Apple clear.

Chinese firm at center of cyber fears
The Washington Post, Hayley Tsukayama & Dan Lamothe, 2016 04 23
Washington - Ever since Chinese computer maker Lenovo spent billions of dollars to acquire IBM's personal-computer and server businesses, **some lawmakers have called on federal agencies to stop using the company's equipment out of concerns over Chinese spying**.This past week, those lawmakers thought the Pentagon finally heeded their warnings. An email circulated within the Air Force appeared to indicate that Lenovo was being kicked out."For immediate implementation: **Per AF Cyber Command direction, Lenovo products are being removed from the Approved Products List and should not be purchased for DoD use.** Lenovo products currently in use will be removed from the network," stated the message. The apparent directive was generally welcomed as it circulated around Capitol Hill.Then the Pentagon's press office weighed in. Not so fast, it said.Ann Stefanek, an Air Force spokeswoman, said the message was mistaken, "not properly coordinated" and should not have been sent. Neither the Air Force nor the rest of the Defense Department has banned Lenovo products, she added.In fact, the "Approved Products List" referenced in the Air Force message focused on communications equipment such as routers, rather than personal computers, for which Lenovo is known. Army Lt. Col. Valerie Henderson, a Pentagon spokeswoman, said Lenovo has never been on that list.

Bay Area judge upholds FBI's secret national security letters
San Francisco Chronicle, Bob Egelko, 2016 04 22
San Francisco - A Bay Area **federal judge has upheld the FBI's power to keep secret the tens of thousands of "national security letters"** the agency issues each year demanding customer records from phone companies, banks and other record keepers. In 2013, U.S. District Judge Susan Illston of San Francisco ruled that the letters violated freedom of speech because they were accompanied by gag orders forbidding the recipients from disclosing that they had been contacted by the FBI. But she put her ruling on hold while the government appealed, and last year Congress passed a law, the USA Freedom Act, that made it somewhat easier to challenge national security letters in court and increased judges' authority to lift the veil of secrecy.

Color index for US border security is rejected
Associated Press, Staff report, 2016 04 22
San Diego - Five years ago, the **U.S. Department of Homeland Security dropped its color-coded terror threat index developed after the 9/11 attacks amid widespread confusion and ridicule**. So what did it do when tasked by Secretary Jeh Johnson in 2014 with measuring security along the country's borders? Agency staff proposed another system of reds, yellows

and greens. The Institute for Defense Analyses, a consulting firm, was hired by DHS to review the idea and found the index simplistic and misleading, noting that colors were a "disaster" for communicating terror threats. "DHS should learn from its own history and avoid repeating this error," the consultants said in its 53-page report. The DHS proposal was never made public, nor was the report.

Ex-CIA officer faces extradition from Portugal to Italy for alleged role in cleric's rendition
Washington Post, Ian Shapira, 2016 04 22
Washington - **More than 13 years after an Egyptian cleric was kidnapped off the streets of Milan by CIA operatives, one former agency officer now living in Portugal faces extradition to Italy and the possibility of a four-year prison sentence for the abduction** -- an outcome that a former agency historian describes as "unprecedented." **Sabrina De Sousa**, 60, was one of 26 Americans convicted in absentia by Italian courts for her alleged role in the February 2003 rendition of Hassan Mustafa Osama Nasr, also known as Abu Omar. Like the other convicted Americans, De Sousa never really faced the threat of Italian imprisonment, because she had moved back to the United States long before their Italian trials began. But last spring, De Sousa traveled to Portugal to visit relatives. In the fall, she was detained by local authorities at the Lisbon airport on a European arrest warrant. This week, Portugal's highest court upheld the country's lower courts' rulings, declared that they did not violate the constitution, and said De Sousa should be sent to Italy as soon as May 4.

F.B.I. Director Suggests Bill for an iPhone Hacking Topped $1.3 Million
New York Times, Eric Lichtblau, Katie Benner, 2016 04 22
Washington - The **director of the F.B.I. suggested Thursday that his agency paid at least $1.3 million to an undisclosed group to help hack into the encrypted iPhone** used by an attacker in the mass shooting in San Bernardino, Calif. At a technology conference in London, a moderator asked James B. Comey Jr., the F.B.I. chief, how much bureau officials had to pay the undisclosed outside group to demonstrate how to bypass the phone's encryption. "A lot," Mr. Comey said, as audience members at the Aspen Institute event laughed. He continued: "Let's see, more than I will make in the remainder of this job, which is seven years and four months, for sure." The F.B.I. director makes about $185,100 a year -- so Mr. Comey stands to earn at least $1.35 million at that base rate of pay for the remainder of his 10-year term.

Justice Department won't block CIA interrogation suit
Associated Press, Staff report, 2016 04 22
Washington - The **Justice Department has signaled that it won't try to block a lawsuit arising from the CIA's harsh interrogation techniques**, leaving the door open for a court challenge over tactics that have since been discontinued and widely discredited. Lawyers call the government's stance unprecedented, but also a recognition that a once-secret program is now largely out in the open. They say it's the first time the Justice Department has not sought, as its first step, to dismiss a lawsuit over the interrogation program by arguing that its mere existence is too secret to discuss in court. Judges have previously accepted that assertion, turning aside cases about a program that was designed to extract intelligence from suspected militants captured overseas. The lawsuit at issue, pending in federal court in Washington state, accuses the two Air Force psychologists who designed the interrogation program of endorsing and teaching torture tactics under the guise of science.

C.I.A. to Pay Death Benefits to Relatives of Terror Victims
New York Times, Nicholas Fandos, 2016 04 21
New York - For almost two years, the family of **Glen Doherty, a C.I.A. contractor and former Navy SEAL** who was among four Americans killed in the 2012 terrorist attack in Benghazi,

Libya, has fought to claim the government death benefits they believe Mr. Doherty deserved. **On Monday, the C.I.A. informed the Doherty family and others like them that their wait would end. The agency has secured funds to begin paying out death benefits of up to $400,000 each** to families like the Dohertys who are survivors of unmarried and childless federal employees or contractors killed in acts of terrorism overseas. The measure circumvents a 1941 law that requires overseas contractors -- including those working for the C.I.A. -- to carry disability and life insurance but pays out death benefits only to those with surviving spouses or children. Kate Quigley, Mr. Doherty's sister who led the family's lobbying efforts, said her brother, who had no spouse or children, did not know that his life insurance package would not pay any death benefits.

FBI urges agents to keep secrets - from each other ; Bureau doesn't want surveillance tactics revealed in court
USA Today, Brad Heath, 2016 04 21
Washington - The **FBI guards its high-tech secrets so carefully that officials once warned agents not to share details even with federal prosecutors for fear they might go on to work as defense attorneys**, newly disclosed records show. A supervisor cautioned the bureau's "technically trained agents" in a memo in 2003 not to reveal techniques for secretly entering and bugging a suspect's home to other agents who might be forced to reveal them in court. "We need to protect how our equipment is concealed," the unnamed supervisor wrote. The records, released this year as part of a Freedom of Information Act lawsuit, offer a rare view of the extent to which the FBI has sought to keep its most sensitive surveillance capabilities secret, even from others within federal law enforcement. That secrecy remains a common feature of the FBI's most sophisticated investigations, including recent cases in which it cracked the encrypted iPhone of a gunman in last year's San Bernardino, Calif., terror attacks and breached the anonymous **Tor computer** network.

U.S. court rejected claim FBI use of spy data is unconstitutional
Reuters, Staff report, 2016 04 21
Washington - The **top judge on the secretive Foreign Intelligence Surveillance Court ruled last year against a constitutional challenge to U.S. surveillance rules permitting the FBI to access foreign intelligence data** for use in domestic criminal investigations, according to a newly declassified court opinion. **Judge Thomas Hogan** said there was no requirement that access to email and other forms of Internet communications under a controversial surveillance program be restricted only to foreign intelligence uses, he wrote in a November opinion released this week in partially redacted form. Hogan's ruling dismissed a legal challenge submitted by **Amy Jeffress**, a former federal prosecutor, who was appointed to serve as a "friend of the court" to advocate privacy considerations before the court.

F.B.I. Tells Panel It Needs Hackers to Keep Up With Tech Companies
New York Times, Cecilia Kang, Eric Lichtblau, 2016 04 20
Washington - The F.**B.I. defended its hiring of a third-party company to break into an iPhone used by a gunman in last year's San Bernardino, Calif., mass shooting**, telling some skeptical lawmakers on Tuesday that it needed to join with partners in the rarefied world of for- profit hackers as technology companies increasingly resist their demands for consumer information. **Amy Hess, the Federal Bureau of Investigation's executive assistant director for science and technology**, made the comments at a hearing by members of Congress who are debating potential legislation on encryption. The lawmakers gathered law enforcement and Silicon Valley company executives to discuss the issue, which has divided technology companies and authorities in recent months and spurred a debate over privacy and security. The hearing follows a recent standoff between the F.B.I. and Apple over a court order to force

the company to help gain access to an iPhone used by one of the San Bernardino attackers. Apple refused to comply with the order, citing harm to the privacy of its users.

FBI can't unlock 13% of protected phones it seized
USA Today, Erin Kelly, 2016 04 20
Washington - **The FBI cannot unlock 13% of the password-protected cellphones it has seized as evidence in the past six month**s, a top bureau official told a House panel Tuesday. About 30% of the 3,000-plus phones that the FBI has seized since Oct. 1 require passwords to open, said **Amy Hess**, executive assistant director of the FBI's science and technology branch. The FBI was able to unlock most of those phones, but the number that they can't get into is growing as tech companies build devices with stronger data encryption, Hess said. She also said passwords are becoming longer and more difficult to guess, even with special computer programs designed to crack them.

Judge Rejects Challenge to Searches of Emails Gathered Without a Warrant
New York Times, Charlie Savage, 2016 04 20
Washington - A **federal judge has rejected a legal challenge to rules permitting F.B.I. agents, when working on domestic criminal cases**, to search emails written by Americans that the government has intercepted without a warrant in the name of gathering foreign intelligence. In an 80- page opinion that was issued in November and remained classified until being made public on Tuesday, **Judge Thomas F. Hogan**, the chief judge of the Foreign Intelligence Surveillance Court, ruled that what critics call "backdoor searches" of messages by the F.B.I. comply with both the **Constitution and the FISA Amendments Act**.

Secret U.S. court issues first order for phone data under new law
Reuters, Mark Hosenball, 2016 04 19
Washington - **The secretive U.S. Foreign Intelligence Surveillance Court has issued its first order allowing the National Security Agency to collect telephone records under a new electronic spying law** Congress passed last year. According to an order from the court posted Tuesday on a website operated by the **Office of the Director of National Intelligence**, the court issued the order on Dec. 31. The order, signed by FISC Chief Judge **Thomas Hogan**, said the court concluded that a surveillance application, apparently submitted by the NSA, met the requirements of the USA Freedom Act, which President Barack Obama signed last year. That law replaced an older one that allowed NSA to collect telephone "metadata" - records of American citizens' and residents' calls, including their origin and destination, when a call was placed and how long it lasted. However, U.S. intelligence officials have said the NSA did not collect the content of phone calls under this program and did not look at the data without some specific justification.

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

Tech: A double-edged sword for national security
Tech City News (UK), Emily Spavin, 2016 04 26

London - "I remember my first day at Mi6. I thought it was probably going to be nothing like the James Bond books and films. 'It'll just be a desk job', I told myself. I was wrong." **Matthew Dunn** now lives in Gloucestershire and writes spy novels for a living - an interesting enough way to earn a crust, but his previous career is much more fascinating. **He served as a British intelligence officer and Mi6 field officer, taking part in around 70 missions that saw him travel the world, moving undercover from one hostile environment to another**. "I was tasked with targeting senior echelons, people who had access to secrets in rogue states that offered significant threats in terms of things like regional conflicts, nuclear conflicts and hostile threats against the West in the guise of intelligence attacks or military attacks," Dunn explained. He used his training in all aspects of intelligence collection and direct action, including explosives, military unarmed combat, surveillance, advanced driving, infiltration techniques and covert communications, with one particular mission earning him a rare personal commendation from the Secretary of State for Foreign and Commonwealth Affairs.

Former Top U.K. Spy Now Works for Team Putin--and a Mobbed-Up Russian Lawyer
The Daily Beast, Michael Weiss, 2016 04 25
Washington - If Robert Ludlum and Bertolt Brecht ever collaborated on a plotline, they might have come up with something like "**The Browder Effect**," which aired on April 13 on Rossiya-1 as a two-hour documentary and follow-up discussion. **In this paranoid rendering, Alexey Navalny, the leader of Russia's decimated opposition, is an agent of either the CIA or MI6 (or maybe both, it's never explained) who was recruited in 2006 by William Browder, the CEO of Hermitage Fund** and a onetime apologist for Russian President Vladimir Putin who had turned into a prominent Kremlin gadfly. Browder, in this rendering, was himself recruited by MI6 in 1995. But what's so interesting about the broadcast of "The Browder Effect" is that a key source lending ostensible credibility to the allegations is named as Andrew Fulton, a former high-ranking MI6 spy once implicated in a plot to assassinate Slobodan Milosevic. His opinion was presented on air as that of an independent analyst who verifies the authenticity of these dubious documents. In fact, email correspondence leaked online and independently verified by The Daily Beast by a source who asked to remain anonymous, shows that Fulton has been working as a private investigator for Andrey Pavlov, the lawyer for the alleged Russian mafia types accused of committing the crimes the television channel is trying to pin on U.S. and British intelligence.

Dark Days': UK Spy Agency Files Reveal Bulk Data Capture of Citizens
Sputnik News, 2016 04 24
London - The **bulk personal datasets collected by British intelligence agencies is reminiscent of dark days and dark regimes, Yair Cohen, of the London-based law firm Cohen Davis Solicitors, told Sputnik**.In an interview with Sputnik, Yair Cohen, of the London-based law firm Cohen Davis Solicitors, slammed the UK intelligence agencies' bulk personal datasets (BPD) as a reminder of dark days and dark regimes.The interview came after the human rights **watchdog Privacy International managed to obtain a cache of documents which shed light on the UK spy agencies' controversial BPDs**. This is the collection of personal data of people, most of whom present no particular interest to the intelligence services."It appears that the vast majority of data was supplied on a volunteer basis. I suspect that some of the information was being supplied by email providers or organizations that handled emails as well," Cohen said.

UK guards 'powerless to stop jihadi suspects'
London Daily Telegraph, David Barrett, Camilia Turner, 2016 04 22
London - **British border guards are virtually powerless to stop and detain Britons they suspect of returning from jihad or terrorism training**, a whistleblower claims today. UK

Border Force guards have "zero discretion" to detain and interview travellers trying to re-enter Britain if they hold a UK passport and have not been "flagged" by police or security services. It means that the UK border has a potentially fatal flaw in relation to "cleanskin" jihadis, who have never come to the attention of police but could go on to commit atrocities on British soil. **The Terrorism Act 2000** sets out how immigration officers could be granted the power to "stop, question and detain" anyone they believe is "concerned in the commission, preparation or instigation of acts of terrorism". However, these powers have not been conferred on immigration and borders staff. The Home Office whistleblower, who The Daily Telegraph is not identifying, said it was a "glaring omission" that border guards have been forbidden from using the powers set out in Schedule 7 of the Act.

Border security budget to fall by £2 million, Theresa May confirms
London Daily Telegraph, David Barrett, 2016 04 21
London - The **Government is to cut the UK Border Force's resource budget by £2 million this year despite fears over Britain's border security**. A debate in the House of Commons, which highlighted The Telegraph's campaign examining worrying shortcomings in border security, said the agency's budget - which covers staffing - will decline by 0.4 per cent to £558 million. However, **Theresa May**, the Home Secretary, insisted border spending had been "protected" because capital spending on technology such as electronic passport gates will rise from £40.1 million last year to £68.3 million. She told the Commons: "That means that Border Force spending to all intents and purposes is protected compared to 2015-16 with increased capital investment to improve the technology at the border, to **improve security and intelligence and strengthen control**."

UK spy agencies have collected bulk personal data since 1990s, files show (Canada)
The Guardian (London), Owen Bowcott, Richard Norton-Taylor, 2016 04 21
London - **Britain's intelligence agencies have been secretly collecting bulk personal data since the late 1990s** and privately admit they have gathered information on people who are "unlikely to be of intelligence or security interest". **Disclosure of internal MI5, MI6 and GCHQ documents reveals the agencies' growing reliance on amassing data as a prime source of intelligence** even as they concede that such "intrusive" practices can invade the privacy of individuals. A cache of more than 100 memorandums, forms and policy papers, obtained by Privacy International during a legal challenge over the lawfulness of surveillance, demonstrates that collection of bulk data has been going on for longer than previously disclosed while public knowledge of the process was suppressed for more than 15 years. The files show that GCHQ, the government's electronic eavesdropping centre based in Cheltenham, was collecting and developing bulk data sets as early as 1998 under powers granted by section 94 of the 1984 Telecommunications Act. The documents offer a unique insight into the way MI5, MI6, and GCHQ go about collecting and storing bulk data on individuals, as well as authorising discovery of journalists' sources. Bulk personal data includes information extracted from passports, travel records, financial data, telephone calls, emails and many other open or covert sources. Often they are "fused" together to help pinpoint suspects. Bulk personal data is exchanged with "foreign agencies", presumably mainly those from other countries in the UK's traditional **"Five Eyes" alliance - the USA, Canada, Australia and New Zealand.**

We cannot be complacent about security in face of Islamist attacks, says former spy chief
London Daily Telegraph, Tom Whitehead, 2016 04 21
London - A **former spy chief** has joined calls for a review of border security as he warned Britain cannot afford to be complacent. **Sir David Omand**, who was director of GCHQ in 1996 and 1997, said the main focus of any review must be on whether there is adequate staffing at

our ports and points of entry and whether intelligence sharing is at its best. It came as a former head of the Royal Navy warned Britain's coastline away from major ports is "highly vulnerable". Mr Omand spoke a day after former senior policemen and counter terrorism experts signed an open letter calling for the UK's borders to be tightened, to better protect against the threat from Islamist fanatics. Sir David told this newspaper: "I welcome any rational review. We can never be complacent about these things." He said the main drive of a review should examine staffing levels and training at the borders, amid concerns that they are under pressure.

Border Security: How the US and Britain compare
London Daily Telegraph, David Barrett, Nick Allen, 2016 04 20
London - The **United States deploys a much tougher regime than Britain to hunt down Islamists in their midst** and screen out potential extremists who attempt to reach American soil. Intelligence and security The **US deploys its formidable intelligence network to keep out extremists and other undesirables,** drawing on the surveillance capabilities of agencies including the **CIA and the National Security Agency**. In comparison, Britain takes a more softly-softly approach. The Home Office places heavy emphasis on community-based schemes, as part of the Prevent strategy, to encourage Muslim families, imams and other community leaders to report concerns about potential extremism. Raffaello Pantucci, of the British think-tank the Royal United Services Institute, said US intelligence agencies take a more "vigorous, pro-active approach", including extensive surveillance, to track down potential terrorist threats. "A lot of that is based on surveillance of online activities, which then leads to further action in the offline world," Mr Pantucci said.

GCHQ should split into separate defence and attack units, says expert
Computing (UK), Stuart Sumner, 2016 04 20
London - **Government listening agency GCHQ should be split into separate attack and defence units, reporting to the Cabinet via different government ministers**, according to a leading security expert. This would allow the body responsible for defence to operate more openly, and would make other public and private organisations more likely to collaborate with it, according to Professor Ross Anderson, professor of security engineering at the computer laboratory, University of Cambridge. "The problem is that the UK government has demonstrated repeatedly that it's not trustworthy," said Anderson. "The Snowden documents made it clear that the British State is more interested in exploiting stuff than protecting it. If you find a vulnerability in Windows, do you report it to Microsoft and protect 60 million Brits, or do you keep quiet and exploit a billion Chinese, a billion Indians and around 100 million Russians? From a GCHQ perspective it's a no brainer," he argued.

Return to Table of Contents/ Retour à la table des matières

Australia/ Australie

Australia PM launches cybersecurity campaign
Reuters, 2016 04 21
Sydney - **Australia set out a far-reaching cybersecurity strategy on Thursday**, invoking the leaks of United States whistleblower Edward Snowden, terrorism and even the threat of war to push for a coordinated global approach to protection of online data.Prime Minister Malcolm

Turnbull, who faces an election in July amid waning popularity, is trying to position himself as a leader who can transform Australia into a tech-savvy business hub as its economy deals with a commodities downturn. In a speech in Sydney, the former online entrepreneur said hacking attacks cost the country A$1 billion ($780 million) a year and unveiled a long list of measures - from appointing his own special cybersecurity adviser to having internet safety taught in schools - to make the online world freer and safer. Turnbull, who delivers his first budget in May, two months before the election, said he wants to spend A$230 million on 33 cybersecurity measures involving 100 new jobs, including extra resources for the government's Computer Emergency Response Team, and law enforcement agencies. He **also plans to relocate the cybersecurity office of intelligence agency, the Australian Signals Directorate, outside the broader Australian Security Intelligence Organisation to make it easier to coordinate with busineses.**

Asio backs down in bid to keep security assessment 'law' secret
The Guardian, Paul M. Farrell, 2016 04 20
Canberra— **Australia's domestic spy agency sought to suppress parts of a document which it was argued forms part of Australian law – and would therefore usually be available to the public** – to fight a legal challenge to a security assessment it made. Evidence has also emerged in the case of junior officers allegedly making "embellishments" in a security report to the **director general, Duncan Lewis**.Court documents reveal the extraordinary lengths the **Australian Security Intelligence Organisation (Asio)** has gone to to fight a judicial review of an adverse security assessment of a man currently held in immigration detention. The man, who cannot be named for legal reasons, is challenging his security assessment in the federal court, in part, because he alleges the Asio officers who interviewed him embellished facts in a report to the director general. He also claims they attributed comments to him that he did not make.

UK spy agencies have collected bulk personal data since 1990s, files show
The Guardian, staff reporters, 2016 04 20
London— Agencies privately concede that 'intrusive' practices can invade privacy and that data is gathered on people 'unlikely to be of interest." **Britain's intelligence agencies have been secretly collecting bulk personal data since the late 1990s and privately admit they have gathered information on people who are "unlikely to be of intelligence or security interest". Disclosure of internal MI5, MI6 and GCHQ documents reveals the agencies'** growing reliance on amassing data as a prime source of intelligence even as they concede that such "intrusive" practices can invade the privacy of individuals. A cache of more than 100 memorandums, forms and policy papers, obtained by Privacy International during a legal challenge over the lawfulness of surveillance, demonstrates that collection of bulk data has been going on for longer than previously disclosed while public knowledge of the process was suppressed for more than 15 years. The files show that GCHQ, the government's electronic eavesdropping centre based in Cheltenham, was collecting and developing bulk data sets as early as 1998 under powers granted by section 94 of the 1984 Telecommunications Act. The documents offer a unique insight into the way MI5, MI6, and GCHQ go about collecting and storing bulk data on individuals, as well as authorising discovery of journalists' sources.

Return to Table of Contents/ Retour à la table des matières

New Zealand/Nouvelle-Zélande

Light coverage/couverture légère.

Return to Table of Contents/ Retour à la table des matières

International

China/Chine

Spy alert: foreign Romeos leave China dolls in chains
The Australian, Rowan Callick, 2016 04 23
Canberra - **David**, who is living in Beijing for a while, has red, wavy hair and a pointy nose, and wears glasses. He could be taken for Woody Allen.He claims to be "a visiting scholar researching issues about China". And he starts dating a "pretty lady", Xiao Li, who recently started work in a government agency. **But he's really a foreign spy.Spoiler alert: This romance will end in tears.China has introduced a National Security Day to alert people to the need to be guarded about what information they share, and with whom, and to keep their eyes peeled for foreigners with evil intent.**The cautionary tale of David and Xiao Li has been related in posters distributed around apartment compounds in Beijing's oldest district, Xicheng, this week.In Nanjing, the city authorities responded to the new security day by highlighting to schoolchildren the case — clearly intended to scare them — of the Australian citizen Stern Hu. Hu was jailed for 10 years in 2010 for "stealing business secrets" and for accepting bribes to ensure certain steel companies received shipments of iron ore from his employer, Rio Tinto, during a time of excess demand.China Central TV used the example on Wednesday night, as part of a series of reports on national security concerns, of Chen Wei — who was arrested in December 2013 in the port city of Ningbo, near Shanghai, after he was seen taking photographs at the East Fleet naval centre.While working for a joint- venture company, he had met a foreigner — with a Japanese- sounding name — who asked him to provide some photos, at first of Christians worshipping in China then of ships in port, especially those equipped with weapons, and of the routes of vessels sailing to the Diaoyutai Islands contested with Japan, which administers them as the Senkaku Islands.

Chine : Xi Jinping en « commandant en chef »
Le Figaro, Patrick Saint-Paul, 2016 04 22
Pekin--Campé dans son uniforme militaire aux couleurs camouflage, **Xi Jinping vient de s'offrir un nouveau titre prestigieux : « commandant en chef » des armées.** L'annonce est intervenue, mercredi, alors que le numéro un chinois visitait le nouveau centre de commandement interarmées du pays, dont il a pris la direction. Le dirigeant communiste consolide ainsi son emprise sur l'armée. Et la formulation ne laisse rien au hasard, puisqu'elle est identique à celle attribuée au président des États-Unis, signalant ainsi que le dirigeant de la République populaire se place sur un pied d'égalité avec son alter ego américain. Les images du « commandant en chef » , apparu pour l'occasion en treillis, sans insigne ni grade, ont été diffusées à la télévision publique et par les médias d'État. **L'Armée populaire de libération (APL) se doit d'être « totalement loyale » , a martelé Xi Jinping.** Et d'ajouter que l'APL doit

être « ingénieuse dans la bataille, efficace dans le commandement, audacieuse et apte à remporter des guerres » .

Overseas security to get upgrade
China Daily, Zhong Nan, 2016 04 22
Beijing - **China will beef up its private security services overseas to protect life and property, with stronger manpower, better equipment and intelligence, and more effective operations**, industry analysts and insiders said on Thursday. The country now has about 3,200 security professionals protecting Chinese companies overseas. That is far fewer than major global security service providers such as US-based Blackwater Worldwide, which has more than 23,500 employees around the world and has trained over 100,000 professionals, data from the **China Overseas Security and Defense Research Center** in Beijing show. Large companies, including China Security and Protection Co and JAS Security Group, both based in Beijing, plan to recruit more professionals, as well as to establish an industry union to integrate resources of China's 20 largest security service companies to gain more contracts. Tools including multifunctional safety rooms, armored vehicles, anti-bomb walls, police dogs and chemical defense equipment will help them upgrade their ability to protect such clients as China National Petroleum Corp and China Road and Bridge Corp in Africa and Latin America. Liu Xinping, deputy director of the China Overseas Security and Defense Research Center, said members of the union will share intelligence, maritime-and land-based logistics networks, base facilities and defense equipment.

PLA orders anti-spy software for soldiers' smartphones
South China Morning Post, Minnie Chan and Celine Ge, 2016 04 20
Beijing - The **People's Liberation Army (PLA) has come up with comprehensive counter-espionage software** since it lifted a ban on its soldiers using smartphones in their spare time, state media reported on Monday. All devices used by PLA soldiers should be installed with special software created by the army's IT experts and domestic mobile operators, so their activities can be closely monitored by the army's newly established internet administration centres, according to Communist Party mouthpiece People's Daily. The software aims to filter all "unhealthy and negative messages" that could harm the army's political spirit and morale, curb access to sensitive information that might lead to leaking of military intelligence, the report said. It also tracks off-duty officers incase they visit "unwanted places".

Spy who sold codes sentenced to death
South China Morning Post, Liu Zhen, 2016 04 20
Beijing - **China has sentenced to death an employee at a scientific research institution for espionage. Huang Yu**, 41, sold more than 150,000 classified documents to foreign intelligence agencies, CCTV reported. These included 90 "top confidential", 292 "confidential" and 1,674 "secret" files which leaked cipher codes for Communist Party, government, military and financial communications. "This case would have led to bloodshed and cost lives had it happened in wartime," the television report quoted a National Security Agency official as saying. The report did not say for whom Huang was spying.

Xi vows to boost cyber Deterrence
South China Morning Post, Catherine Wong, 2016 04 20
Beijing - **China will beef up its cybersecurity capabilities, including cyber deterrence, President Xi Jinping said yesterday**, a move analysts said was needed to counter other countries' capabilities. Speaking to senior officials, engineers and information technology executives, Xi encouraged internet firms to expand globally and told governments bodies to help companies lure global talent to work in China's internet sector. Xi said **accelerated**

development of China's cybersecurity systems was needed to protect key information infrastructure and to "strengthen cyber defence and deterrence capabilities". The new five-year plan, passed in March, devotes much attention to the development of the internet sector and cybersecurity, including cyber defences. But it does not mention "cyber deterrence". Last year, the US defence department updated its cyber strategy to include "cyber deterrence". "Some countries would use supremacy in cyber power to attack other countries," said Huang Chengqing, director of the National Computer Network Emergency Response Technical Team/Coordination Centre of China, who was at the meeting.

Return to Table of Contents/ Retour à la table des matières

Russia/Russie

Putin Builds New Force To Tighten Security Grip
Wall Street Journal, Thomas Grove, 2016 04 25
Moscow - The **Kremlin is creating a new internal security force that answers directly to Russian President Vladimir Putin**, ahead of parliamentary elections. The Russian government says the new force, called the **Russian Guard**, **will be headed by Viktor Zolotov**, who served as Mr. Putin's personal bodyguard for 13 years. Mr. Putin directed the creation of the force this month through an executive order now under review by the lower house of parliament. Mr. Putin said the security force is intended to tighten control over the arms trade in the country and streamline counterterrorism efforts. "We believe we can. . .reduce the cost of having various services," he said in a televised question-and-answer session. With parliamentary elections set for September, Russian security experts said the new force will be capable of putting down the kind of mass protests that arose following allegations of voting violations in the last such polls in 2011. "This is really about upcoming elections and the possibility of mass unrest," said Boris Volodarsky, a former Russian military intelligence officer.

Eye-Watering Spies: Russia's State-Of-The-Art Jets Stir Envy in Washington
Sputnik News Service, 2016 04 23
Moscow - **Russia's military modernization program and impressive improvements within conventional forces arsenal, especially its signals intelligence (SIGINT)** and electronic warfare (EW) capabilities have apparently come as a big surprise to Washington.In Syria, Russia has supposedly deployed two **Electronic Intelligence (ELINT) and SIGINT aircraft**, which "may be gaining the envy of some in Washington", according to Caitlin Patterson, a veteran of the US Marine Corps where she served as Cryptologic Linguist and Signals Intelligence Analyst.One of the planes is Ilyushin Il-20 surveillance aircraft, "Coot" in NATO code."The Il-20 comes packed with an array of sensors, antennas, IR (Infrared) and Optical sensors, a SLAR (Side-Looking Airborne Radar), and satellite communication equipment for real-time data sharing," Patterson describes the aircraft.The Il-20 is a military version of the Il-18 passenger airplane. It was designed for intelligence gathering with its distinguishing features being the Igla-1 phased-array SLAR pod under the forward fuselage, housings for A-87P LOROP cameras and the Romb 4 sigint system, according o the GlobalSecurity.com website.Two antennas also protrude from the top of the fuselage for the Vishnaya communications intelligence gathering system.It is flown by a crew of five accompanied by eight mission specialists.

Return to Table of Contents/ Retour à la table des matières

Europe

Les moyens manquaient pour suivre les frères Abdeslam
Le Soir (Belgique), Journaliste maison, 2016 04 26
Paris - Le Comité P pointe les failles qui ont abouti au classement sans suite du dossier de surveillance des deux terroristes. C'est ce mardi qu'est rendu public le second rapport intermédiaire du Comité P évaluant l'enquête sur les auteurs des attentats de Paris. Le Soir a pris connaissance des grandes lignes de ce rapport. La police des polices met en lumière une série de « manquements » qui ont permis à Salah et Brahim Abdeslam d'échapper à la surveillance dont ils auraient dû faire l'objet. On apprend ainsi que début 2015, un inspecteur de Bruxelles-Ouest signale par P.-V. à la cellule antiterroriste de cette zone de police que les frères Abdeslam cherchent à se rendre en Syrie. Ceux-ci sont auditionnés sans faire l'objet d'aucune inculpation. Informé des faits, le parquet demande à l'unité antiterroriste de la police fédérale d'enquêter sur la téléphonie des frères Abdeslam et de vérifier leurs mails. Mais l'enquête finira parmi les « dossiers rouges » : ceux qui sont urgents mais pour lesquels la section antiterroriste ne dispose pas de moyens suffisants.

Les écoutes judiciaires ont coûté un milliard d'euros depuis dix ans
Le Figaro, Pauline Chateau, 2016 04 26
Paris - Dans un courrier adressé au Premier ministre, la Cour des comptes dénonce le coût exorbitant des interceptions judiciaires. Pour des résultats jugés peu satisfaisants. Interception des conversations téléphoniques, SMS, MMS, emails... **Les interceptions judiciaires coûtent de plus en plus cher à l'État, selon la Cour des comptes.** Dans un référé adressé au premier ministre en février dernier, et publié lundi dernier, la **dépense cumulée des écoutes est estimée à 1 milliard d'euros,** par les Sages de la rue Cambon, sur les dix dernières années. Dans le détail, le coût global des interceptions judiciaires est passé de 89,78 millions d'euros en 2005, à 122,55 millions d'euros, en 2015. Soit une hausse de 37%, en dix ans! Comment expliquer une telle augmentation? Pour la Cour des comptes, elle est essentiellement due à la mise en place, très laborieuse, de la plateforme nationale des interceptions judiciaires (PNIJ), censée faciliter la centralisation, la collecte, et l'analyse des interceptions judiciaires, afin de réaliser des économies budgétaires.

Supo: Foreign intel tried to influence Finnish energy policy
Yle (Finland), Staff report, 2016 04 26
Helsinki - **Finland was the target of an attempt by foreign powers to influence energy policy decision making, according to a report by STT news agency**. STT said Monday that **Supo** revealed the espionage attempt in a new yearbook released Friday. Supo did not name the party suspected to be behind the attempt to influence Finnish energy policy, however. Nor did it indicate which specific area of energy policy was targeted. The publication offers an assessment of issues such as developments in terrorism and the actions of foreign intelligence services in Finland. Supo said that 2015 had been a very active year for intelligence activity in Finland. The organisation added that in many instances espionage had clearly been more aggressive than in previous years.

The Very Strange Extradition of a CIA Spy
The Daily Beast, Christopher Dickey, Barbie Latza Nadeau, 2016 04 26
Rome - Former **CIA employee Sabrina De Sousa**, now fighting extradition from Portugal to Italy, was skiing on a mountainside far away from the action, skiing, on February 17, 2003,

when Hassan Mustafa Osama Nasr was snatched off a street in Milan on his way to the mosque. The cleric, known as **Abu Omar**, was first flown by executive jet to Germany and then to Cairo, where he was tortured for nearly seven months, according to his own testimony and Amnesty International accounts. The kidnap was part of the infamous "extraordinary rendition" program being run at the time by the United States. The CIA was grabbing suspected terrorists from all over the world and shipping them to various countries, including Bashar Assad's Syria, Muammar Gaddafi's Libya and Hosni Mubarak's Egypt, to suffer the tortures of the damned and in some cases execution. In 2015, De Sousa, a naturalized American who was born in India and who has a Portuguese passport (her family is from the former Portuguese colony of Goa), defied warnings by the U.S. State department not to travel to Europe where she could be picked up on a European arrest warrant and sent to Italy to serve the prison term. It's not like De Sousa didn't know the risk. Indeed, **in 2009 after the Italian conviction she filed a lawsuit against the U.S. Central Intelligence Agency, former Rome station chief Castelli**, he former boss Robert Seldon Lady, the State Department and Secretary of State Hillary Rodham Clinton, alleging that they had failed to protect a loyal public servant. In the meantime, Italy reluctantly followed through with the request for extradition as stipulated on the European arrest warrant. A source close to the Italian president's office told The Daily Beast that they had never actively sought extradition, but couldn't avoid it if one of the convicted operatives was "dumb enough to travel to Europe."

Former CIA officer faces extradition to Italy over Abu Omar kidnapping
The Guardian, Stephanie Kirchgaessner, 2016 04 25
Rome— A **former undercover CIA officer is to be extradited to Italy** following her conviction over the 2003 extraordinary rendition of a terror suspect to Egypt. **Sabrina De Sousa**, a dual US and Portuguese citizen, was arrested in Portugal last October and has since lost three appeals against being handed over to Italian authorities. Her extradition is scheduled for 4 May.At the heart of the case lies the kidnapping of an Egyptian cleric, **Hassan Mustafa Osama** Nasr – known as Abu Omar – who was snatched off the streets of Milan by the CIA, allegedly with the help of Italian officials, and sent to Egypt, where he was allegedly tortured. The case was investigated by an independent prosecutor in Italy, leading to the conviction in absentia of De Sousa and 21 other CIA operatives and high-ranking officials. At the time, the case was seen as the only exhaustive investigation of the illegal counter-terrorism practice known as extraordinary rendition, and exposed US allies' role in helping to execute the strategy. Convictions of members of the **Italian military intelligence agency Sismi** were later overturned by Italy's high court on the grounds of "state secrecy".

CIA and Bosnia authorities cooperating in anti-terror fight
Hina-Croatan News Agency, 2016 04 23
Zagreb— The **Director of the Central Intelligence Agency, John Brennan**, who arrived in Sarajevo on Friday unannounced, **informed the senior officials of local law enforcement and security authorities of Washington's full support to Bosnia and Herzegovina's fight against terrorism**, according to local media outlets. "We have received support and we are reassured that we can count on cooperation with CIA and on exchange of data," the Bosnian Croat-Muslim Federation's Interior Minister Aljosa Campara said after the meeting in Sarajevo. The CIA Director arrived in Sarajevo from Riyadh and held talks with Bosnia's representatives on the struggle against terrorism.

Head of the CIA unexpectedly arrives in Bosnia
Associated Press, Staff report, 2016 04 22
Sarajevo - **Bosnia government officials say the U.S. intelligence director, John Brennan, arrived unexpectedly in Sarajevo to meet officials of the nation's anti-terrorism group**.

Officials spoke under condition of anonymity on Friday because the visit was not officially announced. The CIA director arrived from Riyadh, Saudi Arabia, where met with senior officials from six Arab nations aimed at coordinating efforts in the conflicts in Iraq, Syria and Yemen. The U.S. Embassy in Sarajevo had no comment. Bosnian officials said Brennan would meet with officials of several agencies which are coordinating anti-terrorism efforts. About 130 Bosnians are thought to be fighting in Syria for the Islamic State group. According to the government, many of them want to return home although they could face jail sentences.

Vers une meilleure coordination entre le GIGN et le RAID
Le Monde, Soren Seelow, 2016 04 21
Paris - Le **ministère de l'intérieur a décidé d'autoriser l'unité la plus proche à intervenir en cas d'attaque de masse** A défaut de parvenir à fusionner les trois unités d'élite de la police et de la gendarmerie - **RAID, BRI et GIGN** - en une seule force compétente sur l'ensemble du territoire, le ministre de l'intérieur a annoncé, mardi 19 avril, un " schéma national d'intervention " visant à coordonner leurs actions en situation de crise. Les derniers attentats ayant frappé la France n'ont pas révélé de - dysfonctionnement dramatique, mais ils ont ravivé suffisamment de tensions et de rivalités entre ces trois corps pour convaincre **Bernard Cazeneuve** de remettre à plat leurs protocoles d'intervention. La mesure la plus spectaculaire de ce plan réside dans la suspension des zones de compétences territoriales de la police et de la gendarmerie en situation d'urgence absolue.

German court: anti-terror laws partially unconstitutional
Deutsche Welle, Staff report, 2016 04 20
Berlin - The **German Federal Constitutional Court** in Karlsruhe said on Wednesday that although secret **surveillance powers given to the Federal Criminal Police (BKA) are in principle in line with the country's constitution**, the current legal framework granting these powers does not satisfy the principle of proportionality. In 2009, a law was passed granting the BKA the power to act preventatively against crimes relating to international terrorism. Previously, the BKA was responsible for law enforcement, with preventative measures assigned to state police forces. This included the ability to secretly conduct surveillance through recorded conversations or photographs, carry out wiretaps, or to remotely search computers. The appeal to the Constitutional Court argued that these preventative powers of the BKA went too far and intruded on the private lives of German citizens. The court's ruling addresses these concerns without completely rejecting the law. Specifically, the court said "with regard to the legal requirements for carrying out covert surveillance measures, the provisions introduced in 2009 are in part too unspecific and too broad."

Antiterrorisme : Cazeneuve met de l'ordre
Sud Ouest, Benoît Lasserre, 2016 04 20
Paris - Sécurité Le **ministre de l'Intérieur a annoncé hier après- midi des mesures destinées à accélérer la coopération et l'intervention des forces de l'ordre en cas d'attentat** L'épisode a contribué à bâtir la réputation de **Bernard Cazeneuve**, jusqu'alors ministre de l'Intérieur passe- muraille. En pleine traque des frères Kouachi, les assassins de " Charlie Hebdo ", en janvier 2015, et en pleine prise d'otages à l'Hyper Cacher de la porte de Vincennes, Bernard Cazeneuve, exaspéré par les cachotteries des services de police qui handicapent l'enquête, pique une de ces colères froides dont il a le secret. Il enferme tous les patrons du Quai des Orfèvres et de la gendarmerie dans une salle du sous-sol du ministère de l'Intérieur pour s'assurer de leur collaboration pleine et entière.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Shin Bet mulls renewed entry permits for Palestinians
Jerusalem Post, Ben Hartman, 2016 04 26
Jerusalem - The **Shin Bet (Israel Security Agency) is reevaluating the way it provides entry permits after large numbers of Palestinians were denied entry to Israel due to security concerns**, despite the fact that they had previously received permits to enter Israel. The Shin Bet said that the permits were revoked due to recent security concerns, including a wave of attacks carried out by Palestinians in recent months. "Due to the security situation in recent months, the Shin Bet carried out a reassessment of the criteria for giving entry permits to Palestinians from the West Bank, in order to make it more difficult for potential suspects to enter Israel," the Shin Bet said Monday, adding that "it's impossible to rule out the possibility that Palestinian who previously had received entry permits were recently denied them when they asked to enter Israel for the purpose of work."

Terrorists' Huge Bomb Workshop Discovered by Iranian Intelligence Agents
Fars News Agency, 2016 04 25
Tehran - **Iranian Intelligence Minister Seyed Mahmoud Alavi said his forces discovered and dismantled a large bomb-making workshop of the terrorists** during the parliamentary election days in February. "Two days before the election, meaning on February 24, and on the election day, meaning February 26, and even two days after the election, terrorist teams were identified and came under raid by the Iranian security forces and a number of them were killed and some others were arrested," Alavi said on Sunday. "The security forces also discovered and seized the terrorists' huge bomb-making workshop," he added. Stressing the Iranian forces' high vigilance and capability in war against terrorism, Alavi said the sound of explosions is heard in different parts of the world from the regional states to the European countries, while Iran enjoys unique security due to the supremacy and control of its **intelligence forces**.

In 'Post' interview, state attorney backs Shin Bet's interrogation tactics
The Jerusalem Post, Yonah Jeremy Bob, 2016 04 22

Jerusalem— **State Attorney Shai Nitzan** has a wide smile, is sometimes quiet, and can switch suddenly into reciting poetry or putting forth philosophical positions on judicial activism. But there is always a certain passion and an all-encompassing seriousness that animates him. He is so busy that he rarely speaks to the media on or offthe- record and is hardly even available to the spokespeople who are supposed to represent him to the public. He was appointed state attorney in November 2013 – somewhat as an outsider who has never served as a prosecutor – replacing Moshe Lador. **But one position Nitzan has always felt comfortable holding, earning enemies on both the Right and Left, is his defense of the Shin Bet's (Israel Security Service)** use of aggressive interrogation tactics. Nitzan admitted in the past that individual agents of the service may have exaggerated in interrogations on rare occasions, emphasizing however that as an institution it obeys the law with strong oversight. The High Court's 1999 torture ban and the 2013 Turkel Report on the compliance of interrogations with international law, led to the transfer of investigations of torture complaints against the Shin Bet to the Justice Ministry's responsibility.

Israel to give Jordan and Egypt intelligence help against Islamic State
Jerusalem Post, Staff Report, 2016 04 21
Jerusalem - **Israel provides Jordan and Egypt with intelligence assistance in their fight against Islamic State,** a senior Israeli military officer said on Wednesday, describing the U.S.-

backed Arab neighbors as stable despite the insurgent threat. Egypt made peace with Israel in 1979, followed by Jordan in 1994. They are the only Arab countries to have treaties with Israel, a matter unpopular with many Egyptians and Jordanians and which generally keeps Amman and Cairo quiet about the ties. Major-General Yair Golan, deputy commander of the Israeli armed forces, said in a briefing that the countries were working with Israel as they try to beat back Islamic State. "Egypt fights the Islamic State in the Sinai peninsula. Jordan is terrified by the presence of the Islamic State in Jordan's cities and towns. And we try to work with them in order to contribute something to their security," he said.

Israelis accused of spying in Romania ordered to stay in jail
Times of Israel, Raoul Wootliff, 2016 04 20
Jerusalem - **Two Israelis suspected of espionage in Romania were ordered by a local court to remain in police custody for another 30 days**, Romanian media reported Monday. David Geclowitz and Ron Weiner, employees of the Israeli private intelligence firm Black Cube, were arrested on April 3 on suspicion that they had tried to intimidate the head of the national anti-corruption agency and had hacked her emails. The Bucharest Magistrate's Court accepted the request of the Romanian serious crime investigation unit and ruled that the two remain in police custody for the next month. There was no immediate response from Black Cube following the Monday decision.

The bomber who slipped through the net
Jerusalem Post, Yaakov Lappin, 2016 04 20
Jerusalem - The **terrorist bomb that tore through a Jerusalem bus on Monday is just the type of attack that security forces, led by the Shin Bet (Israel Security Agency) domestic intelligence agency,** have been working intensively for months to try and prevent. Security forces are looking the possibility that the bomber is among one of the seriously wounded in hospital. Beyond that fact, they are maintaining a fog of secrecy around their investigation into the bombing, and key questions remain unanswered, at least in the public domain, at this stage. These include the question of whether the attacker acted alone,was part of small, amateur cell, or whether an organized terrorism cell, sent and funded by one of the established Palestinian armed factions, is behind the atrocity. Additionally, it remains unclear whether the attack occurred when it did because the bomb went off prematurely, or whether a suicide bomber detonated an explosive device.

Intelligence minister: Nuclear agreement removes sanctions' pressure
Islamic Republic News Agency, 2016 04 20
Tehran - **Intelligence Minister Seyyed Mahmoud Alavi underlined that the nuclear agreement signed between Iran and the six world powers lifted the sanctions' pressures**. 'Nuclear agreement with Group 5+1 countries removed the pressures of the sanctions imposed on the country,' Alavi said, addressing the people of Damghan on Tuesday. He reiterated that the positive effects of lifting the sanctions influences the entire country and all individuals will benefit from such effects. 'The Islamic Republic of Iran should reach a level of self-sufficiency and self-reliance in order to prevent the oppressive sanctions to influence Iran's economy,' Alavi added.
Return to Table of Contents/ Retour à la table des matières

Asia/Asie

S. Korea prepares to protect athletes' health and safety at Rio Olympics
Yonhap News Agency, 2016 04 25

Seoul— South Korea will be ready to protect its athletes' health and safety at the Rio de Janeiro Summer Olympics as various organizations have teamed up to provide a secure sporting environment. South Korea will first concentrate on defending its athletes from the Zika virus, which the World Health Organization has declared an international public health emergency. Brazil is believed to be the country hit hardest by Zika. South Korea will also put its best effort forward to protect players from crime and terror attacks. **The Brazilian intelligence agency** recently revealed that terror threats for the Rio Olympics are rising, led by the Islamic State (ISIS) and other extremist groups. The government said that its joint inspection team last week already checked and discussed with Brazilian authorities the security plans for the Summer Games. The South Korean inspection team included officials from the **Terror Information Integration Center, which is a counterterrorism unit under the National Intelligence Service.**

Call for better intelligence on kidnap groups
The Star Online, Ruben Sario and Stephanie Lee, 2016 04 21
Kota Kinabalu - **Better intelligence is key to stopping southern Philippines-based, kidnap-for-ransom groups striking in Sabah's east coast waters**, said a state assemblyman. Datuk Shamsuddin Yahya (BN-Sekong) said Malaysian security forces should work with their Philippine counterparts in **building up their intelligence capabilities against these criminal groups.** "We cannot merely rely on improved assets or increased manpower," he said when debating Yang di-Pertua Negeri Tun Juhar Mahiruddin's policy speech. He said there was a need to work with the Philippines and Indonesia regarding patrols and other security arrangements in the sea off Sabah's east coast. "We already have similar security arrangements in the Strait of Malacca with Singapore and Indo-nesia," said Shamsuddin. Noting that many Sabahans had grown impatient over the persistent kidnapping cases in the east coast, he said the full brunt of the law should be enforced.

Attack on Intelligence Unit Carried Out By Haqqani
TOLO News, Sayed Sharif Amiri, 2016 04 21
Kabul - **Tuesday's deadly attack on the intelligence unit tasked with the protection of VIPs was reportedly carried out by the Haqqani Network**, said officials Wednesday. Kabul NDS Chief Mohammad Omar Azizi said at a press conference in Kabul that the attack was organized outside the country. In Tuesday's attack 64 people were killed and 347 were wounded. The question being asked however is how did a truck, loaded with explosives, reach the intelligence unit, which is part of the greater ring of steel within Kabul city? In a bid to test the level of security within the city, Sharif Amiri, TOLOnews' correspondent, on Wednesday traveled through the heart of the capital in the same type of truck used in Tuesday's bombing. Amiri traveled a distance of seven kilometers, from Pul-e-Charkhi in east Kabul and went through five check posts.

S. Korea considers biometric sensors for gov't offices
Yonhap News Agency, 2016 04 21
Seoul-- The **South Korean government is reviewing an option to beef up security at public office buildings by adopting a biometrics recognition system**, the interior minister said Thursday.The policymaker's announcement comes as Seoul took fire for lax security after a man broke into a government building earlier this month. The 26-year-old, identified only by his surname Song, was formally arrested over unauthorized entry into the government complex in central Seoul and manipulating the result of the civil service examination he took. Song illegally entered the building a total of five times after he stole an identification card of a public official working in the building in February, according to the **National Police Agency (NPA).**

Taliban Strikes a Deadly Attack in Kabul on Elite Agency
Asharq Al-Awsat, Staff Report, 2016 04 20
Kabul - More than 320 people injured and more than 24 killed in one of the most devastating attacks in Kabul since years as the aftermath of **an attack by Taliban militants on a government security agency with a suicide bomb and gunfire Tuesday**, Afghan officials said. Noting that this attack has ended all efforts and disappointed the several past weeks of peace and relative calm in the capital of Afghanistan, **the main target was an elite Afghan intelligence unit tasked with protecting senior government politicians** - a direct strike against the Western-aided government only a week after the Taliban announced its spring offensive. This attack is remarked as one of the biggest attacks to rock the Afghan capital in years. It took place by the time a suicide bomber blew himself up at the gates of the agency, touching off a three-hour gun battle less than a mile away from the presidential palace and the Ministry of Defense in a densely-populated part of the city.

Japan, Canada agree to cooperate on counterterrorism measures (Canada)
Kyodo News, 2016 04 20
Tokyo - **Japan and Canada agreed Tuesday to strengthen cooperation in counterterrorism at a meeting of their vice foreign and defense ministers in Tokyo**, the Japanese Foreign Ministry said. Japan, Canada and the other Group of Seven countries of Britain, France, Germany, Italy and the United States -- at a summit in May in central Japan -- plan to adopt an action plan on countering terrorism in the wake of the attacks by Islamic State militants in Brussels and Paris. They also reaffirmed that nations must act in accordance with international law amid concerns raised by China's construction and potential use for military purposes of facilities in contested waters of the South China Sea, the ministry said. That issue is also expected to be discussed at the G-7 summit in May. Japan was represented by Deputy Foreign Minister Shinsuke Sugiyama and Vice Minister of Defense for International Affairs Toru Mimura in the so-called 2-plus-2 security talks, the third of their kind. Canada was represented by Daniel Jean, deputy minister of foreign affairs, and **John Forster**, deputy minister of national defense.

Arrested RAW agents reveal communication codes
Pakistan Observer, 2016 04 20
Islamabad— Two **Research and Analysis Wing's (RAW) agents copped by Counter-Terrorism Department have made key revelations during interrogation including coded sentences that they used to communicate.** The two agents belong to a group that comprises of ten members. The two arrested agents named Saddam Hussain and Bachal Solangi revealed that nine different Indian telephone numbers were used to contact them. Indian officer named 'Karan Singh' provided the agents with mobile phones that were equipped with advanced softwares. Nabbed agents revealed that they used different coded sentences to communicate with one another.

S. Korean pastor convicted of breaching security law
Yonhap News Agency, Staff reporter, 2016 04 20
Seoul - The **nation's top court has sentenced a 54-year-old pastor to six months in prison for praising North Korea in violation of South Korea's national security law**, court records showed Wednesday. Upholding a lower court's decision, the **Supreme Court convicted Park Kwang-hyuk of supporting the authoritarian regime on the website of a pro-North Korean online community from 2010**. The top court agreed with the lower court's judgment that Park's posts on the website pose a clear threat to national security as they can be distributed to many people. Still, the jail term was suspended for two years. The Ulsan District Court said there is a lack of evidence to say Park tried to preach his thoughts at the church. It also took into

consideration that he had no other criminal records. South Koreans are prohibited from supporting or praising the North in any way under the National Security Law. They are also banned from joining a pro-Pyongyang organization or having unauthorized contact with North Korea.

Return to Table of Contents/ Retour à la table des matières

Africa/Afrique

Failure to Share Data Hampers War on Boko Haram in Africa
The New York Times, Eric P. Schmitt & Dionne Searcey, 2016 04 24
Dakar, Senegal - The **military campaign by Nigeria and neighboring nations to combat the West African militant group Boko Haram has been hampered by a failure among those countries to share crucial intelligence** — sometimes even within their own security services, American and other Western officials say.Western partners have balked as well. **The Pentagon and American intelligence services have struggled at times to provide information quickly about Boko Haram militants to the African countries — Cameroon, Chad, Niger and Nigeria** — without violating restrictions on what can be shared from spy satellite imagery or electronic eavesdropping within rules for not disclosing sources and methods.Until recently, Western officials and analysts said, Britain and the United States provided only sanitized intelligence reports to the Nigerian military. The countries feared that more detailed information might be misused by an army that human rights groups say has committed abuses against civilians as it battled Boko Haram, which has pledged loyalty to the Islamic State.And a new intelligence "fusion center," created in Chad as part of a multinational task force, has only recently overcome budget and staffing shortfalls, as well as lingering mistrust among the participating countries, to help coordinate operations."

Délivrance du passeport biométrique (Canada)
L'Essor (Mali), 2016 04 22
Bamako--**Face aux impératifs de sécurité liés au terrorisme, nombre de Maliens ont adopté - à juste titre - de nouveaux comportements**. Le nouveau contexte a également incité les hautes autorités du pays à prendre une batterie d'initiatives et de mesures parmi lesquelles **l'introduction de la carte NINA** et, aussi et surtout, le lancement le 4 avril dernier du passeport biométrique. Si l'opération se déroule bien pour les Maliens de l'intérieur, nos compatriotes de la diaspora éprouvent des difficultés à se procurer le document. En effet à la date du 20 avril 2016, 8596 demandes de passeports étaient en souffrance dans nos représentations diplomatiques. Ce chiffre s'élevait à 7000, il y a une dizaine de jours. Selon le ministère des Maliens de l'extérieur, la principale raison de ce retard réside dans l'absence de moyens d'enregistrement dans la plupart de nos ambassades et consulats. Seuls neuf de nos représentations à l'étranger en disposent : France, Côte d'Ivoire, Gabon, Congo Brazzaville, **Canada**, New York, Washington, Djeddah et Riyad.

Sudan appoints new ambassador to European Union
Sudan Tribune, 2016 04 21
Khartoum— The foreign ministry in Khartoum this week announced that **Motrif Siddiq has been appointed as Ambassador Extraordinary and Plenipotentiary of Sudan to the European Union** (EU). His appointment comes as Sudan and EU's relations have been witnessing remarkable improvement recently. Siddiq was a member of the Sudanese intelligence community before to join the diplomatic corps. He **served as the deputy director**

of the External Intelligence Agency till 1995 when Sudan was accused of attempting to kill the Egyptian president Hussani Mubarak. He also served as deputy minister of the humanitarian and the foreign affairs ministries when he left the external intelligence agency.

Return to Table of Contents/ Retour à la table des matières

Americas/Amériques

Experts accuse Mexico of 'torture' in investigation into missing 43
Buenos Aires Herald, 2016 04 25
Mexico City-- At an emotional press conference that drew tears from families of the victims and the investigators themselves, a panel of international experts yesterday accused Mexico's government of "torture" and of undermining their probe into the fate of 43 trainee teachers massacred in 2014 — the most notorious human rights case in Mexico in recent years. The independent panel, commissioned by the Inter-American Commission on Human Rights (IACHR), said the government's stonewalling had allowed "impunity" and repeatedly stopped them from finding out the truth. The panel said they had discovered "strong evidence" that suspects had been tortured. While the experts' probe showed that the municipal police were the main culprits of the detention and disappearance of the students, they said the federal police should also be investigated. They also said both the Army and the **intelligence agency known as CISEN had failed to hand over reports that could help the case.**

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

27-04-2016 to/au 03-05-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Spy agency cagey on privacy breaches
Toronto Star, Alex Boutilier, 2016 05 03
Ottawa - **The Communications Security Establishment is refusing to release the number of privacy breaches the agency has logged since 2007.** Documents obtained by the Star state the **intelligence and cyber defence agency has maintained a central database for certain privacy violations since 2007**. These breaches are categorized as minor "procedural errors" or more serious "privacy incidents," and reviewed by the CSE Commissioner's office every year. "In these files, CSE records any incidents it identifies that put at risk the privacy of a Canadian in a manner that runs counter to (or is not provided in) its operational policies," says a September 2014 letter from former CSE **chief John Forster** to a senior Treasury Board official. The Star requested just the number of breaches - no details about what actually transpired or the Canadian personal information involved - but was told the agency could not comply due to "operational security concerns." "Releasing the number of (breaches) would provide insight into CSE's capacity to conduct operations, the extent of its capabilities, the degree to which partner organizations benefit from sharing and the reach of the programs," wrote spokesperson **Ryan Foreman** in an email last week.

What Happens When Canadian Cops Find a Software Security Flaw?
Motherboard, Matthew Braga, 2016 05 03
When l**aw enforcement and intelligence agencies in Canada discover flaws in computer software--say, a bug that could help hackers steal messages from a smartphone, or spy on unsuspecting victims via internet**- connected webcams--do they disclose those holes to the software's creator so they can be plugged? Or do they keep such flaws secret for their own use in future investigations, with the hope that no one else will find and use them maliciously first? These types of weak spots, if left unpatched, can pose a very real security risk to users. But unlike counterparts in the US, the Canadian government has never gone on the record about how it handles the disclosure of newly discovered software bugs. Often referred to as zero day vulnerabilities, such flaws are valuable to spies and police because their existence is not widely known, not even to the companies themselves. Thus, they can be used to gain access to computer networks, smartphones, or other electronic devices again and again, until the vulnerability is discovered, or disclosed and patched. . "**We generally do not comment on specific investigative methods, tools and techniques outside of court**," wrote **Sgt. Julie Gagnon. Ryan Foreman, spokesperson for the Canadian government's cyberspy agency Communications Security Establishment (CSE),** wrote in an email that CSE shares "cyber threat information" with government stakeholders that "may originate from CSE's own analysis," but did not not specifically address software exploits, nor whether a policy comparable to the VEP exists.

No toilets, no light - DND workers to get headlamps
Ottawa Citizen, David Pugliese, 2016 05 03
Ottawa - **Federal public servants and military staff will be issued headlamps and bottled water in preparation for working in the dark at National Defence headquarters** in **Ottawa for three days this month**. Fire alarms and the sprinkler system will be turned off, but the workers, who will be on the 11th floor, have been told the likelihood of a blaze breaking out in the headquarters is remote, according to documents obtained by the Citizen. They can use their

BlackBerries to contact emergency crews. The ventilation system will also be shut down and the elevators won't be working. **The arrangements will affect 15 military and civilian staffworking their regular shifts at a communications centre at National Defence headquarters over the May long weekend**. The building will be without electricity as part of regular maintenance. Generators will be used to temporarily power the communications system, which is used to keep in touch with overseas military missions.

Ex-CSIS source guilty of fraud
Ottawa Citizen, James Bagnall, 2016 05 03
Ottawa - **Ontario Superior Court Judge Timothy Ray could not have been clearer Monday in delivering his verdict to former construction boss and CSIS informant Roland Eid**. "ICI (Construction) was a sham from early 2007 until its demise," Ray said in delivering a summary of his 89-page decision. ICI was the construction company launched by Eid in 2006. It went bankrupt early in 2008 after Eid transferred $1.7 million from its coffers to a personal account in Beirut. The money was never returned. The judge found Eid guilty of 10 counts of breaching the Criminal Code and the Bankruptcy and Insolvency Act. He found Eid had defrauded ICI creditors, causing them to suffer collective losses of $3.8 million. The judge also found that Eid had "perpetrated a fraud by taking $1.7 million which were trust funds belonging to the subcontractors and suppliers out of Canada and beyond their reach." Eid's defence contended the money was to have been used to finance a new construction project in Lebanon and Syria. He claimed the Syrian government would match the money deposited in his Beirut account - money that Eid said he would return to ICI in Ottawa.. **The judge made no note of what impact, if any, Eid's history as an informant for the Canadian Security and Intelligence Service had on his thinking.** Neither defence counsel Richard Addelman nor Crown lawyer Moray Welch brought it to Ray's attention. Welch said he had "no knowledge" that Eid was engaged in CSIS activities. Indeed, Eid did not appear as a witness during the trial, though he did launch a civil suit last year against CSIS and the RCMP, in which he alleged these organizations triggered the bankruptcy of ICI as retribution for Eid's refusal to take on a "dangerous" CSIS assignment in Lebanon.

Canada's spies in spat over privacy breach reporting
Toronto Star, Alex Boutilier, 2016 05 01
Ottawa - **Canada's electronic spies are concerned reporting too many details about serious privacy breaches could reveal too much about the agency's highly secretive surveillance and cyber-defence activities, the Star has learned**. The **Communications Security Establishment has been in a yearlong spat with privacy commissioner Daniel Therrien's office over reporting "material" privacy breaches**. The spy agency's reluctance comes despite government-wide regulations requiring all serious privacy breaches - - those that potentially could cause serious harm to an individual, or involving a large number of Canadians - - to be disclosed to the independent watchdog. "As with all (government) departments and agencies, CSE is required to report material privacy breaches to the Office of the Privacy Commissioner," CSE spokesman **Ryan Foreman** wrote in a statement. "However, we do continue to discuss the most effective manner to report material privacy breaches when they occur in the operational space, in a matter that safeguards the sensitive nature of information related to CSE's mandated activities."

Vice Media appeals court order to give records of terrorist interviews to RCMP
Canadian Press, Colin Perkel, 2016 04 30
Toronto - **A Canadian news outlet is asking an appeal court to throw out a ruling forcing one of its journalists to give the RCMP records of interviews he did with an accused terrorist.** Documents filed this week show Vice Media also wants the Ontario Court of Appeal to

allow publication of the information police relied on to get their order for the records. "This appeal raises issues concerning one of the hallmarks of a democratic society -- a free and independent press," the appeal application states. "Journalists' ability to pursue the truth without fear of reprisal or interference is essential to every facet of Canadian life." Vice argues that the RCMP demand would have a "detrimental chilling effect" on journalism in Canada if it is allowed to stand. Last month, Superior Court **Justice Ian MacDonnell ordered Vice and reporter Ben Makuch to turn over background materials related to stories about Farah Shirdon**. Three Vice stories in 2014 were largely based on conversations Makuch had with Shirdon via an online instant messaging app called Kik Messenger. RCMP want access to Makuch's screen captures of those chats. Among other things, Makuch cited Shirdon, of Calgary, as saying from Iraq: "Canadians at home shall face the brunt of the retaliation. If you are in this crusader alliance against Islam and Muslims, you shall see your streets filled with blood."

B.C. woman seeks millions for being wrongly branded as terrorist
Canadian Press, Geordon Omand, 2016 04 29
Vancouver - **A British Columbia woman's life was "destroyed" after the federal government wrongfully branded her a terrorist** and ruined her multimillion-dollar business in its zeal to appear tough on crime, alleges a lawsuit filed in Washington state court. Perienne de Jaray is suing the Canadian government for at least $21 million for what the court documents say was "extreme and outrageous conduct" that saw her lose her home, her health and her business after enduring years of baseless and aggressive investigations on both sides of the border. "The only thing worse in this day and age than being labelled a terrorist is being wrongly labelled a terrorist," reads the complaint for damages, filed April 19 in Seattle. "The label breeds fear and hatred across the world." **Also named in the civil action filed in U.S. District Court in Seattle are the Canadian Border Services Agency, the Department of Foreign Affairs, Global Affairs Canada and several civil servants.**

Trudeau fills senior job at Indigenous and Northern Affairs
Ottawa Citizen, Kathryn May, 2016 04 28
Ottawa - Prime Minister Justin Trudeau promoted a Finance Canada executive to fill a key top job at Indigneous and Northern Affairs, one of the government's toughest portfolios. Diane Lafleur, assistant deputy minister of Finance's federal and provincial relations and social policy branch moves into the associate deputy minister post effective May 9. **Trudeau still has to name a national security adviser to replace Richard Fadden**. David McGovern, the deputy national security adviser, is acting national security advisor and is among a list of contenders to replace Fadden. There has been much speculation over who has the leadership and security experience to fill the job. Few can match Fadden, who held deputy level jobs in five departments and agencies including many of the key security and intelligence portfolios, as well as an early version of the security advisor job under the Jean Chrétien government. Possible dark-horse candidates **include Greta Bossenmaier, the current chief at Communications Security Establishment.**; some argue she needs more experience. **Another is John Ossowski, deputy commissioner at Canada Revenue Agency who worked at Public Safety, Treasury Board's international affairs, security and justice sector and CSE.**

ISIL uses canadians: ex-CSIS official; Propaganda wing
National Post, Stewart Bell, 2016 04 28
Ottawa - **The propaganda wing of ISIL**, known for its gory videos and exploitation of social media, **has recruited several Canadians**, a former senior counter-terrorism official told a security conference Wednesday. **Andy Ellis, who recently retired from the Canadian Security Intelligence Service, where he was assistant director of operations, said not all the roughly 100 Canadians who have converged in the region are active in combat**

operations. "Many of the Canadians, for example, found their way into the propaganda wing of Daesh," the 30-year-veteran of CSIS said, using another name from the Islamic State of Iraq and the Levant, in a speech at the Royal Canadian Military Institute in Toronto.

Agents unilingues anglophones au parlement La GRC a enfreint la loi fédérale
La Presse canadienne, Journaliste maison, 2016 04 28
Ottawa **- La Gendarmerie royale du Canada (GRC) a enfreint la Loi sur les langues officielles, puisque des agents n'ont pas été en mesure d'offrir des services en français au public sur la colline du Parlement.** Le commissaire aux langues officielles, Graham Fraser, s'est penché sur le cas de plaignants - dont l'ancien député Yvon Godin - qui disaient s'être adressés en français à plusieurs reprises à des policiers de la GRC patrouillant sur la colline. Les agents étaient incapables de leur fournir des services en français. Dans son rapport préliminaire d'enquête, le commissaire donne raison aux plaignants. Il note que des agents « peuvent avoir à dicter des consignes de sécurité, telles que des ordres d'évacuation ». « Dans de telles situations, il est essentiel que les membres des deux communautés de langue officielle soient en mesure de bien comprendre les consignes dictées », signale le commissaire.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

Pentagon on alert after names of American generals appear on ISIS 'hit-list'
Jerusalem Post, Yasser Okbi, Maariv Hashavua, 2016 05 03
Jerusalem - **The Pentagon is on alert following the publication of the names of several high ranking American military officials on the latest Islamic State "hit list."** Hackers affiliated with **the Islamic State Hacking Division posted details of more than 70 American military personnel including their full names, addresses, phone numbers, emails and photographs on the Internet**, claiming that the officials named were directly involved in attacks on Syria and Iraq. Topping the list of names is Lieutenant Sean McFarland, the commander of the coalition forces in Syria. "As you continue your aggression towards the Islamic State and your bombing campaign against Muslims, know that we are in your e-mails and computer systems, watching and recording your every move," read the warning to the US military officials.

CIA to boost benefits for workers' survivors
Washington Post, Catharine Ho, 2016 05 03
Washington - **The CIA will provide $400,000 in new survivor benefits to family members of federal employees and contractors killed by acts of terrorism while working overseas.** The change, confirmed by the agency, comes three years after the family of **Glen Doherty - one of two CIA contractors killed during the 2012 attacks in Benghazi, Libya - began lobbying the federal government for survivor benefits.** Before the change, surviving family members received benefits from the employee or contractor's life insurance and some additional benefits from the CIA, depending on each individual's situation. Now, the CIA will provide a uniform $400,000 to families. On top of that, the agency will provide one year's salary and financial assistance that can be put toward educational expenses for surviving children. The benefits will go to family members of a very specific subset of federal employees and contractors - those killed overseas as a result of acts of terrorism dating to April 18, 1983 - the date of the bombing of the U.S. Embassy in Beirut.

Feds have found 'unbelievable' amounts of child porn on National Security computers. Is this the answer?
Nextgov.com (US), Staff report, 2016 05 03
Washington - **A top National Security Agency official wants to keep tabs on national security personnel off-the-clock, in part by tracking their online habits at home**. The aim is to spot behavior that might not be in America's best interests. Historically, some illicit activity, like downloading child pornography, has occurred on government computers and been prosecuted. But today, the digital lives of employees cleared to access classified information extend beyond the office. About 80 percent of the National Security Agency workforce has retired since Sept. 11, 2001, says **Kemp Ensor,** NSA director of security. **When the millennial and Gen Y staff that now populate the spy agency get home, they go online. "That is where were we need to be, that's where we need to mine," Ensor said.**

CIA Chief on ISIS: Not Just an Organization, 'It's a Phenomenon'
Meet The Press (NBC), Sally Bronston, 2016 05 01
Washington - On the fifth anniversary of the raid that killed Osama bin Laden, **Director of the Central Intelligence Agency John Brennan** spoke exclusively with NBC's Chuck Todd on "Meet the Press". In a wide- ranging interview, **Brennan soberly discussed the threat of ISIS, dismissed allegations of Saudi Arabia's role in 9/11, and reacted to Donald Trump and the current political climate in the country. On the threat of ISIS, Brennan assured viewers,** "We will destroy [ISIS], I have no doubt in my mind. And we have to remove the leadership that directs that organization to carry out these horrific attacks." ISIS' number one is Abu Bakr al-Baghdadi, and if he were to be killed, Brennan believes it would have an affect on the terrorist group. "If we got Baghdadi, I think it would have a great impact on the organization, and it will be felt by them," he said. Brennan warned fighting ISIS has its unique challenges, calling them not just an "organization," but "a phenomenon." "We know that ISIS is trying to carry out attacks in Europe and in other parts of the globe. Also, we are working very, very closely with our European partners," he said. ABrennan was careful not to oversell America's ability to affect change in the Middle East. "The United States has only limited influence to shape events in the Middle East. And a lot of individuals think that the United States can wave a magic wand, and we can't," the CIA Director said.

CIA director: '28 pages' contain inaccurate information
The Hill, Jessie Hellmann, 2016 05 01
Washington **- CIA Director John Brennan said Sunday that releasing the 28 classified pages from the 9/11 Commission report would be a mistake because they contain inaccurate, un-vetted information that could be used to tie Saudi Arabia to the Sept. 11, 2001, terror attacks**. "This chapter was kept out because of concerns about sensitive methods, investigative actions, and the investigation of 9/11 was still underway in 2002," Brennan said on NBC's "Meet the Press." He said information in the 28 pages hasn't been vetted or corroborated, adding that releasing the information would give ammunition to those who want to tie the terror attacks to Saudi Arabia. "I think there's a combination of things that are accurate and inaccurate [in the report]," Brennan said. "I think the 9/11 Commission took that joint inquiry and those 28 pages or so and followed through on the investigation and then came out with a very clear judgment that there was no evidence that ... Saudi government as an institution or Saudi officials or individuals had provided financial support to al Qaeda."

Former NSA head: US safer from terrorism than Europe
The Hill, Harper Neidig, 2016 05 01
Washington **- Former National Security Agency (NSA) Director Gen. Michael Hayden said**

on Sunday he believes the U.S. is safer from terrorism than European countries. During a radio interview with John Catsimatidis, Hayden was asked if European nations are becoming larger targets than the U.S. "No question about it," Hayden responded. "Now, John, that doesn't mean there's no threat here. There are a variety of things that actually make us more safe." The first, Hayden said, is simply that Europe is closer to where groups like the Islamic State in Iraq and Syria operate. "Second is we're actually pretty good at this, John," he continued. "Our security services have a pretty good record compared to the European services, or at least to many of the European services."

How the CIA failed a spy who went missing in Iran
Washington Post, Valerie Plame, 2016 05 01
Book Review: In a world of seemingly random massacres in Paris, Brussels and San Bernardino, Calif.; Islamic State beheadings; and an erratic potentate in a nuclear-armed North Korea, we like to think that the **CIA, the FBI and the other 14 agencies charged with gathering intelligence are doing their damnedest to keep us safe**. And, for the most part, they are. But embedded within the vast U.S. intelligence complex is a bloated bureaucracy that creates turf battles and inefficiencies that can lead to dire and even deadly consequences. The tale of Robert Levinson - a retired Drug Enforcement Administration and FBI agent turned CIA contractor who disappeared in 2007 from a resort island in the Persian Gulf - underscores the dangers of the multi-headed bureaucratic monster called the CIA. In January of this year, after the United States and Iran reached a deal to curb the Islamic republic's nuclear program, the two countries swapped prisoners. Levinson was not part of the agreement. Proof that he was alive has come only twice - in a 2010 video, during which he pleaded for help from his government, and in 2011 photos of Levinson wearing an orange prison jumpsuit and looking ill and disheveled. **Barry Meier's new book, "Missing Man," catalogues how Iranian and U.S. officials knew far more about Levinson's disappearance than previously acknowledged**. Through the contacts and machinations of Doug Coe, head of a powerful and secretive Christian organization called the Fellowship, the U.S. government learned from the Iranian ambassador to France in late 2011 that Iran was holding Levinson.

How to Beat ISIS: Blow Up the Money
NBC News, Robert Windem & William Arkin, 2016 05 01
Washington - **The U.S. has quietly turned to a new strategy in fighting ISIS -- follow the money, then blow it up,** U.S. officials tell NBC News. At least four times in the past four months, U.S. military jets have targeted [major] ISIS financial centers, destroying them in strikes that have turned millions of U.S. dollars into confetti. The war is not just about tracing the movement of money but the movement of individuals linked to the cash. It's part of what CIA Director John Brennan calls a broader cyber effort against ISIS. "They are murderers and we need to be able to change this narrative -- including in the cyber environment, the digital domain, in social media," said Brennan. "It is a question of what type of activities might take place in that cyber environment that we would be able to carry out destructive actions against." Financial transactions, one senior intelligence official tells NBC News, have become one of the most lucrative forms of intelligence on personal relations, foreign fighter movements, and sources of supply. The intelligence community tracks ISIS financial transactions through data collection programs with such secret code names as **"Kaching" (CIA), "TRACKFIN" (NSA) and FINO (the National Clandestine Service). Newly created electronic portals for the processing of what is now called financial intelligence (or FININT) -- Swordfish, QLIX/HYDRA and Sentry,** among others -- fuse together conventional banking, transaction and intercepted data.

U.S. Steel Accuses China of Hacking
Wall Street Journal, John W. Miller, 2016 04 29
Pittsburgh - **U.S. Steel Corp. is alleging that Chinese government hackers stole proprietary methods for making lightweight steel on behalf of Chinese steel producers seeking to supply a bigger share of the U.S. auto- making market**. Pittsburgh-based U.S. Steel, in a complaint filed on Tuesday with the International Trade Commission, said a computer belonging to a Pittsburgh researcher was hacked in 2011, and that plans for developing new steel technology were stolen. The ITC, an independent agency that reviews and enforces U.S. trade policy, has within 30 calendar days to decide whether to launch an investigation. The agency typically investigates complaints. U.S. Steel says it expects any ITC probe resulting from its complaint "to reveal that the Chinese government disseminated U.S. Steel's trade secrets to" Chinese steelmakers, "enabling them to manufacture [lightweight steels] that [compete] with U.S. Steel's products." In a statement Wednesday, China's Commerce Ministry urged U.S. authorities to reject U.S. Steel's trade complaint, and said that allegations of intellectual property infringement "are completelywithout factual basis." The Commerce Ministry on Thursday didn't respond to a request for comment on the hacking allegations by U.S. Steel.

U.S. high court approves rule change to expand FBI hacking power
Reuters, Staff report, 2016 04 29
Washington - The Supreme Court on Thursday approved a rule change that would let U.S. judges issue **search warrants for access to computers located in any jurisdiction despite opposition from civil liberties groups who say it will greatly expand the FBI's hacking authority**. U.S. Chief Justice John Roberts transmitted the rules to Congress, which will have until Dec. 1 to reject or modify the changes to the federal rules of criminal procedure. If Congress does not act, the rules would take effect automatically. Magistrate judges normally can order searches only within the jurisdiction of their court, which is typically limited to a few counties. The U.S. Justice Department, which has pushed for the rule change since 2013, has described it as a minor modification needed to modernize the criminal code for the digital age, and has said it would not permit searches or seizures that are not already legal. Google, owned by Alphabet Inc., and civil liberties groups such as the American Civil Liberties Union and Access Now contend the change would vastly expand the Federal Bureau of Investigation's ability to conduct mass hacks on computer networks.

FBI paid under $1 million to unlock San Bernardino iPhone: sources
Reuters, Mark Hosenball, 2016 04 29
Washington - **The FBI paid under $1 million for the technique used to unlock the iPhone used by one of the San Bernardino shooters - a figure smaller than the $1.3 million the agency's chief initially indicated the hack cost, several U.S. government sources said on Thursday**. The Federal Bureau of Investigation will be able to use the technique to unlock other iPhone 5C models running iOS 9 - the specifications of the shooter's phone - without additional payment to the contractor who provided it, these people added. FBI Director James Comey last week said the agency paid more to get into the iPhone than he will make in the remaining seven years and four months he has in his job, suggesting the hack cost over $1.3 billion, based on his annual salary. The identity of the contractor is so closely-held inside the FBI that not even Comey knows who it is, one of the sources said.

Fears of risk to key phone database
Washington Post, Ellen Nakashima, 2016 04 29
Washington - **Federal officials fear that national security may have been jeopardized when the company building a sensitive phone-number database violated a federal requirement that only U.S. citizens work on the project**. The database is significant because it tracks

nearly every phone number in North America, making it a key tool for law enforcement agencies seeking to monitor criminal or espionage targets. Now Telcordia, a Swedish- owned firm, is being compelled to rewrite the database computer code - a massive undertaking - **to assuage concerns from officials at the FBI and Federal Communications Commission that foreign citizens had access to the project**. These officials fear that if other countries gain access to the code, they could reap a counterintelligence bonanza, learning the targets of U.S. law enforcement and espionage investigations. The security rewrite began in March after the agencies learned that a **Chinese citizen** with a U.S. work permit had helped write the system code, said individuals familiar with the matter who spoke on the condition of anonymity to discuss a sensitive matter. made public this week that he was fired in retaliation for blowing the whistle on a foreign worker.

Letter details plan for secretive anti-radicalization committees
The Intercept, Cora Currier, Murtaza Hussain, 2016 04 28
Washington - **Of the plans put forward by the federal government to identify and stop budding terrorists, among the least understood are the FBI's "Shared Responsibility Committees."** The idea of the committees is to enlist counselors, social workers, religious figures, and other community members to intervene with people the **FBI thinks are in danger of radicalizing -- the sort of alternative to prosecution and jail time many experts have been clamoring for**. But civil liberties groups worry the committees could become just a ruse to expand the FBI's network of informants, and the government has refused to provide details about the program. The Intercept has obtained a letter addressed to potential committee members from the FBI, outlining how the process would work. While the letter claims that committees will not be used "as a means to gather intelligence," it also makes clear that information from the committees may be shared widely by the FBI, including with spy agencies and foreign governments, and that committee members can be subpoenaed for documents or called to testify in cases against the people they are trying to help. At the same time, committee members are forbidden even from seeking advice from outside experts without permission from the FBI.

Three TSA managers say 'bullies' punish whistleblowers
Washington Post, Ashley Halsey III, 2016 04 28
Washington - **The Transportation Security Administration on Wednesday was caught in a crossfire by three of its executives who said the agency's managers punish employees when they point out security lapses at the nation's airports**. "These leaders are some of the biggest bullies in government," Jay Brainard, a TSA security director in Kansas, told the House Committee on Oversight and Government Reform. "While the new administrator of TSA has made security a much-needed priority once again, make no mistake about it, we remain an agency in crisis."

T.S.A. Official Discloses Advice to Target Somalis
New York Times, Ron Nixon, 2016 04 28
Minneapolis - **A Transportation Security Administration manager here said he was instructed by his supervisor to provide the names of Somali-American leaders visiting the agency's local office so they could be screened against national security databases for terrorist ties,** a disclosure that quickly drew **accusations of racial profiling**. In a midyear performance evaluation, **David McMahon**, the supervisor of Andrew Rhoades, an assistant federal security director, wrote that he had advised Mr. Rhoades to check potential visitors to the agency's offices with the field intelligence officer to determine "if we want them in our office space or meet elsewhere." The Office for Civil Rights and Civil Liberties said Tuesday that it had opened an investigation into the allegations.

F.B.I. Opts Not to Share iPhone-Unlocking Method
New York Times, Eric Lichtblau, Katie Benner, 2016 04 28
Washington - **The F.B.I. closed the door Wednesday to the possibility of giving Apple the technical solution that the government bought to unlock the iPhone** used by one of the attackers in the mass shooting in San Bernardino, Calif. The decision leaves Apple in the dark about the technical details of how the F.B.I. -- with help from an unknown outside group that was apparently paid at least $1.3 million -- managed to bypass the company's vaunted encryption. Apple declined to comment on Wednesday. Soon after the government said that a third party had successfully gotten data from the phone, after giving the F.B.I. a demonstration of its method in February, many security professionals were hopeful that the method would be made public. "It's the position of Obama administration that security flaws should be disclosed to the parties that can fix them," said Denelle Dixon-Thayer, chief legal and business officer at Mozilla.

U.S. Kills ISIS Operatives Linked to Europe Attacks
The Daily Beast, Kimberly Dozier, 2016 04 28
Washington **- As the self-proclaimed Islamic State trumpets its global terrorist campaign, U.S. special operations forces have quietly killed more than three dozen key ISIS operatives blamed for plotting deadly attacks in Europe and beyond**. Defense officials tell The Daily Beast that U.S. special operators have killed 40 "external operations leaders, planners, and facilitators" blamed for instigating, plotting, or funding ISIS's attacks from Brussels and Paris to Egypt and Africa. That's less than half the overall number of ISIS targets that special operators have taken off the battlefield, one official explained, including top leaders like purported ISIS second-in-command Haji Imam, killed in March. **The Central Intelligence Agency, the National Security Agency, and other elements of the U.S. intelligence community** are also driving the effort, finding and feeding the intelligence to the coalition strike force.

The CIA Illegally Let the Wrong People Do Intelligence Work, Declassified Report Finds
Vice News, Jason Leopold, 2016 04 27
New York - **The CIA violated federal laws and its own internal regulations by hiring independent contractors for a wide variety of intelligence and national security-related work** that was supposed to be performed by government employees, according to a CIA Office of Inspector General (OIG) audit report obtained by VICE News in response to a Freedom of Information Act lawsuit. The report said the CIA "relies heavily on independent contractors to accomplish important facets of its mission," particularly at the National Clandestine Service, the covert arm of the agency responsible for clandestine operations around the world. The report, dated June 22, 2012 but only declassified last month, raised numerous red flags about the CIA's use of independent contractors throughout all divisions within the agency, and for work performed work in areas that included covert operations and protective security services overseas. By law, that work must be done by CIA employees.

After Missteps, U.S. Tightens Rules for Espionage Cases
New York Times, Matt Apuzzo, 2016 04 27
Washington - The **Justice Department has issued new rules that give prosecutors in Washington greater oversight and control over national security cases** after the collapse of several high-profile prosecutions led to allegations that **Chinese-Americans were being singled out as spies.** The new rules are intended to prevent such missteps, but without undermining a counterespionage mission that is a top priority for the Obama administration. While (the) cases raised the specter of Chinese espionage, none explicitly charged the

scientists as spies. The cases involved routine criminal laws such as wire fraud, so national security prosecutors in Washington did not oversee the cases. In a letter last month to federal prosecutors nationwide, Deputy Attorney General Sally Q. Yates said that would change. All cases affecting national security, even tangentially, now require coordination and oversight in Washington. That had always been the intention of the rule, but Ms. Yates made it explicit. "The term 'national security issue' is meant to be a broad one," she wrote.

After the Snowden NSA leaks, fewer people are searching for info on terror groups online (Canada)
Reuters, Joseph Menn, 2016 04 27
San Francisco - **Internet traffic to Wikipedia pages summarizing knowledge about terror groups and their tools plunged nearly 30 percent after revelations of widespread Web monitoring by the U.S. National Security Agency,** suggesting that concerns about government snooping are hurting the ordinary pursuit of information. A forthcoming paper in the Berkeley Technology Law Journal analyzes the fall in traffic, arguing that it provides the most direct evidence to date of a so-called "chilling effect," or negative impact on legal conduct, from the intelligence practices disclosed by fugitive **former NSA contractor Edward Snowden**. Author Jonathon Penney, a fellow at the University of Toronto's interdisciplinary Citizen Lab, examined monthly views of Wikipedia articles on 48 topics identified by the U.S. Department of Homeland Security as subjects that they track on social media, including Al Qaeda, dirty bombs and jihad.

FBI chief sees better cyber cooperation from China
Agence France-Presse, Staff report, 2016 04 26
Washington - **FBI Director James Comey said Tuesday he has seen some improvement in cooperation from China in fighting cybercrime following last year's bilateral agreement on the issue.** Chinese authorities "seem to have an agreed upon framework for what is nation-state action appropriate, that is intelligence collection, and what is theft," Comey told a cybersecurity event in Washington, when asked about international cooperation on cybercrime. "There are signs of progress in the Chinese helping us impose costs on active engagement and theft. I'm reasonably optimistic (about China), less so with Russia."

FBI says it can't explain how iPhone was hacked
Washington Post, Ellen Nakashima, 2016 04 27
Washington - **The FBI intends to tell the White House this week that its understanding of how a third party hacked the iPhone of a shooter in San Bernardino, Calif., is so limited that there's no point in undertaking a government review of whether the tool should be shared with Apple, officials said**. The decision, said officials familiar with the discussion who spoke on the condition of anonymity, ends several weeks of internal debate by bureau lawyers and technical experts about the FBI's obligation to disclose the method. Last month, the FBI paid more than $1 million for a tool to crack an iPhone used by one of the shooters in California. But the contract did not include rights to the software flaws that went into the tool, officials said. As a result, the bureau has a limited technical understanding of how the method worked, officials said.

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

Former head of MI5 says French authorities were blamed too quickly for the Paris terror attacks
BT.com (UK), Staff report, 2016 05 03
London - A **former head of MI5 believes French authorities were blamed too quickly for the Paris terror attacks. Baroness Eliza Manningham- Buller** also said the hunt for scapegoats was damaging and that no service is automatically at fault when something like last November's tragedy occurs. However she added that she was not seeking to suspend accountability and that she would have resigned if MI5 was found to have made a serious error under her leadership. Baroness Manningham-Buller told the Radio Times: "The head of a Commonwealth security service once told me he intended to resign if a terrorist act happened under his watch, but it's a mistake to assume that a service is automatically at fault when that happens.

ISIS hackers threaten to leak 'British secret intelligence' obtained from Ministry of Defence
The Mirror UK, Jonathan Sharman, 2016 05 01
London - **Islamic State hackers have threatened to leak "secret intelligence" they claim to have obtained from a mole at the Ministry of Defence, and say they are slowly "infiltrating" the UK and America.** A group calling itself the **Islamic State Hacking Division** made the claim in an anti- drone warfare document that purported to make public the identities, addresses and other details of US Predator and Reaper drone operators. The terrorists used the hit-list document to suborn the murder of drone teams it dubbed "cowards". But the the details of US military personnel appeared to have been scraped from publicly-accessible sources like Facebook, rather than obtained through a hack or leak, the Sunday Times reported. Several British ISIS terrorists, including the murderer Mohammed Emwazi, known as Jihadi John, have been killed in drone strikes.

GCHQ Has Disclosed Over 20 Vulnerabilities This Year, Including Ones in iOS
Motherboard Blog, Joseph Cox, 2016 04 30
Analysis: Earlier this week, **it emerged that a section of Government Communications Headquarters (GCHQ), the UK's signal intelligence agency, had disclosed a serious vulnerability in Firefox to Mozilla.** Now, GCHQ has said it **helped fix nearly two dozen individual vulnerabilities in the past few months, including in highly popular pieces of software like iOS.** "So far in 2016 GCHQ/CESG has disclosed more than 20 vulnerabilities across a number of software products," a GCHQ spokesperson told Motherboard in an email. CESG, or the National Technical Authority for Information Assurance, is the information security wing of GCHQ. Those issues include a kernel vulnerability in OS X El Captain v10.11.4, the latest version, that would allow arbitrary code execution, and two in iOS 9.3, one of which would have done largely the same thing, and the other could have let an application launch a denial of service attack. The spokesperson also pointed to two vulnerabilities in Squid, a caching proxy which can improve web response times. Recently, GCHQ intervened in the rollout of smart gas and electricity metres, which were planned to use a signal encryption key. "We are not always credited by vendors for bugs that we disclose.

British jihadist taunts security services with account of how he and Jihadi John escaped to Qatar National Bank
International Business Times (UK), Jason Murdock, 2016 04 28
London - **A 1.4GB trove of internal documents, files and sensitive financial data**

purporting to be from the Qatar National Bank (QNB) has been leaked online. The massive data dump appears to contain hundreds of thousands of records including customer transaction logs, personal identification numbers and credit card data. Additionally, dozens of separate folders consist of information on everything from Al Jazeera journalists to what appears to be the Al-Thani Qatar Royal Family. However, it is a folder listed as "SPY, Intelligence" that quickly catches the eye. **Upon analysis, it contains a slew of records listed as Ministry of Defence, MI6 (the UK foreign intelligence service) and Qatar's State Security Bureau, also known as "Mukhabarat".** The MI6 file, which sits alongside similar documents reportedly holding information on Polish and French intelligence, opens up an in-depth report on an alleged agent. This includes names of close relations, phone numbers, social media accounts and credit card data. Furthermore, in one instance, a file marked "wife", opens a photo showing a woman and two children.

Syria on UK passports
London Daily Telegraph, Josie Ensor, 2016 04 27
Beirut - **A British jihadist has taunted security services with a detailed account of how he and Isil executioner "Jihadi John" managed to travel through Europe to Syria on UK passports, despite being on terror watchlists**. Mohammed Emwazi, the Londoner filmed beheading Western hostages, and the unnamed friend, managed to leave Britain in early 2013 without attracting the attention of authorities. Writing in Islamic State's monthly Dar al-Islam magazine, the author says they travelled in a freight lorry carrying migrants along a popular people-trafficking route to a Channel port. **After giving UK border control the slip, they continued on to France and then Belgium, where he says they shaved off their beards, bought new clothes and booked flights to Albania using their British passports - confident MI5 had not shared its intelligence with the Belgian authorities.** Terrorism experts speculate that the account could come from Emwazi's associate Ibrahim Magag, a Somalia-born Londoner who went missing in late 2012 when he absconded from a Terrorism Prevention and Investigation Measure (Tpim) notice after ripping off his electronic tag.

Open borders let Isil into Britain, warns US spy chief
London Daily Telegraph, Josie Ensor, Tom Whitehead, 2016 04 27
London - **Open borders across Europe have allowed Isil to plant sleeper cells in the UK, poised to carry out Paris or Brussels-style massacres, America's intelligence chief has warned**. **James Clapper**, the US Director of National Intelligence, warned that the free movement of citizens around the European Union was "in conflict" with the need to protect security. He said there was evidence of fanatics from Islamic State of Iraq and the Levant (Isil) in Britain, Germany and Italy secretly plotting attacks like those witnessed in France and Belgium. He warned that some had taken advantage of the migrant crisis to slip into Europe and called for better intelligence-sharing between EU member states. The comments came a week after The Daily Telegraph launched a campaign to highlight weaknesses in border security with senior policing and counter-terrorism figures calling for a review. The US operates a far more stringent border control policy which sees potential suspects profiled and background checks carried out before they are allowed in. **Mr Clapper's warning echoes concerns voiced by the head of MI5 that Isil is intent on carrying out mass casualty attacks in the UK. Keith Vaz, chairman of the Commons home affairs select committee**.

Return to Table of Contents/ Retour à la table des matières

Australia/ Australie

ASIO has its funding cut
Australian Associated Press, Staff reporter, 2016 05 03
Canberra - **The Turnbull government has cut funding for ASIO by almost $15 million.** Despite being the lead security agency responsible for dealing with Australians who have joined IS, the federal government announced on Tuesday that ASIO's funding would be cut to $518,639 in 2016- 17. (Full report)

Money cards come under terror law scrutiny
Australian Associated Press, Staff Writer, 2016 05 01
Canberra - **The federal government plans to assess the risk of stored-value cards, which are believed to have been used in the Paris terror attacks, as it strengthens Australia's anti-money-laundering and counter- terrorism financing laws**. A review of the nation's AML/CTF laws tabled in parliament on Friday includes 84 recommendations to bolster the regime. One of the recommendations Justice Minister Michael Keenan says the government has identified for action is a risk assessment of the stored-value cards. **The report says anti-money laundering regulator AUSTRAC should assess the risks of these cards, to see whether the AML/CTF regulatory thresholds for these cards - at $1000 or more**, if cash can be withdrawn, or $5000 or more, if cash cannot be withdrawn - should be maintained.

Cyber security check-up
The Age, Georgia Wilkins, 2016 04 28
Canberra - **The federal government will foot the bill for cyber security "health checks" at some of Australia's biggest companies. The top 100 ASX-listed companies will be have the chance to get their voluntary check under the government's new $230 million cyber security package**. The government has declined to say how much it will spend on the scheme but said it hoped to eventually roll out the service to all public and private companies. It would not say whether the checks would be done by a government regulator or private consultants. Industry experts said on Monday that large companies should have to shoulder the burden of data protection themselves. "If the ASX100 are not competent enough to govern their own cyber security issues, those boards are not doing their jobs," said Dr Robert Merkel, a lecturer in software engineering at Monash University. Prime Minister Malcolm Turnbull last week announced the government's cyber security strategy, which will focus on closer collaboration of government and business. It is the result of a year-long review of the industry. The strategy will see the **Australian Cyber Security Centre** moved away from the **Australian Security Intelligence Organisation** in Canberra to allow for greater ties with business.

ASIO thought terror teen Numan Haider was being 'deliberately antagonising'
Nine MSN News Australia, Staff Writer, 2016 04 27
Canberra - **An ASIO director has been forced to justify the agency's failure to prevent a 2014 terror attack in Melbourne that left two police wounded and a teenager with a bullet in his head**. Testifying before an inquest into the stabbing of two Endeavour Hills police officers by radicalised teen Numan Haider, the high-level spook defended ASIO's inaction in the face of what seems to be compelling evidence that a plot was afoot. The inquest heard that Haider had used Google to search for "firecrackers wrapped in steel", "Tony Abbott next visit to Victoria", information about AFL, and the Holsworthy military base before telling a friend he planned to "do it soon". But ASIO failed to act, the Herald Sun reports, with the director, giving evidence under the codename "Natalie Mayfair", telling the hearing that the spy agency did not know what "it" was. Despite admitting security operatives had been warned against approaching the 18-

year-old, Ms Mayfair confirmed ASIO, which had discussed Haider with Victoria Police, had not changed his "threat level"."It seemed like he was being deliberately antagonistic and may have been attention seeking," she said.

Vic teen searched Tony Abbott's plans
Australian Associated Press, Genevieve Gannon, 2016 04 27
Melbourne - **ASIO had fears a radicalised Melbourne teen was considering targeting the then prime minister, Tony Abbott, an AFL game and a military base before he was shot in 2014 while attacking two police**. In the weeks before he was killed, Numan Haider had conducted internet searches of the terms "firecrackers wrapped with metal sheet", "Tony Abbott next visit to Victoria", "Holsworthy military base" and "AFL football", which a senior ASIO officer says was an unusual search for him. Haider had also told an associate he would "do it soon", an inquest into the young man's death heard on Wednesday in Melbourne. The ASIO officer, giving evidence under the pseudonym Natalie Mayfair, said she had shared this information with federal police in a meeting on September 17, 2014. Haider, 18, was shot in the head outside the Endeavour Hills police station after he stabbed a Victoria Police officer and an Australian Federal Police officer attached to the Joint Counter Terror Team on September 23, 2014. ASIO met with police three times in the week before Haider's death.

Return to Table of Contents/ Retour à la table des matières

New Zealand/Nouvelle-Zélande

Trust a vital asset as NZ faces future
New Zealand Herald, Gehan Gunasekara, 2016 05 03
Op-ed:With the recent announcements of manufacturing closures in New Zealand, such as Fisher & Paykel's Auckland plant, it is important to develop new knowledge-based jobs here. Twenty-first century business is increasingly data-driven by analytics and Big Data.. The recent Independent Review of Intelligence and Security by the Hon Sir Michael Cullen and Dame Patsy Reddy has produced remarkably **detailed recommendations for revamped laws surrounding the activities of our spy agencies. If they are implemented in their entirety we will have some of the toughest controls on such agencies in the western world**. If instead the Government cherry-picks aspects of the Cullen-Reddy report then the gaps would quickly be exploited by the agencies concerned and we may as well not have bothered with any reform. To give just one example, one of the currently neglected areas is "incidentally gathered information". **Electronic surveillance tends to "vacuum up" vast amounts of information. Most is undoubtedly discarded by the likes of the GCSB but currently it can be sent to its partners in the Five-Eyes network who can do what they want with it.** The report recommends plugging this gap by requiring the New Zealand agency to decide which part of the data it wants to keep or share and to go through procedures (such as an obtaining an interception warrant). Note: Gehan Gunasekara is an associate professor in commercial law at the University of Auckland Business School and advised the Law Commission on reform of the Privacy Act 1993.

New Zealand government seeking business help in cybercrime fight
Xinhua News Agency, John Macdonald, 2016 04 28
Wellington - **Leading international cyber security specialists will discuss how New Zealand businesses can help fight cybercrime at the first government-backed Cyber Security Summit in Auckland next week,** Communications Minister Amy Adams said

Thursday. "Cyber-attacks can and do damage our economy. Businesses are acutely aware of the 257 million NZ dollars (178.2 million U.S. dollars) lost to cybercrime last year," Adams said in a statement. "The challenge cyber security presents can't be met by the public sector alone. What's clear is that we need a joined up response - - the private and public sectors working together to share information and expertise," she said. "The summit is an opportunity for chairs and chief executives from across New Zealand to continue the conversation around how as a country we tackle the threat of cybercrime, and improve our resilience and security in this increasingly digital age."

Return to Table of Contents/ Retour à la table des matières

International

China/Chine

Children in Xi's China Urged to 'Spot the Spy'
Wall Street Journal, Te-Ping Chen, 2016 04 30
Beijing - **In Xi Jinping's campaign to galvanize China around threats to national security, the latest focus has turned to spies**. In recent weeks, **the country has dramatically amped up a call for vigilance even from its youngest citizens, with games such as "Spot the Spy" being played in schools**. Around the first-ever **National Security Education Day** in mid-April, volunteers in Beijing handed out thousands of umbrellas imprinted with a hotline to call to report any perceived risks. Posters have gone up in housing complexes and at subway stops with a cartoon story of a foreigner posing as an academic who tricks his Chinese girlfriend into leaking state secrets. The various campaigns warn of other guises as well, including consultants or commercial investigators. Since Mr. Xi assumed power in 2012, the country has sought to beef up domestic security, including passing a counterespionage law and a national-security law last year. The emphasis comes as Mr. Xi moves to shore up the party's hold on power and build social cohesion amid more trying economic times. The government says the national- security law was needed to counter emerging threats, from cybercrime to terror.

China Reins in Foreign Groups Under New Law
New York Times, Edward Wong, 2016 04 29
Beijing - **China took a major step on Thursday in President Xi Jinping's drive to impose greater control and limit Western influences on Chinese society**, as it passed a new law **restricting the work of foreign organizations and their local partners, mainly through police supervision**. More than 7,000 foreign nongovernment groups will be affected, according to state news reports. Foreign groups working across Chinese civil society -- on issues including the environment, philanthropy and cultural exchanges, and possibly even in education and business -- will now have to find an official Chinese sponsor and must register with the police. This also applies to groups from Taiwan, Hong Kong and Macau. Those organizations that do not receive official approval will be forced to stop operating in the country.

Taiwan Readies for Fresh Wave of Espionage by China
Voice of America, Ralph Jennings, 2016 04 28
Taipei - **Taiwan's incoming ruling party is signaling its intention to get tougher on espionage by China as cross-strait relations sour and increased contact between the two sides makes spying easier.** The **Democratic Progressive Party** government of President-elect Tsai Ing-wen intends to raise the military budget and experts said it may add a cyber-

espionage unit to the defense ministry. Parliament, which is controlled by the same party, aims to pass a bill by year's end that would cut pensions for Taiwanese military retirees who spy for China. Analysis said spying cases, which embarrassed Taiwan in November and again this week, stand to increase because China will lack legal channels to understand the island's new government after May 20, when Tsai takes office.

Beware of secret lovers; China warns women of seductive foreign agents
Los Angeles Times, Julie Makinen, 2016 04 28
Beijing - When Yu Hongna, a 24-year-old graduate student in English language and literature, told her mom she was dating a British guy, her mother was wary. "She warned me not to be deceived by a foreigner's honey tongue, and they can be bad guys," Yu said. But it's not just parental approval that Yu has to worry about. **The Chinese government itself is cautioning young women to think twice before taking up with boyfriends from overseas. Handsome gents from abroad, authorities say, are on the prowl for ladies with access to state secrets.** To mark China's first **National Security Education Day** this month, propaganda officials plastered certain neighborhoods of the capital with a poster campaign called "Dangerous Love" warning of devious Don Juans lurking in their midst.

Aviation workers may face security checks
China Daily, Xin Dingding, 2016 04 27
Beijing - **The civil aviation authority is adding measures to a regulation to prevent terrorist attacks on passenger planes and airports,** including for the first time requiring that all industry employees receive security clearance. According to the draft of the revised **Regulation on Safety and Security of Civil Aviation**, all of the country's civil aviation personnel must undergo background security investigations. Additionally, civil aviation and public security administrations, airports and airlines are asked to enhance their anti-terrorism intelligence capabilities. Safety and security plans drafted by foreign airlines that operate in China also must conform with China's laws and regulations, and the plans need to be examined and approved by local civil aviation administrations. Besides anti- terrorism measures, **the draft also bans passengers from attacking or occupying check-in counters, security check lanes and boarding gates in airports, and it stipulates penalties for various offenses**. These parts of the plan are designed to deal with an increasing number of angry passengers who are frustrated by flight delays. The draft is posted on the website of the State Council's Legislative Affairs Office to solicit public opinion before May 20. The current regulation was adopted 20 years ago.

Return to Table of Contents/ Retour à la table des matières

Russia/Russie

'ISIS recruiters' arrested - including sisters who worked at Moscow airport and for Russian intelligence - after raid on apartment uncovers grenades and explosives
Daily Mail (UK), Will Stewart, 2016 04 28
Moscow - **A Russian secret services operation has exposed a gang of alleged jihadist recruiters including a woman who is said to work for an intelligence agency and her sister who is believed to be employed at a Moscow airport**. Four people - the women and two men - were detained on suspicion of involvement in terrorist activities, along with associates, it was reported today. A **Federal Security Service (FSB)** and police operation detained the group plus an alleged male 'leader'. They were identified as recruiters for the Islamic State working in the Russian capital, it was claimed. A source cited by pro-Kremlin

media outlet LifeNews stated: 'According to information from the secret service, all are active ISIS recruiters.' A woman named only as Saida K was reported to be working at Vnukovo Airport in Moscow, used by major airlines but also VIPs including President Vladimir Putin and senior officials as well as visiting foreign dignitaries.

Return to Table of Contents/ Retour à la table des matières

Europe

La Suisse craint le retour de djihadistes
Le Temps (Suisse), Valérie de Graffenried, 2016 05 03
Berne - **Dans son rapport 2016, le Service de renseignement suisse avertit: des individus radicalisés basés en Suisse peuvent commettre des actes de violence sans avoir été en contact direct avec un groupe terroriste** ou s'être rendus dans une zone de djihad Menaces La Chine citée comme facteur de risque Extrémisme de gauche, extrémisme de droite, PKK, prolifération nucléaire, espionnage: les « menaces » pour la sécurité de la Suisse se suivent et se ressemblent chaque année dans le Rapport de situation du SRC, avec quelques variations sur le baromètre de la peur. Mais cette année, **le Service de renseignement de la Confédération (SRC),** les yeux rivés vers le futur, a décidé de mettre l'accent sur la Chine.Le pays est le principal partenaire commercial de la Suisse en Asie et, après l'UE et les Etats-Unis, le troisième plus important du monde. L'accord bilatéral de libreéchange entré en vigueur en 2014 a permis des conditions favorables pour les entreprises suisses, de nombreuses taxes de douanes étant progressivement abaissées. Et l'augmentation éclair de la nouvelle classe moyenne en Chine a provoqué l'enregistrement de plus d'un million de nuitées de Chinois en Suisse en 2014, précise le rapport. Mais c'est justement cette dépendance de plus en plus marquée vis-à-vis de la croissance économique de la Chine qui est considérée comme un risque.

Germany's domestic intelligence chief calls for more powers in anti-terror fight
Deutsche Welle, Staff report, 2016 05 02
Berlin - Hans-Georg Maassen told a symposium in Berlin his intelligence agency needed more resources to fight threats from militant Islamists and right-wing extremists. He warned of a growing danger of terror attacks in Germany. Maassen told Monday's symposium, called to discuss the global threat posed by militant Islamists, that "a worsening security situation needed corresponding adjustments" in the powers and resources given to security authorities. Among other things, he suggested tighter supervision of conduct for convicted Islamists and the introduction of electronic tagging. He also criticized a recent ruling by Germany's highest court, based on personal privacy concerns, to revoke some anti-terror powers accorded to the authorities under a 2009 law.

Comment Europol lutte contre la propagande djihadiste sur Internet
Le Point, Marc Leplongeon, 2016 05 02
Paris - La communication de l'EI peut-elle être contrée ? Un officier supérieur du **centre antiterroriste d'Europol répond aux questions du Point.fr. Cette cellule est composée de 17 personnes et a été mise en place très rapidement après les attentats de janvier 2015 contre Charlie Hebdo et l'Hyper Cacher de Vincennes.** Le coeur de métier d'Europol est l'analyse criminelle. Historiquement, nous possédions un service appelé « check the web » dont l'objectif était de surveiller sur Internet toutes les sources ouvertes, c'est-à-dire les sources que tout le monde peut consulter. Nous suivons ainsi depuis une dizaine d'années l'évolution de la propagande terroriste et nous concentrons principalement sur deux groupes que sont Al- Qaïda

puis l'État islamique (EI). Qui en sont les grands penseurs ? Quels thèmes sont le plus souvent abordés ?

Secret service can hack innocent people to reach target: Volkskrant
Dutch News, Staff Writer, 2016 04 30
Amsterdam - **The new law giving greater powers to the secret service to intercept internet traffic will allow officials to hack innocent people despite protests by privacy groups**, the Volkskrant said on Friday. The paper bases its claim on the new draft legislation, which has not yet been officially published. The new powers mean that people who share the same server as suspects could be hacked by the spy service to get access to their targets. Ministers say this is crucial because suspects are often well protected against hacking.

Poroshenko Removes Foreign Intelligence Service Head Hvozd
Ukraine News Agency, 2016 04 29
Kiev—**President Petro Poroshenko has dismissed Chairman of the Foreign Intelligence Service Viktor Hvozd.** Ukrainian News Agency learned this from Decree 193 dated April 29. The decree did not indicate the cause of the dismissal. As Ukrainian News Agency earlier reported, Poroshenko has dismissed an advisor to the President Yurii Biriukov

Hans Leyendecker: 'The BND has a life of its own'
Deutsche Welle, Staff report, 2016 04 28
Interview - Over two years after the NSA affair, **the head of Germany's foreign intelligence agency is leaving his post.** Investigative journalist Hans Leyendecker tells DW it's because he didn't know whom his staff were spying on. DW: More than two and a half years ago, the German people - who are very sensitive when it comes to matters of privacy protection - were shocked to learn about the NSA affair. Now, Gerhard Schindler, the head of Germany's foreign intelligence agency, BND, is being replaced. Why is that only happening now? Hans Leyendecker: Because, at the time, the assumption was that he didn't know what certain departments were doing. But now, looking back, it's become clear that this has often been the case at the BND. You could say that the BND, which is turning 60 this year, has always tended to have a life of its own, no matter who was president. Now this president is suffering from this tendency to act independently. **In this case, it's about the fact that selectors were being used [search terms provided by the NSA to conduct surveillance, including on allies - Ed.] and that Schindler had no knowledge about what these selectors were.** DW: You talk about the BND having a life of its own.

Romania's Anti-Graft Chief Slams Intelligence Service
Balkan Insight, Staff report, 2016 04 28
Bucharest - **The chief prosecutor of the National Anti-Corruption Directorate, the DNA, Laura Codruta Kovesi, on Tuesday accused Romania's Foreign Intelligence Service, SIE, of not sending the DNA any information about possible crimes abroad since she became head of the DNA.** "I have never received any counter-intelligence reports from the SIE since I took over this office at the DNA. However, we see many suspects setting up businesses abroad. This raises the reasonable question about why we have never received any information about such activities," she said. "We haven't been informed about foreign bank accounts, luxury villas or luxury yachts," Kovesi said, emphasizing that "it is illegal to have information about possible crimes and not inform the DNA.

Head of Department at National Security Agency Indicted for Corruption, Classified Information Disclosure

Bulgarian News Agency, 2016 04 27
Sofia—The **Specialized Anticorruption Unit (SAU) of the Sofia City Prosecution Office has presented to the Sofia City Court an indictment against Miroslav M., head of department at the Financial Security Specialized Directorate of the State Agency for National Security (SANS)**, the prosecution service said on Wednesday. The indictment states that in Sofia between September 27, 2013 and October 1, 2015, M. disclosed information classified as a state secret, contained in 11 documents which were entrusted to him in his official capacity. M. provided copies of the documents to a former voluntary collaborator with the National Security Service at the Interior Ministry and the SANS and used him to obtain extra cash. The information in question concerned the operational methods and means used by the security services and their voluntary collaborators, which could have endangered their life and safety and could have obstructed work on operational cases. **The offence had a particularly grave consequences for national security** because the information contained in the documents reveals events and actions against national economic and financial security, reveals the operational interest that the service takes in particular persons, the information gathered about them and other persons who have committed or who were preparing to commit offences endangering national security, the press release says.

Belgique / Terrorisme - Antiterrorisme: la police des polices belge pointe des manquements
Radio France Internationale, Pierre Bénazet, 2016 04 27
Bruxelles - **La police des polices belge a présenté mardi 26 avril devant une commission parlementaire les premiers résultats d'un rapport entamé après les attentats de Paris** qui conclut à **de nets manquements**. Parmi les noms des personnes soupçonnées de radicalisation figuraient à la fois Salah Abdeslam et son frère Brahim, celui qui s'est fait exploser boulevard Voltaire lors des attentats du 13 novembre. Il y a un an, dans le cadre d'une enquête relative à un trafic de drogue, un procès-verbal signé par un commissaire de police bruxellois signale à la cellule antiterroriste que Brahim se serait peut-être rendu en Syrie. Les deux frères sont auditionnés mais pas inculpés. Leur dossier est classé « rouge », code des dossiers urgents mais auquel il n'est pas donné suite en l'absence de nouvel élément concret, et aussi parce que d'autres priorités s'imposent entre temps.

Tough Grilling Behind German Intel Chief's Abrupt Sacking
Sputnik (Russia), Staff report, 2016 04 27
Moscow - **The reasons behind the abrupt replacement** - two years early - **of the head of Germany's BND foreign intelligence agency, Gerhard Schindler, by Chancellor Angela Merkel are a combination of mistrust and tiredness**. Schindler had faced tough questions by German lawmakers after it was revealed that his agency had cooperated with the **US National Security Agency (NSA) in surveillance operations on its European allies via the Bad Aibling surveillance station used by the BND and Americans near Munich**. An investigation by German broadcasters ARD, NDR and WDR, together with the Süddeutsche Zeitung said various reasons were behind the reported reshuffle, including a major BND restructuring that will see the agency transfer many of 6,500 employees from Munich to new headquarters in Berlin by next year. However, sources within the **BND suggested Schindler's position had become untenable because of the NSA links**, which caused anger when it was revealed and led to a parliamentary investigation in which he faced a barrage of criticism.

Germany confirms that spy agency chief will leave his post 2 years early
Reuters, Staff report, 2016 04 27
Berlin - **The German government confirmed on Wednesday that Gerhard Schindler, the head of the BND foreign intelligence agency, would leave his post two years early but**

provided no reason for the surprise change. In a short statement, Chancellor Angela Merkel's chief of staff Peter Altmaier said Mr Schindler, who has run the BND since 2012 and is not due to retire until 2018, **would be replaced on July 1 by Mr Bruno Kahl,** an official in the Finance Ministry responsible for privatisations and government real estate. "The BND faces major challenges over the coming years, encompassing all aspects of its work," Mr Altmaier said. "These include the evolution of its mission in light of shifting security challenges, the upgrading of the agency on the technical and personnel front, **organisational and legal consequences arising from the parliamentary investigation into the NSA** and the move of large parts of the BND from Pullach to Berlin." The move comes a year after damaging revelations that the BND had helped the United States National Security Agency spy on European allies.

François Heisbourg: « L'état d'urgence permanent est une victoire psychologique du terrorisme »
L'Opinion, Charles Sapin, 2016 04 27
Non identifié - Contributeur aux trois derniers livres blanc sur la défense et la sécurité nationale, **François Heisbourg liste les défaillances des pouvoirs publics dans la lutte contre le terrorisme** Conseiller spécial à la Fondation pour la recherche stratégique, président de l'International institute studies de Londres et du Centre de politique de sécurité de Genève, François Heisbourg signe mercredi un essai aux éditions Stock, intitulé **Comment perdre la guerre contre le terrorisme.** Un retour critique sur la façon dont les gouvernements successifs luttent contre le terrorisme. Au fil des semaines, la capacité de réaction du gouvernement s'est révélée très faible. Cette année 2015 a été marquée par un certain nombre d'événements que je ne veux pas voir se reproduire. C'est pour cette raison que j'ai écrit ce livre. Quelles sont les principales erreurs du gouvernement dans la lutte contre le terrorisme? La première erreur a été commise sous le mandat de Nicolas Sarkozy: marginaliser ce que l'on peut appeler le renseignement de proximité. **Tout d'abord en éliminant les renseignements généraux, lors de la création de la direction centrale du renseignement intérieur (DCRI) en 2009, et en bannissant la gendarmerie nationale du premier cercle du renseignement, alors qu'elle couvre près 90 % du territoire**. Nous avons vu les conséquences très rapidement sur le terrain, notamment à Toulouse avec l'affaire Merah en 2012.

Berlin axes scandal-hit foreign spy chief
The Local (Germany), Staff report, 2016 04 27
Berlin - **The German government confirmed on Wednesday that the head of its foreign intelligence service would be replaced two years ahead of schedule, triggering mass speculation about the cause. Gerhard Schindler** had given "long years of commendable service" at the head of the **Bundesnachrichtendienst (BND),** Germany's foreign spying agency, Chancellery chief Peter Altmaier said on Wednesday. The departure had initially been reported by German media including the Süddeutsche Zeitung before the government confirmed Schindler's replacement. And it seems that the spy chief needed to be pushed out of the door. Schindler at first refused to resign and had to be forced to leave by his superiors at the Chancellery, Berlin's Tagesspiegel reported citing government sources. But questions remain over whether the BND boss is being replaced because of embarrassing stories about the agency in the press - or whether the government prefers an intelligence chief who is politically closer to them.

Les renseignements français recrutent leurs indics au Maroc
Libération, Journaliste maison, 2016 04 27
Paris - **Le danger terroriste se fait de plus en plus menaçant. Pour le contrer, les**

renseignements français sont en passe de recourir à des méthodes bien adaptées. Le dernier moyen mis en place serait le recrutement d'indicateurs et d'agents marocains pour leur prêter main forte en vue de déjouer les stratagèmes des cellules dormantes, ou en action dans des quartiers populaires habités par une majorité de ressortissants d'origine maghrébine. L'expertise marocaine en la matière n'est plus à démontrer. Les renseignements marocains ont été ofn ne peut plus efficaces, en fournissant à leurs homologues français des tuyaux d'une extrême importance. **Selon des médias français, la direction générale de la sécurité intérieure (DGSI) recrutera 430 personnes dans les cinq années à venir**. Il y a quelques jours seulement, le Premier ministre Manuel Valls a annoncé, dans ce contexte, le renforcement des services de renseignements.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Crown Prince Muhammad: Architect of counter-terrorism strategy
Saudi Gazette, Mansour Al-Shahri, 2016 04 29
Jeddah - **Crown Prince Muhammad Bin Naif, deputy premier and minister of interior, is regarded as the architect of the Kingdom's successful counter-terrorism strategy and modernizing the Kingdom's security forces and enhancing its efficiency at par with world-class standard**. He can rightly be called as the "Royal Military Commander." This is because he has won two royal honors for his relentless efforts in combating terrorism, decimating Al-Qaeda in the Kingdom, and foiling several planned terror attacks and plots aimed at undermining the security and stability of Saudi Arabia. Crown Prince Muhammad has possessed extraordinary caliber and wisdom as well as very good expertise in governance, handling security issues and taking prompt decisions and swift actions.

Hadramout security agencies being rebuilt with coalition help
Gulf News, Saeed Al Batati, 2016 04 28
Al Mukalla - The **chief of security of Yemeni province of Hadramout, Brigadier Mohammad Saeed Al Jariri,** said on Wednesday that he is working with UAE officers **to reconstruct security institutions that broke down a year ago** when Al Qaida stormed the province's capital and many other major cities. The UAE officers are working in Yemen under a Saudi-led coalition to restore order in the impoverished country. "I have been in touch with UAE officers for months discussing how to build effective security agencies. They promised to build the security bodies from scratch," Al Jariri told Gulf News. Government forces backed by the Saudi-led coalition recaptured the city of Al Mukalla, Yemen's fifth largest city, on Sunday night after fierce clashes with Al Qaida in the eastern suburbs of the city. Al Jariri said that security forces have arrested many Al Qaida operatives in the city and raided many suspected arms depots.

Intelligence services minister: We can't count on US at UN
Jerusalem Post, Gil Hoffman, 2016 04 28
Jerusalem - US President **Barack Obama's administration has not been supportive enough of Israel at the UN and elsewhere, Intelligence Services Minister Israel Katz** charged on Tuesday night in an interview with The Jerusalem Post. Katz will be coming to New York next month to address The Jerusalem Post Conference on May 22. While he is in the US, he intends to seek Democratic and Republican support for legislation in Congress backing proactive sanctions on Hezbollah and whoever helps the terrorist group with money or weapons. He said the fact that Arab countries also see Hezbollah as a terrorist organization helps on the issue. "It

is very important for Israel to know that the US supports us in international organizations, including with its veto at the United Nations Security Council," he said. "This is a key component of our national security and our security considerations. Unfortunately, with the current administration, we cannot be sure of that."

Senate panel endorses constitutional amendments
Jordan Times, 2016 04 28
Anam—The Senate's legal committee on Thursday endorsed the draft constitutional amendments as sent by the Lower House during a meeting chaired by Senate President Faisal Fayez, the Jordan News Agency, Petra, reported. Fayez said the amendments show that the Kingdom is marching steadily towards political reform, embodied by the formation of parliamentary, partisan governments, based on a clearly defined vision. The Lower House on Wednesday passed the constitutional amendments that gave new powers to the King and allowed citizens with dual nationalities to occupy senior public posts and parliamentary seats with a sweeping majority. As reworded by the Council of Ministers, a new paragraph was added to Article 40 of the Constitution to read: Despite what is stated in Paragraph A, the King shall exercise his powers individually and **appoint the Crown Prince,** the Regent, Senate president and members, and members of the Constitutional Court, president of the Higher Judicial Council, **the army's chairman of the Joint Chiefs-of-Staff and the General Intelligence Department and Gendarmerie Department directors.**

Operational Cyber Intelligence
Times of Israel, 2016 04 27
Jerusalem - **Visitors to the CyberTech 2016 exhibition had the impression that every single exhibitor boasted a cyber intelligence capability.** Indeed, **cyber intelligence (or threat intelligence) has evolved** into one of the hottest trends of the cyber technology industry in the last few years. Even the relatively small Israeli market generates massive demand for intelligence services and some ten product and service companies are involved in this activity, competing one another.

Return to Table of Contents/ Retour à la table des matières

Asia/Asie

Identity of key IS recruiter still a mystery (Canada).
The Hindu, Vijaita Singh, 2016 05 03
New Delhi - Three months after Indian agencies busted a widespread Islamic State network with many members in India, its key recruiter's identity still remains a mystery. Security agencies believe that Shafi Armar alias Yousuf al Hindi operates from Syria but are not fully convinced if all communications in his name are from this former Indian Mujahideen member. Eight of the 25 suspects in the custody of the **National Investigation Agency** and allegedly recruited by Armar have told interrogators that they had never seen him as he did not communicate with them through video calls. Armar used only web-based applications, 'We Chat', 'Kick' and the audio messaging service on Skype. The answer to Armar's location and whether he indeed posted messages from Syria, now lies in requests sent to the U.S., **Canada**, China and Hong Kong.

Radicalisation a real threat, says intel official
The Hindu, Vijaita Singh, 2016 04 27
New Delhi - **Top intelligence officials have been asked to step up techniques to keep a watch on activities related to the Islamic State,** with 80-100 youths in India still under the

scanner for links to the terror outfit. The IS threat was one of the topics discussed at a **two-day conference organised by the Intelligence Bureau in Delhi.** At the conference, National Security Adviser Ajit Doval is learnt to have given a pep talk to intelligence officials from across the country. A senior official said that as for the unrest in Kashmir, intelligence officials felt "radicalisation" was a more real threat than the Pakistan-backed terror outfits that operated in the State. "The number of militants killed so far this year is more than that in the previous year in the Valley. The real threat is radicalisation of young men, and this has to be prevented. We have more or less controlled Pakistan-based terrorist elements in the Valley, and they are not gaining ground," the official said.

20 overseas N. Korean restaurants closed: spy agency
Yonhap News Agency, Staff reporter, 2016 04 27
Seoul - **Some 20 overseas restaurants run by the North Korean regime have either stopped operations or closed down, a South Korean ruling party lawmaker said Wednesday, citing Seoul's spy agency.** Lee Chul-woo of the ruling Saenuri Party made the comment to reporters after holding a meeting with officials from the National Intelligence Service (NIS) at the National Assembly. "The restaurants in foreign countries have either halted business or have been closed due to financial difficulties," Lee said, adding that the NIS believes Pyongyang will more likely turn to illegal means to raise hard currency. North Korea-run restaurants in foreign nations serve as one of the main sources of hard currency flowing into North Korea. Some of these funds are suspected of bankrolling the North's nuke and missile programs amid toughened international sanctions.

Return to Table of Contents/ Retour à la table des matières

Africa/Afrique

Intersociety Accuses FG, Security Agents of Gross Human Rights Abuses
This Day, 2016 05 03
Abuja—The **International Society for Civil Liberties & the Rule of Law (Intersociety) has accused the President Muhammadu Buhari-led Federal Government of gross human rights violation aided by the activities of the security agencies**. This was contained in a well detailed statement signed by the Board Chairman, Intersociety, Emeka Umeagbalasi, titled: "Ethnic Bloodshed, Rights Abuses & Other Regime Atrocities In Nigeria: Exposing The Conspiratorial Roles Of Some CSOs, Buhari Administration & Security Forces". Umeagbalasi, in the statement, gave instances of what the group viewed as the conspiratoral roles of the security agents, in the state of insecurity and killings across the country. He noted that while the security agencies including the military, **Nigerian Police and Department of State Security Service (DSS),** were quick to act in arresting and quelling protests by members of Indigenous People of Biafra (IPOB) and Movement for the Actualisation of the Sovereign State of Biafra (MASSOB), they were on the other hand slow to act in defence of the defenceless citizens in Agatu in Bunue and Nimbo at Uzo-Uwani in Enugu State massacred by suspected herdsmen.

Le Quai, nid d'espions
L'Opinion, Pascal Airault, 2016 04 28
Dakar - **Ancien haut responsable de la DGSE, Christophe Bigot vient d'être nommé comme ambassadeur de France au Sénégal**. Un mouvement symptomatique : les diplomates ont aujourd'hui un pied au sein des services secrets, qui ont des agents dans les ambassades françaises. Au fil des ans, la Direction générale de la sécurité extérieure (DGSE) et le ministère des Affaires étrangères ont fini par cohabiter harmonieusement même s'ils forment un couple

singulier. La relation entre le ministère des Affaires étrangères et la Direction générale de la sécurité extérieure (DGSE) n'a toujours pas été idyllique mais elle est aujourd'hui sanctuarisée. Les cadres passent même allègrement d'une maison à l'autre. Le 15 avril, **Christophe Bigot** a succédé à Jean-Félix Paganon à la tête de l'ambassade de France au Sénégal. **Il occupait le poste le directeur de la stratégie (DS) à la DGSE**, après avoir été ambassadeur en Israël de 2009 à 2013. Le choix de cette personnalité, à la double experience diplomatique et du renseignement, ne sera pas inutile d'un pays actuellement très exposé à la menace terroriste. Dakar accueille les éléments français du Sénégal (EFS), commandés par le général Pascal Facon, sur la base de Ouakam.

Pour la création d'une association algérienne de cryptographie
All Africa, Journaliste maison, 2016 04 27
Oran, Algérie - **La création d'une société savante dédiée à la cryptographie figure parmi les ambitions affichées mardi à Oran par des participants à un un premier workshop international consacré à cette spécialité scientifique portant sur le développement des techniques de protection des données informatiques**. "La réflexion est engagée en vue de la création d'une association algérienne de cryptographie", a indiqué Pr Adda Ali Pacha, président de la rencontre réunissant deux jours durant une cinquantaine de participants algériens et étrangers à l'Université des sciences et de la technologie Mohamed Boudiaf (USTO-MB).

Return to Table of Contents/ Retour à la table des matières

Americas/Amériques

Argentina ex-air force head on trial for disappearances
Agence France Presse, 2016 05 03
Buenos Aires - **An Argentine former military chief has gone on trial for the disappearance of a left-wing couple during the country's dictatorship**. The former chief of the air force, Omar Graffigna, 90, is accused with two other defendants of the forced disappearance of Jose Manuel Perez Rojo and Patricia Roisinblit in 1978. His trial opened on Monday, with the court on the outskirts Buenos Aires hearing the charge list of accusations of crimes against humanity. Perez and Roisinblit were allegedly kidnapped by air force personnel on October 6, 1978 and have never been found. The victims' families say Roisinblit gave birth in captivity and her child was stolen. **One of the two other defendants, former intelligence officer Francisco Gomez, was already convicted in 2005 of stealing Roisinblit's child.**

Honduras strengthens border security in anticipation of Salvadoran gangs fleeing
Southern Pulse Info Latin America News, 2016 05 28
Tegucigalpa - **Honduras announced on 27 April 2016 an increase in security forces along land and sea borders to keep out individuals with criminal motives, alluding to Salvadoran gangs (La Prensa Grafica). The Fuerza de Seguridad Nacional (Fusina)** announcement comes after El Salvador unveiled new elite police-military groups to regain territorial control and target gang members. **Fusina added it would increase intelligence gathering on individuals planning to illegally enter Honduras.** Furthermore, citizen security operations focused on decommissioning weapons, ammunition, explosives, drugs, illicit money, as well as capturing criminal groups would continue throughout the country (El Heraldo).

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

04-05-2016 to/au 10-05-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Armed with chalk, Ottawa women take on Canada's spy agencies -- over parking
CBC News, Hillary Johnstone and Trevor Pritchard, 2016 05 10
Ottawa - **Two women living in Ottawa's east end say they're upset their neighbourhood's been taken over by employees of Canada's intelligence agencies -- and they're fighting back with pieces of chalk.** Retired nurses **Danielle Sullivan** and **Diane Day** have been patrolling the residential streets that border the headquarters of the **Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE), outlining parked cars and trucks with chalk and carefully marking down the time the vehicles arrived.** They do it because the drivers of those vehicles, they say, tend to overstay their welcome. "It's an ongoing issue. We've had this for three years. And it's just unbearable," said Sullivan, who lives on Leigh Crescent, near the two agencies. 3-hour limit On most of the residential streets around CSIS and CSE headquarters, vehicles are allowed to park for a maximum of three hours. Sullivan said drivers often arrive early in the morning, well before the posted restrictions kick in, and leave their vehicles in their spots for longer than the posted limit -- or they move their car just up the block before it gets ticketed. The resulting glut of vehicles makes life difficult for residents who want to do renovations, the pair said, while also hampering snowplows, buses, and other city vehicles. In a statement to CBC News, CSIS noted that while there are "limited number of parking spaces" at its headquarters, the agency works to ensure that employees are obeying municipal and private parking restrictions. CSIS employees are also "encouraged to consider alternative transportation methods" like public transit, the agency said. CSE issued a similar statement, noting that they also offer an "internal ride sharing tool" for employees looking for a ride to work.

RCMP to examine Panama Papers data: Goodale
iPolitics.ca, Staff reporter, 2016 05 10
The RCMP and other **Canadian police forces will be poring over the Panama Papers data released Monday, searching for possible connections to criminal activity, says Public Safety Minister Ralph Goodale.** Speaking to reporters on the way out of question period, Goodale said Canadian tax authorities aren't the only ones that have taken an interest in the documents from the Panamanian law firm Mossack Fonseca, obtained by the International Consortium of Investigative Journalists (ICIJ). "Now that it is in the public domain it will be possible for all the appropriate authorities, including the revenue agency and the RCMP, potentially other police forces to take a look at it and determine whether or not it reveals behaviour that ought to be further investigated." **Goodale also didn't rule out the possibility the data could be of interest to the Canadian Security Intelligence Service (CSIS), Canada's spy agency. "If there is a security dimension to this that raises any kind of alarms with CSIS, they will take the appropriate steps."** Goodale's comments come as the ICIJ further lifted the veil of secrecy over the identities of thousands of people around the world who hold bank accounts in offshore tax havens Monday, making part of the information from the 11.5 million documents it obtained public through a searchable database and through downloads. In April, a network of media outlets around the world led by the ICIJ began rolling out a devastating series of stories based on a year-long investigation of 11.5 million files leaked from the Panamanian law firm Mossack Fonseca. The stories detail one bank's part of the global web of offshore companies that enables clients ranging from members of the Mafia to

international political leaders or members of their families to stash assets in secretive tax havens.

Eid's counsel mulls strategy for sentencing on fraud convictions
Ottawa Citizen, James Bagnall, 2016 05 07
Ottawa - Former construction boss and CSIS informant Roland Eid appeared in court Friday for the first of what could be several sessions before Justice Timothy Ray in connection with the sentencing phase of his criminal fraud proceeding. Eid was convicted on Monday of 10 counts of fraud and other offences related to the 2008 bankruptcy of his firm, ICI Construction. Ray ruled that Eid had perpetrated a fraud by shifting $1.7 million in company funds to a personal account in his native Lebanon - funds, the judge said, should have been held in trust to pay for wages and materials at ICI's ongoing projects. The judge also ruled that Eid's actions caused ICI's creditors to suffer combined losses of $3.8 million. Had the events taken place after 2012, when the former Conservative government amended the Criminal Code, Eid would be facing a minimum of two years in prison. But under the pre-2012 regime, Ray has considerable discretion in applying a sentence. Eid's counsel, Richard Addelman, on Friday suggested the penalty should reflect Eid's state of mind at the time. "There is a mental issue here that the court should know about," Addelman told Ray in reference to Eid's claim that he suffers from bipolar disorder, a brain illness that can cause people to exhibit huge swings in mood, and exercise poor judgment. Eid, a Christian, claimed to have secured a housing project contract in the region - one that would see the government of Syria match his funds if he could show a $2-million deposit. Eid said that was why he arranged to transfer ICI's cash. Judge Ray characterized this scheme as "a sham and a fraud." Eid's next appearance is scheduled for June 6, when opposing counsel will argue over whether the number of counts should be reduced.

La GRC a saisi des calepins djihadistes troublants
Journal de Montréal, Hugo Joncas, 2016 05 07
Montréal - **En mai 2015, la GRC arrêtait in extremis huit jeunes soupçonnés de vouloir rejoindre les djihadistes en Syrie, à l'aéroport Pierre-Elliott-Trudeau de Montréal. Parmi eux, une jeune femme transportait deux calepins de notes troublants dans ses bagages**. Ils détaillaient la marche à suivre pour les jeunes, et les raisons qui les ont poussés à partir en zone de guerre. **L'un de ces calepins contient une lettre d'adieu. La jeune femme y explique qu'elle devait quitter le Québec, une terre de «mécréants», pour aller faire la «hijra», l'émigration vers un pays musulman, souligne une déclaration de la GRC qu'a obtenue notre Bureau d'enquête.** Parmi tous les pays où l'islam est majoritaire, elle choisit la partie de la Syrie sous le contrôle de l'État islamique, «puisque c'est là que la charia est appliquée», selon le document déposé à la Cour du Québec. Elle ajoute que «si un morceau des terres musulmanes est touché, il est obligatoire de faire le djihad pour repousser l'ennemi». «L'auteure dit que si elle tombe en martyre, Allah lui demandera qui sont les personnes qu'elle aime pour [qu'elles] puissent entrer au paradis», rapportent aussi les enquêteurs de l'Équipe intégrée de sécurité nationale (EISN), l'escouade antiterroriste que dirige la police fédérale. Dans l'un des calepins se trouve détaillée la procédure à suivre pour passer en Syrie. «Il faut prendre un billet aller-retour. Une fois en Turquie, il faut faire un appel téléphonique. Les passeurs vont informer qu'il faut se rendre à Gaziantep et qu'ils viendront les chercher», résume l'EISN. La ville de Gaziantep est l'un des principaux points de passage des djihadistes entre la Turquie et la Syrie. La jeune femme dit qu'elle voulait «se marier avec un frère», mais que sa famille s'y était opposée.

Canada's Sorely Needed Enhanced National Security Oversight and Review May Be Near
The Algemeiner, Scott Neward, 2016 05 06
Opinion - They are the issues that won't go away. First raised following the 2010 investigation and report into the 1985 Sikh terrorist attack on an Air India flight that killed 329 people, the issues of improving national security operational oversight and after-the-fact review resurfaced during the debate on Canada's C-51 terrorism legislation and the 2015 election. The new Liberal government campaigned on changing national security oversight and review. This was further emphasized in the mandate letter provided to Public **Safety Minister Ralph Goodale i**n November 2015, which included a direction to: Assist the Leader of the Government in the House of Commons in the creation of a statutory committee of Parliamentarians with special access to classified information to review government departments and agencies with national security responsibilities. In practical terms, operational oversight means having an independent entity as part of the ongoing interagency investigative groups. This helps ensure that all of the governmental agencies cooperate, and helps identify and fill in any gaps that can accompany interagency work. Such a process may have identified the intended Air India attack or prevented the departure from Canada to Syria of convicted Toronto 18 terrorist Ali Mohammed Dirie, who escaped despite being under a supervision order. Enhanced oversight can also be achieved through full use of the existing review procedures under the **Canadian Security Intelligence Services (CSIS) Act, whereby the Security Intelligence Review Committee (SIRC) can investigate and review the activities of CSIS in defined scenarios.** It should also be noted that SIRC does appear to have express statutory authority under the CSIS Act in defined circumstances to summon and question representatives from other agencies or Departments beyond CSIS and, with some restriction to seek relevant information from them. Clearly for oversight to be effective, it must include the activities of all relevant agencies. (Note: Scott Newark is a former Alberta Crown Prosecutor who has also served as Executive Officer of the Canadian Police Association, Director of Operations for the Investigative Project on Terrorism and as a Security Policy Advisor to the Governments of Ontario and Canada.)

Trudeau's pick for security adviser shows focus on foreign affairs expertise
Ottawa Citizen, Kathryn May, 2016 05 06
Ottawa - **Prime Minister Justin Trudeau has picked an experienced deputy minister in foreign affairs rather than a senior security bureaucrat as his new national security adviser. Daniel Jean, the deputy minister at Foreign Affairs, takes over the weighty job, effective May 16, filling the vacancy left when his predecessor, Richard Fadden, retired**. The national security adviser wields much influence. He has the prime minister's ear on security and intelligence issues, foreign and defence policy and acts as a conduit for conveying the prime minister and cabinet's directions to the national security community. The departure of Fadden left a gaping hole in the senior ranks that many speculated Trudeau would have to fill with either an experienced senior leader or someone who knows the security portfolio well. There appeared to be few candidates like Fadden, who had an abundance of both. Several senior bureaucrats say Jean's appointment is a deliberate departure from the Conservatives' emphasis on direct security experience and shows how interrelated foreign affairs and security issues have become. They say dealing with thorny security issues around Syria, Libya or Iran would be more effective with a broader global view or "foreign affairs sensibility."**With Jean's appointment, other key bureaucrats in the broader security file include Shugart, Malcolm Brown, deputy minister at Public Safety, and CSIS director Michel Coulombe.**

Bilateral talks may resolve Huawei workers' spy spat
South China Morning Post, Bien Perez, 2016 05 06

Hong Kong - A bilateral dialogue between Beijing and Ottawa could help allay concerns about spying levelled by Canadian authorities on the immigration applications of two Chinese employees of Huawei Technologies, an expert said. "If there are genuine concerns of espionage, and if there is genuine evidence to support these concerns, then governments should communicate," said Paul Haswell, a partner at international law firm Pinsent Masons. The South China Morning Post reported yesterday that Canadian immigration officials have cited the risk of espionage as they prepared to reject the immigration applications of the two Huawei employees, the first such cases to emerge amid a swirl of unsubstantiated security concerns about the Shenzhen-based telecommunications equipment manufacturer. Victor Lum, vice-president at Well Trend United, the two applicants' immigration consultant, said it was the first time Huawei employees are being singled out in such a manner. The procedural fairness letters gave the applicants 30 days to respond. "Huawei cannot substantiate any speculative allegations on any independent person's application to emmigrate to Canada or any other country," a Huawei spokesman told the Post . Haswell played down speculation that other Huawei, Hong Kong-listed ZTE and otherChinese technology companies could now be suspected ofespionage. "Nationals from a range of countries have been denied entry, detained and in some cases charged on allegations of spying by countries around the world," Haswell said. "This issue says more about the current climate regarding security than itdoes about tech companies and their actions." (Full report)

Canada Says Huawei Employees May Be Spies, Rejects Immigration Applications
Epoch Times, Joshua Philipp, 2016 05 06
Ottawa - **The Canadian consulate in Hong Kong allegedly rejected the immigration requests of two Huawei employees, citing "reasonable grounds" that they may be spies.** The reasons for the rejections were outlined in two letters, obtained by the South China Morning Post. A letter from Canada's Hong Kong consulate in March states the immigration application was rejected on ground the individual falls under section 34(1)(f) of the Immigration and Refugee Protection Act. The section refers to people employed by organizations involved in subversion, terrorism, or espionage. The second rejection letter, sent in April, cited the same concerns over an individual's spouse. South China Morning Post did not release names of the alleged spies, but the piece is slanted in their defense. **The Hong Kong-based news outlet has for years been growing closer to the Chinese regime, but came under more direct influence after its purchase by Alibaba CEO Jack Ma in December 2015.** The Canadian consulate in Hong Kong did not immediately respond to an email inquiring about the claims. Huawei is a Chinese telecommunications company which has been accused of spying on behalf of the Chinese Communist Party. The U.S. House Intelligence Committee listed the company in 2012 as a national security threat, and it has since been accused of launching cyberattacks and placing backdoors in its products.

Canada cites spy risk in barring Huawei workers
South China Morning Post, Staff reporter, 2016 05 05
Beijing - Canada is citing the risk of espionage as it prepares to reject the immigration applications of two Chinese employees of mainland telecom giant Huawei, in the first such cases to emerge amid a swirl of unsubstantiated international spying concerns about the firm. In a letter obtained by the South China Morning Post, an immigration officer at Canada's Hong Kong consulate told one applicant in March: "There are reasonable grounds to believe that you are a member of the inadmissible class of persons described in section 34(1)(f) of the Immigration and Refugee Protection Act." That refers to people who belong to an organisation engaged in espionage, government subversion or terrorism. A second applicant was told last month that the same concern existed about their spouse, who was included in the immigration application. "After careful and thorough

consideration ... I am preparing to refuse your application," said both letters, which were provided to the Post bythe applicants' immigration consultants, Beijing-based Well Trend United.This is the first time we've seen Huawei employees singled out in this wayWell Trend vice-president, Victor Lum Well Trend vice-president Victor Lum said the two Huawei staff "definitely and categorically" denied being spies. Their unrelated applications were lodged separately more than two years ago, Lum said, but the so-called "procedural fairness" letters arrived within days of each other on March 18 and March 21. Huawei , the world's third-biggest smartphone maker and a major provider of global telecoms infrastructure, has long been cited by the United States as a Chinese espionage risk, but Well Trend's clients are believed to be the first individuals singled out by any foreign government in such a way. Huawei has repeatedly denied involvement in espionage. But in 2012, a US House intelligence committee concluded Huawei was a threat to national security. The firm has been barred from bidding on US and Australian broadband projects. The Post has agreed not to identify the two employees, who work in low- and mid-ranking non-executive positions. "Their respective job-description narratives could not be more mundane," said Lum, who said hebelieved the immigration applications were lodged withoutHuawei's knowledge. "The only common thread is that they work for Huawei, the largest telecom equipment manufacturer in the world, with over 170,000 employees, and R&D institutes all over the world, including, ironically, Canada. What our clients find particularly galling is that they know of many former Huawei colleagues who have successfully emigrated to Canada." Scott Bradley, Huawei's vice-president of corporate and government affairs in Canada, said he was unaware of the two cases, and had "no idea" of the identity of the employees. "We have a very defined process for [immigration] applications," Bradley said, referring to cases in which Huawei staff are transferred abroad. "There is nothing to indicate this has anything to do with us." A spokeswoman for Canada's immigration department said that it could not comment on individual cases.

More oversight coming for CBSA, says Goodale
The Hill Times, Peter Mazereeuw, 2016 05 04
Canada's border agency "undoubtedly" needs a new oversight mechanism, Public Safety Minister Ralph Goodale told The Hill Times in a wide-ranging interview on his role guiding the government's public safety priorities. Mr. Goodale said April 30 that **his government will create "another tool" for keeping an eye on the Canada Border Services Agency, beyond the promised all-party parliamentary oversight committee for Canada's intelligence and security agencies**. He noted the public outcry over the lack of supervision for CBSA, which became louder following the deaths of two immigration detainees in the agency's custody within one week in March. Mr. Goodale promised to listen to the public during consultations on reforming **Bill C-51,** the so-called anti-terrorism act passed by the previous government that granted the government's security agencies more powers. The minister also said he's considering a long list of people to head a new counter-radicalization co-ordinator's office, set to get off the ground this year. The following interview has been edited for length and style. When do you plan to bring forward the legislation to change and repeal parts of Bill C-51? "I would hope that we would see that later on this year. "There are four really important responses to C-51. The first one, and the flagship commitment that we made: establish a committee of Parliamentarians to provide a new dimension in review and scrutiny that we have not had before. Other countries have had this, all of the Five Eyes countries have a parliamentary mechanism. Most of the democracies in the Western world have that kind of a mechanism. Canada has been the anomaly. So that legislation is being drafted now, and we hope to have that in the public domain by the time Parliament rises for the summer. "The second element is the creation of our new Office of the Community Outreach and Counter-Radicalization Co- ordinator. We will have that operation up and running later on this year. There's some consultation to be done with provinces and local communities and NGOs and so

forth, but that work is getting underway. The Liberal campaign platform included promises to address several issues in its review of C-51, including no-fly lists, the right to take part in lawful protests, requiring warrants for the Communications Security Establishment, and more. Should Canadians expect that the government's legislation is going to address each and every one of those promises? "They are very much a part of our plan, that's what we intend to do. There will be a variety of consultations undertaken; some of them are already underway. We will obviously listen to what we are told in that consultative process. But, based on what I've heard so far, I would expect to hear people commenting on all of the issues I've mentioned here, saying that the changes have to be made, as we indicated in our platform. And there may well be others that they would want to raise.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

Americans still believe in intelligence community
Washington Times, Michael Hayden, 2016 05 10
Column - It's been six months since I've appeared in these pages. That gap hasn't been about a boycott or a contract dispute. Actually, The Washington Times has been rather generous, giving me that time to finish a book, **get it cleared through the intelligence community review process and then endure an aggressive countrywide book tour organized by my publisher, Penguin**. For the most part...the public dialogues were lively, respectful, occasionally challenging and generally fun. I found a good reservoir of support out there for American espionage and its practitioners, a reality that gave me pause the longer the tour continued. Americans are very practical folks. Accustomed to hard choices in their own lives, they are willing to give us in intelligence a lot of slack as we make the hard choices our profession demands. All that was heartening but also a little scary. With the D.C. political rhetoric cut away, it was clear that there is a large body of people out there who instinctively both believe in and depend on the intelligence community. If nothing else, that should underscore the heavy burden on those still in the game to do what they do well -- technically, operationally and legally.

The former CIA head talks about 'firing yourself', hard lessons learnt, and why there's no substitute for US leadership
Financial Times, Edward Luce, 2016 05 08
Interview: Just four years ago, Petraeus was lionised as the Douglas MacArthur of his generation. Even discounting the hype, he stood head and shoulders above other US generals. In the depths of the Iraq war, when the country was undergoing death by a thousand improvised explosive devices, he was dubbed "King David" of Mosul -- a city he cleared and held before it fell back into rebel hands. He was then appointed chief architect of George W Bush's 2007 Iraq surge and, after a stint as head of the Pentagon's Central Command, Barack Obama put him in charge of his own surge in Afghanistan. His reward was to be made head of the **Central Intelligence Agency in 2011. Many thought the CIA was a springboard for Petraeus's own presidential ambitions.** America loves a successful general and his approval ratings were stratospheric. Could anything stand in his way? The answer was yes -- David Petraeus himself. Shortly after Obama's re-election in 2012, Petraeus abruptly resigned from the CIA when it emerged he had shared eight notebooks of classified information with his biographer, Paula Broadwell. They had also had an affair. Rarely has a fall from grace been so brutal. It did not help that Broadwell's fulsome biography was entitled All In: The Education of

General David Petraeus. It was a gift to late-night comics. Following a long investigation, Petraeus, who had pleaded guilty to the unauthorised removal of classified information, was fined $100,000. Some thought him lucky to escape jail. Either way, his downfall was absolute (he remains married to his wife Holly). Almost a year after the dust has settled, I email Petraeus to invite him to do a Lunch with the FT. His acceptance pops up within minutes. What lessons should the US draw from Iraq though? Was today's Isis insurgency not born of post-invasion mistakes? Petraeus agrees with much of the critique that blunders were made in the early US occupation. "There is no question that two decisions early on created enormous problems that continue to this day," he said. The first was de-Ba'athification, which rooted out former Saddam Hussein loyalists from government jobs. The second was demobilisation of the Iraqi military, which threw a lot of angry -- and often armed -- men on the streets. "We had a question on the wall of our operation centre in Mosul," he says. "'Will a policy take more bad guys off the street than put them on?'" and if the answer is no then you should go sit under a tree until the thought goes away. You can't put people out of work and not tell them how they're going to get food on their table. Enormous damage was done that continues to haunt Iraq to this day."

The Former Head of the CIA on Managing the Hunt for Bin Laden
Harvard Business Review, Leon E. Panetta & Jeremy Bash, 2016 05 08
Analysis: May 2 marks the fifth anniversary of the operation that killed the world's most wanted terrorist, Osama Bin Laden. His death was the culmination of a global manhunt that lasted more than a decade and assumed extreme urgency after the September 11, 2001, attacks. The Bin Laden operation was a seminal moment in the campaign to decimate Al Qaeda's leadership. **Three prior CIA directors, and countless senior officials, operations officers, analysts, technical experts, and support teams carried out this campaign, developing important pieces of intelligence along the way**. But when we arrived at Langley in early 2009, there were no solid leads on Bin Laden's whereabouts. The trail had gone cold. The hunt for Bin Laden from 2009-2010 yielded many lessons about managing a large, complex organization that is focused on varied missions under intense pressure. These management lessons, we believe, are relevant far beyond Langley. The CIA is a global institution that undertakes high-risk missions to defend the United States. Its analysis is scrutinized every morning by no less an exacting customer than the president of the United States. Its successes are largely unknown; its failures are legendary. Simply put, CIA has one of the toughest jobs in all of government. The workforce is comprised of career professionals who are deep experts in their craft. They often came to the Intelligence Community early in their careers and stayed. Due to the secret nature of their work, the employees confide mostly in one another, creating skepticism of outsiders and an understandable resistance to doing the life- and-death business of intelligence in a new way. (Note: Leon E. Panetta served as United States Congressman, Budget Director, White House Chief of Staff, CIA Director, and the 23rd Secretary of Defense of the United States. He is the author of "Worthy Fights: A Memoir of Leadership in War and Peace" (Penguin Press, 2014). He chairs the Panetta Institute for Public Policy in Monterey, CA, and is a Senior Counselor at Beacon Global Strategies, a business advisory firm. Jeremy Bash served as Chief of Staff to Leon Panetta at CIA and the U.S. Defense Department. He is a Managing Director of Beacon Global Strategies.)

Twitter Bars Intelligence Agencies From Using Analytics Service
Wall Street Journal, Christopher S. Stewart, Mark Maremont, 2016 05 09
New York - Twitter Inc. cut off U.S. intelligence agencies from access to a service that sifts through the entire output of its social-media postings, the latest example of tension between Silicon Valley and the federal government over terrorism and privacy. The move, which hasn't been publicly announced, was confirmed by a senior U.S. intelligence official and other people familiar with the matter. The service--which sends out alerts of unfolding terror

attacks, political unrest and other potentially important events--isn't directly provided by Twitter, but instead by Dataminr Inc., a private company that mines public Twitter feeds for clients. Twitter owns about a 5% stake in Dataminr, the only company it authorizes both to access its entire real-time stream of public tweets and sell it to clients. Dataminr executives recently told intelligence agencies that Twitter didn't want the company to continue providing the service to them, according to a person familiar with the matter. The senior intelligence official said Twitter appeared to be worried about the "optics" of seeming too close to American intelligence services.

U.S. advisers on the ground in Yemen, Pentagon says
Washington Post, Thomas Gibbons-Neff & Missy Ryan, 2016 05 07
Washington - The Pentagon has placed a small number of U.S. advisers on the ground in Yemen to support Arab forces battling al-Qaeda, military officials said Friday, signaling a new American role in that country's multi-sided civil war. Navy Capt. Jeff Davis, a Pentagon spokesman, said U.S. personnel had been in the country for about two weeks, supporting Yemeni and Emirati forces that are fighting a pitched battle against militants near the southeastern port city of Mukalla. "We view this as short-term," Davis told reporters. Officials said the U.S. military is also providing Emirati forces with medical, intelligence and maritime support, and is flying surveillance and aerial refueling missions. In addition, it has staged ships from the 13th Marine Expeditionary Unit off Yemen's coast. The flotilla includes the USS Boxer, an amphibious assault ship with Marine infantry and aircraft, and two destroyers, the USS Gravely and the USS Gonzalez. Col. Patrick Ryder, a spokesman for U.S. Central Command, said the United States is helping the Arab forces plan operations as part of its "limited" mission in and around Mukalla. "We welcome operations undertaken by Yemeni Forces, with the support of Arab Coalition Forces, to liberate the Yemeni port city of Mukalla from control by al-Qaeda in the Arabian Peninsula (AQAP)," Ryder said in an email.

Washington Accuses Pakistan of Poisoning CIA Representative
Asharq Al-Awsat, Mohammad Ali Salih, 2016 05 09
Washington - On the fifth anniversary of the death of Al Qaeda leader Osama bin Laden, former Central Intelligence Agency (CIA) Leader Mark Kelton believes that Pakistani intelligence businesses poisoned him after the raid on Osama bin Laden. Kelton, who retired from CIA five years ago, said that he began having serious abdomen pains and needed to have stomach surgical operation to clear up the issue. "I'd moderately allow that entire unhappy episode lie," he stated. "I'm very, very pleased with the folk I labored with who did superb issues for his or her U.S. at an overly tricky time. While the real tale is advised, the rustic will probably be very pleased with them." Talking on Kelton's allegations of poisoning, Pakistan Embassy spokesman Nadeem Hotiana brushed aside the tale saying, "Clearly the tale is fictional, now not worth of remark. We reject the insinuations implied within the allegations."

Romanian hacker who claims he breached Clinton server says he spoke with FBI at length
Fox News, Catherine Herridge, 2016 05 07
Washington - The Romanian hacker who says he easily breached Hillary Clinton's personal email server also claimed, in a series of interviews with Fox News, that he spoke with the FBI at length on the plane when extradited from Romania to Virginia last month. "They came after me, a guy from the FBI, from the State Department," 44-year-old Marcel Lehel Lazar, who goes by the moniker "Guccifer," told Fox News during a jailhouse phone interview. He said the conversation was "80 minutes ... recorded," and he took his own notes. A government source confirmed that the hacker had a lot to say on the plane but

provided no other details. Lazar was flown to the U.S. to face separate cyber-crime charges. In addition to the apparent conversation with the FBI on the plane, Fox News has learned a meeting was expected as early as this week at the Alexandria, Va., detention center where he's being held involving Guccifer, the FBI, the U.S. attorney and the defendant's court-appointed lawyer. These officials have not commented on his clams or detention. An intelligence source close to the investigation, speaking with Fox News last month, questioned the timing of Lazar's extradition to the U.S., coming amid the Clinton email probe. As for what was discussed on that plane, Lazar said he told a State Department representative on the plane about "hot" data, some of which was hidden in Google drives, and other data that was too sensitive and deleted. The hacker, who offered no proof for his claims, said cryptically that he could not say more.

Lawmakers, advocates push to reveal extent of surveillance
Associated Press, Staff report, 2016 05 09
Washington - Even though the bulk collection of Americans' telephone records has ended, calls and emails are still being swept up by U.S. surveillance work targeting foreigners. Congress is making a renewed push to find out how many. Six Republicans and eight Democrats on the House Judiciary Committee have asked the nation's top intelligence official for the number of Americans' emails and phone calls collected under programs authorized by Section 702 of the Foreign Intelligence Surveillance Act. The programs target foreigners, but domestic communications sometimes are vacuumed up as well. They were first revealed to the public by **Edward Snowden**, who leaked files from the **National Security Agency.** "Surely the American public is entitled to some idea of how many of our communications are swept up by these programs," the committee members wrote in their April 22 letter to Director of National Intelligence James Clapper.

FBI Told Cops to Recreate Evidence From Secret Cell-Phone Trackers
The Intercept, Jenna McLaughlin, 2016 05 05
Washington - A recently disclosed document shows the FBI telling a local police department that the bureau's covert cell-phone tracking equipment is so secret that any evidence acquired through its use needs to be recreated in some other way before being introduced at trial. "Information obtained through the use of the equipment is FOR LEAD PURPOSES ONLY," FBI special agent James E. Finch wrote to Chief Bill Citty of the Oklahoma City Police Department. The official notice, dated September 2014, said such information "may not be used as primary evidence in any affidavits, hearings or trials. This equipment provides general location information about a cellular device, and your agency understands it is required to use additional and independent investigative means and methods, such as historical cellular analysis, that would be admissible at trial to corroborate information concerning the location of the target obtained through the use of this equipment." The document, obtained by nonprofit investigative journalism outlet Oklahoma Watch, pertains to the use of cell site simulators, or Stingrays -- surveillance technology that mimics a cellphone tower to trick cellphones into transmitting location data and other information, sometimes even the contents of calls.

After presiding over bin Laden raid, CIA chief in Pakistan came home convinced he was poisoned by ISI
Washington Post, Greg Miller, 2016 05 06
Washington - **Two months after Osama bin Laden was killed, the CIA's top operative in Pakistan was pulled out of the country in an abrupt move vaguely attributed to health concerns and his strained relationship with Islamabad**. In reality, the CIA station chief was so violently ill that he was often doubled over in pain, current and former U.S. officials said.

Trips out of the country for treatment proved futile. And the cause of his ailment was so mysterious, the officials said, that both he and the agency began to suspect that he had been poisoned. Mark Kelton retired from the CIA and his health has recovered after he had abdominal surgery. But agency officials continue to think that it is plausible -- if not provable -- that Kelton's sudden illness was somehow orchestrated by Pakistan's Inter- Services Intelligence agency, known as the ISI. Kelton, 59, declined multiple requests for an interview, but in a brief exchange by phone he said that the cause of his illness "was never clarified," and added that he was not the first to suspect that he had been poisoned. "The genesis for the thoughts about that didn't originate with me," he said. In the conversation, Kelton declined to answer questions about his illness or tenure in Pakistan. "I'd rather let that whole sad episode lie," he said. "I'm very, very proud of the people I worked with who did amazing things for their country at a very difficult time. When the true story is told, the country will be very proud of them." The CIA declined to comment. Pakistan dismissed the allegations against the ISI. "Obviously the story is fictional, not worthy of comment," said Pakistan Embassy spokesman Nadeem Hotiana. "We reject the insinuations implied in the allegations."

Spies Worry Candidate Trump Will Spill Secrets
The Daily Beast, Shane Harris, 2016 05 05
Washington **- After Donald Trump is formally chosen as the Republican presidential nominee, he'll be able to receive classified U.S. intelligence briefings, which could include some of the same sensitive information that President Obama is given in the Oval Office**. And that prospect has some spies sweating. Trump, who can't seem to dam his stream of consciousness on Twitter, and who has lately taken to spreading rumors and conspiracy theories on national television, has never been privy to national secrets. Nor has he ever demonstrated that he's capable of keeping them. "My concern with Trump will be that he inadvertently leaks, because as he speaks extemporaneously, he'll pull something out of his hat that he heard in a briefing and say it," said a former senior U.S. intelligence official who has participated in the process of briefing presidential candidates. "It's not an unreasonable concern that he'll talk publicly about what's supposed to stay in that room," said another former senior intelligence official. A currently serving U.S. official echoed some of those anxieties and wondered whether Trump would respect the discretion of the briefing and not use it to his advantage on the campaign trail.

NSA plan to trash employee complaint files raises concerns for some
Nextgov.com (US), Aliya Sternstein, 2016 05 05
Washington - **The National Security Agency plans to immediately discard records containing preliminary workplace complaints raised by employees. The files set to be destroyed are created by the NSA Ombudsman program, a low-profile office that resolves conflicts between personnel.** It is not the ombudsman's job to handle reported abuses of power, rather inspectors general and diversity offices deal with those issues. However, amid a legal battle about the potential improper disposal of whistleblower evidence, there are concerns that informal information reported by informants or victims of retaliation could be thrown out under the ombudsman policy. "Destroy immediately after case is closed," state new recordkeeping instructions for working case files produced by the NSA ombudsman.

Measuring change at the CIA
Foreign Policy, Stephen Slick, 2016 05 04
Essay - **This time next year, a new president will be reviewing recommendations from a transition team, and likely also the views of a new director or director-designate, on the state of affairs at the Central Intelligence Agency** -- including the impact of a major

reorganization initiated by the agency's current director, John Brennan. The new national security team will not lack for advice on this topic from serving officers, CIA alumni, congressional overseers, and the burgeoning intelligence commentariat. This advice will be well-intentioned in the main, but not universally well-informed. There is considerable skepticism in these communities that the changes underway will ultimately produce a more effective CIA. Such skepticism is rooted in a strong (and well-exercised) aversion to change at Langley, nostalgia for tradition-rich institutions that were unceremoniously dismembered, and sincere concern that some of the changes may actually hinder, rather than enhance, the agency's ability to deliver "timely, accurate, and insightful" intelligence to policymakers. **The CIA is an essential institution positioned at the heart of an intelligence community (IC) charged with anticipating, understanding, and often neutralizing threats to our national security.** It would be a mistake to reverse or suspend any of the reforms now underway at Langley without the benefit of a rigorous and objective assessment of how the new priorities, structures, and work processes are actually impacting the Agency's core missions: collecting intelligence from human sources (HUMINT), evaluating information from all sources, and shaping conditions abroad through covert actions. The objective evaluation of the performance of any intelligence organization is fraught, but such an exercise should be completed before the CIA workforce is subjected to the uncertainty and disruption of another makeover. Note: This essay was reviewed and approved by the CIA's Publication Review Board. The PRB requested removal of text that described a counterterrorism program previously acknowledged by the president and recent CIA directors.

How to evade the NSA: OpSec guide for journalists also used by terrorists
The Register (UK), Darren Pauli, 2016 05 04
London - Privacy guides meant for journalists are being re- purposed by terrorist groups, Trend Micro researchers say. The guides are designed to help hacks avoid surveillance by nation-states and well- resourced adversaries focusing on encryption, operational security, recommended and untrusted platforms. It is one finding of dozens from the report Dark Motives Online, which analyses the similarities and differences between terrorist and criminal communications. "... terrorists [are] adopting and distributing anonymising (sic) guides originally meant for activists and journalists ... evidently to teach new or uninitiated members ways to avoid being spied on," the researchers say. "Some of these guides even mention the National Security Agency and how to avoid surveillance." Trend Micro did not name the studied terror group but said it was listed as a designated group by at least seven nations. That limits choices to less than a dozen groups including Hezbollah; al-Qaeda; Islamic State; Al-Nusra Front; and the Kurdistan Workers' Party.

'Mirror Imaging' and America's Dangerous Middle East Illusions
Wall Street Journal, Henry A Crumpton, Allison Melia, 2016 05 04
Op-ed - Intelligence officers are taught to avoid "mirror imaging." That is, assuming your adversary shares your analytic reference points and thinks the way you do. Americans tend to ascribe to other countries the best of our own values: tolerance, equal opportunity, rule of law, freedoms of speech and religion, and separation of church and state. But many countries do not share these values. Two of them are among our most problematic foreign relationships: Saudi Arabia and Iran. These states, one friend and the other foe, promote ideologies that compete with America's vision of liberal institutions, secular democracy and world order. Yet instead of confronting their illiberal, repressive, and often reprehensible narratives, we attempt to reconcile their views with our own, giving them a free pass based on our own tolerance of religious differences. The problem is that in these states religion does not exist in a vacuum. On the contrary, their religion is their political ideology -- and a critical element of their foreign policy. Although Saudi Arabia, sometimes with U.S. support, has launched effective

counterterrorism operations against al Qaeda and ISIS, these efforts are shortchanged if the Saudi kingdom does not also address the underlying ideology that inspires ISIS attacks around the globe. And Riyadh, as custodian of Islam's holiest sites, is uniquely positioned to act. Americans' natural aversion to government involvement in religious matters should not become an excuse for U.S. failure to tackle this ideological challenge. The U.S. should redouble its efforts to counter Iranian terrorism -- with deadly force if necessary. Meanwhile, U.S. economic power continues to be a valuable tool. Even after the removal of some major sanctions as part of the nuclear agreement, Tehran has sought additional access to U.S. dollars to conduct international transactions and has called for the remaining sanctions to be lifted. Yet that should only happen if Iran ceases its violent, destabilizing behavior, which is unlikely under the current regime. Religious tolerance is one of our country's highest ideals. Americans are fortunate to live in a society that respects all religions. Yet we should never allow this inclination to skew our analyses of other nations' behavior. It is important that we see these states not as an image in the mirror, but as actors willing to use religion- based ideology in ways that undermine our interests. Note: Mr. Crumpton, a 24-year veteran of the CIA and former U.S. coordinator of counterterrorism, is the CEO of Crumpton Group LLC, where Ms. Melia, a former CIA analyst and director for Pakistan and Afghanistan on the White House National Security Council, is director of analysis.

CIA: Bin Laden's Takedown is of Historical Value
Asharq Al-Awsat, Mohammed Ali Saleh, 2016 05 04
Washington - The U.S. Central Intelligence Agency (CIA) spokesman Ryan Trapani, in the past few days, defended the agency's tweeted details posted in commemoration of five years marking the takedown of al-Qaeda founder Osama bin Laden. Speaking to ABC- a U.S. based television broadcasting company-, Trapani said that bin Laden's takedown stands to be a historical masterpiece of planning and execution going to the agency's portfolio. "On the fifth anniversary, it is appropriate to remember the day and honor all those who had a hand in this achievement," Trapani told ABC. Out of nowhere, a series of CIA tweets, on bin Laden's takedown flooded the agency's page. The first tweet mentioned that in tribute of the fifth year passing on the raid which killed bin Laden in Abbottabad, Pakistan, the CIA would post details on the event "as if it were happening today." Throughout the day, the agency tweeted non-stop.

DHS sweetens cyber workforce recruiting with new bonuses
Federal News Radio, Jared Serbu, 2016 05 04
Washington - In the intense competition to hire qualified cybersecurity professionals, the government's advantage has always been its appeal to a sense of mission, not necessarily large salaries. On the other hand, money helps too. **So the Department of Homeland Security is about to roll out a new series of incentive payments to lure cyber experts from the private sector and keep them in the civil service.** DHS began piloting the bonuses within its National Protection and Programs Directorate (NPPD) six months ago and is about to expand them across the rest of its headquarters elements. They provide an additional 20 to 25 percent on top of an employee's annual pay, depending on the certifications they've earned and the position they occupy, said Paul Beckman, the chief information security officer for DHS' headquarters.

NSA and CIA Double Their Warrantless Searches on Americans in Two Years
The Intercept, Jenna McLaughlin, 2016 05 03
Washington - **From 2013 to 2015, the NSA and CIA doubled the number of warrantless searches they conducted for Americans' data in a massive NSA database ostensibly collected for foreign intelligence purposes, according to a new intelligence community**

transparency report. The estimated number of search terms "concerning a known U.S. person" to get contents of communications within what is known as the 702 database was 4,672--more than double the 2013 figure. And that doesn't even include the number of FBI searches on that database. A recently released Foreign Intelligence Surveillance Court ruling confirmed that the FBI is allowed to run any number of searches it wants on that database, not only for national security probes but also to hunt for evidence of traditional crimes. No estimates have ever been released of how often that happens. Under Section 702 of the Foreign Intelligence Surveillance Act, the NSA collects hundreds of millions of digital communications at rest and in transit from the major internet backbones running in and out of the U.S., as well as from Google, Facebook, YouTube, and other companies, involving "targets" overseas. The Office of the Director of National Intelligence has said the practice of searching the database for American communications is not "unlawful" because the content is collected legitimately in the first place--and because there are protections against sharing Americans' identities unless it's absolutely necessary.

Obama Plan to Cut Refugee Screening Time Raises Concerns About Terrorism
Washington Free Beacon, Adam Kredo, 2016 05 04
Washington - An Obama administration plan to resettle a greater number of foreign refugees in the United States by expediting the screening process is drawing concern from Capitol Hill, where lawmakers are warning that the administration is not capable of properly screening these individuals for ties to terrorism. The Obama administration has committed to bring at least 10,000 Syrian refugees onto American soil in fiscal year 2016 by accelerating security screening procedures from 18-24 months to around three months, according to sources who spoke to the Washington Free Beacon. Obama administration officials told the Free Beacon that they remain committed to the plan, despite warnings from the FBI and other law enforcement officials who say the federal government is not equipped to properly vet these individuals within that timeframe. The administration is committed to moving forward this year with a plan to resettle 10,000 Syrian refugees and 85,000 refugees overall, officials said.

Top U.S. intel official: ISIS can stage Europe-style attacks in U.S.
CNN.com, Nicole Gaouette, 2016 05 04
Washington - ISIS has the capability to stage a Paris-style attack in the U.S. using local cells to strike in multiple locations and inflict dozens of casualties, according to the Obama administration's top U.S. intelligence official. "They do have that capacity," Director of National Intelligence James Clapper told CNN's Peter Bergen in an exclusive interviews on "AC 360" on terrorism, Osama bin Laden and al Qaeda's most virulent offshoot -- ISIS. "That's something we worry about a lot in the United States, that they could conjure up a raid like they did in Paris or Brussels," where March attacks on a train and at an airport left 32 dead and 300 people injured, Clapper said. The November Paris attacks killed at least 130. However, President Barack Obama and some of his other security advisors spoke of the threat in less stark terms and emphasized efforts to protect the U.S. Obama told Bergen that "we, here in the United States, face less of a threat than Europe" from ISIS. National Security Adviser Susan Rice said "whether or not" ISIS can attack the U.S., the administration would do "our utmost to try to prevent it." Still, Obama said, "The Paris-style attack, the Brussels style attack is the challenge that we're going to continue to face."

Foreign Intelligence Services Targeted 2008 Campaign, Officials Were Warned
The Intecept, Jenna McLaughlin, 2016 05 06
Washington - **The Intelligence Community evidently gave some incoming members of the**

Obama administration a star-spangled welcome briefing -- complete with a stern warning. In a newly disclosed document titled "Unlocking the Secrets: How to Use The Intelligence Community," intelligence officials told incoming officials that foreign intelligence services had been extensively spying on the 2008 political campaigns. "Foreign intelligence services have been tracking this election cycle like no other," the authors from the Office of the Director of National Intelligence wrote. On the campaign trail, the ODNI authors wrote, foreign spooks met with campaign staff and other sources, hacked into campaign data, and engaged in "perception management" more aggressive than traditional lobbying--though the lack of specifics make it's unclear what any of that really entails.

He's the FBI 's inside man; The agency's new No. 2 makes decisions , not headlines , as he prefers it
Los Angeles Times, Del Quentin Wilber, 2016 05 06
Washington - From his perch on the seventh floor of FBI headquarters, Andrew McCabe is one of the most powerful figures in U.S. law enforcement, but most Americans would be hard-pressed to pick him out of a lineup. Responsible for overseeing investigations of terrorists, spies and corrupt officials, as well as the sensitive inquiry into Hillary Clinton's use of a private email server, the longtime FBI agent toils mostly behind the scenes, and he likes it that way. "My focus is on the inside [of the FBI] and all the work we do that is not talked about in the newspaper, on CNN, on the Hill," McCabe, 48, said in his first interview since he was named FBI Director James B. Comey's second-in-command in January. Comey is "totally focused" on high-profile issues like the recent legal fight with Apple over an encrypted iPhone used by one of the San Bernardino killers and questions from members of Congress, McCabe said. "My focus is on the stuff we have done for 100 years and do every day that people never hear about," he added.

Navy 'Spy' Edward Lin Spilled No Secrets To Taiwan
The Daily Beast, Nancy A. Youssef, Shane Harris, 2016 05 06
Washington - A U.S. Navy sailor charged with espionage didn't provide military secrets to a foreign government, but rather to an FBI informant who was posing as a Taiwanese official, military officials revealed Thursday. The latest twist in the case against Lt. Cmdr. Edward Lin, 39, came as military officials allowed reporters to listen to a recording from a military pretrial hearing held on April 8. There, prosecutors alleged that Lin was the target of a sting operation that led to his arrest and two-day interrogation at the Honolulu International Airport last September. Prosecutors said that during questioning, Lin confessed to being a spy. Lin's job, working in and around military reconnaissance aircraft, gave him access to information about sensitive equipment that the U.S. uses to spy on its adversaries. Lin's attorney vigorously refuted the charges and said that his client had been denied his right to speak with a lawyer at the time he was arrested and questioned. The Pentagon Thursday played an 80-minute section from the pretrial hearing, known as an Article 32. But they left out at least a half hour that officials said was classified. The recording sheds new light on Lin's case, but it also raises several unanswered questions. And prosecutors offered no explanation of how Lin, who once spoke in uniform about fulfilling his dreams of becoming a U.S. citizen, had turned from a model sailor to a spy.

NSA reveals hundreds of bugs a year, says former official
San Francisco Chronicle, Sean Sposito, 2016 05 06
San Francisco - A retired technical director for the National Security Agency, Richard George, says that the NSA regularly disclosed more than a thousand software and hardware bugs a year to companies. That may make the agency a far more significant player

in patching the fraying digital fabric that secures our lives than has previously been understood. George's comments come as the technology industry and the government grapple with the question of how intelligence agencies and law enforcement disclose bugs they discover. From the 1990s until his retirement from the NSA in 2011, George said, he was responsible for disclosing serious bugs to private companies. "I imagine everybody had a similar process to the one that we had at NSA," he said. Regulations required a review board, he explained: "Anybody who finds a vulnerability in a product has to report it to that board, so that we can figure out how we are going to address it."

NSA Won't Say How Many Spies Have Child Porn
The Daily Beast, Shane Harris, 2016 05 06
Washington - Two senior U.S. intelligence officials said recently that defense and intelligence employees have an "unbelievable" amount of child pornography on their work computers and devices, and that child porn has been found on the systems of the National Security Agency, the country's biggest intelligence organization. But the NSA, which is responsible for keeping tabs on its own computers as well as military and intelligence agency networks, cannot say just how many time employees have been found to posesses or share child pornogrpany, **or how many times such cases have been referred to law enforcement for investigation and potential criminal prosecution**. An agency spokesperson was unable to provide The Daily Beast with statistics to elaborate on comments by Kemp Ensor, the NSA's director of security, who said at a public conference in Virginia on April 28 that he had seen child porn on agency systems. Despite the fact that NSA employees know they work inside the most powerful surveillance organization on the planet, it doesn't stop some from engaging in criminal behavior. "What people do [at work] is amazing," Ensor said. Privately, current and former intelligence officials told The Daily Beast that the NSA does know when employees are downloading, storing, or sharing graphic and illegal images. Downloading, purchasing, and disseminating child pornography is a crime. But NSA is probably not keeping track of the number of times child porn has been found, the current and former officials said--at least not in any form that it's willing to release publicly.

Once Donald Trump Is Nominee, He Is Likely to Get Intelligence Briefing
New York Times, Charlie Savage, 2016 05 06
Washington - The White House on Thursday said that it expected intelligence officials to provide a classified briefing to Donald J. Trump after the Republican Party formally nominates him for president at its convention in July, a tradition for major party nominees dating back to 1952. Asked whether President Obama was concerned about Mr. Trump's receiving classified information in light of the presumptive Republican nominee's reputation for making unfiltered comments, Josh Earnest, the White House press secretary, said the president would leave it to intelligence professionals to decide what to share with him. Mr. Trump said in an interview with The Washington Post this week that he was eager to start receiving regular classified intelligence briefings. But that overstates the information Mr. Trump will receive. After the party conventions and before the election, the major-party nominees for president and vice president receive only a one-time intelligence briefing about the state of the world. **Michael J. Morell, a former deputy C.I.A. director, who regularly briefed Mr. Obama before retiring in 2013, said the postconvention nominee briefing would last several hours**. The idea is to "get them to understand that they have now stepped into a bigger world" in which foreign allies, adversaries, and neutral parties are paying close attention to whatever they say, and that their words may have broad consequences, he said.

Trump will soon be getting briefings from U.S. spy agencies. It might not go well.
Washington Post, Greg Miller, 2016 05 06
Washington - Presumptive Republican presidential nominee Donald Trump told my colleague Robert Costa that he is eager to start meeting with U.S. intelligence officials for classified briefings on the nation's secrets. The feeling may not be mutual. The outlandish GOP candidate is not known for discretion or nuanced understanding of global security issues, let alone awareness of the widespread revulsion among U.S. intelligence officials over some of Trump's positions -- including his expressed admiration for Russian President Vladimir Putin and pledge to resume torturing terrorism suspects. Where should the U.S. intelligence community's first PowerPoint presentation for Trump begin? "It beggars the imagination," said former CIA director Michael V. Hayden, who was among those who briefed President Obama after the 2008 election. "Given that [Trump's] public persona seems to reflect a lack of understanding or care about global issues, how do you arrange these presentations to learn what are the true depths of his understanding?" "This is a person who doesn't seem to have much of a filter," said Aki Peritz, a former CIA analyst who contributed to the President's Daily Brief (PDB) -- the digest delivered each morning to the Oval Office. "The scary part is that nobody knows who he really is. Is he this blowhard demagogue we see on TV or is he really a sophisticated consumer of information that will keep this information close to his chest?"

Where the FBI's top cybercrime agents go after quitting the force
The Daily Dot, Patrick Howell O'Neill, 2016 05 05
Chicago - The FBI team that brought down Silk Road has a new home. After headline-grabbing investigations, arrests, and prosecutions on some of America's highest-profile cybercriminals, five of U.S. law enforcement's most prized cybercrime aces have all left government service for greener pastures--a titan consulting firm called Berkeley Research Group (BRG). BRG's newly hired gang of five includes former federal prosecutor Thomas Brown, as well as former FBI agents Christopher Tarbell, Thomas Kiernan, and Ilhwan Yum--names that punctuated many of the biggest cybercrime stories of the last decade. That group's 2013 bust of Silk Road, the first major Dark Net market where anyone could purchase drugs and other illicit goods and services, is famous enough. That story will be transformed into a 21st Century Fox movie soon--a fact BRG happily boasted about in its February press release announcing new hires.

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

Chilcot report on Iraq war to be published on 6 July
The Guardian (London), Ewen MacAskill, 2016 05 09
London - The long-awaited Chilcot inquiry into the invasion of Iraq is to be published on Wednesday 6 July, two weeks after the EU referendum. There had been concern that the report might be published in the weeks before the vote, distracting attention from the campaign. **Sir John Chilcot, head of the inquiry, wrote to the prime minister to say that the checking process by the intelligence services to ensure that nothing which might inadvertently endanger national security, such as the name of an agent, had been completed. Intelligence staff spent two weeks vetting the report.** The Chilcot inquiry said in spite of the vetting there had been no redactions in the text. Criticism is expected of intelligence chiefs for providing inaccurate information about Iraq's then president Saddam Hussein having weapons of mass destruction and of military chiefs' failure to stand up to the prime minister.

Don't vote for Brexit, US defence chiefs warn
London Times, Francis Elliott, Matt Chorley, 2016 05 10
London - Britain must not bank on its "special relationship" with the United States to compensate for losing global influence by leaving the EU, foreign and defence chiefs from every White House administration over the past 40 years have warned. In a letter to The Times, 13 former US secretaries of state and defence and national security advisers say that the country's "place and influence in the world would be diminished and Europe would be dangerously weakened" after a vote to leave in next month's referendum. Washington's intervention will inflame the argument over whether Britain would be safer or more vulnerable outside the EU, after David Cameron said yesterday that Brexit could shatter world peace. "In our globalised environment it is critical to have size and weight in order to be heard," **say the group of 13, which includes Ronald Reagan's secretary of state, George Shultz; the former CIA chief and defence secretary Leon Panetta; and Madeleine Albright, the first woman secretary of state. "**The special relationship between our countries would not compensate for the loss of influence and clout that the UK would suffer if it was no longer part of the EU, a union of 28 nations with 500 million inhabitants, which is the largest economic bloc in the world," they add. "This would be true in foreign policy, defence policy and international trade matters, and other areas where the EU is indeed a significant voice."

Ex MI5 chief accused of changing his mind on Brexit
Daily Mail (UK), James Slack, 2016 05 09
London - A former MI5 chief was dragged into a Brexit row last night amid claims he had changed his mind over whether Britain was safer inside the EU. No, 10 hailed an intervention from Jonathan Evans, along with ex-MI6 chief Sir John Sawers, in which the two men said in an article that leaving would hamper 'our ability to protect ourselves' from terrorists. The pair added that the UK benefited from sharing information with fellow EU countries and a vote for Out on June 23 could trigger instability on the continent. But Tory MP Julian Lewis, a former member of Westminster's Intelligence and Security Committee, said he had met Lord Evans in Westminster's Portcullis House less than a month ago - and been given a different story. Dr Lewis, who has known Lord Evans for many years and is now chairman of the Commons defence committee, questioned whether the Government machine was guilty of manipulation. He added: 'I was quite impressed by the fact that although he told me he was in favour of remaining in the EU, it would make no difference to our security. I am very surprised and rather disappointed to see this article has appeared. I find it rather difficult to believe he has changed his mind in such a short period of time.' However, in a statement last night, Lord Evans denied his views had changed since his meeting with Dr Lewis.

Now Experts Say Don't Change Your Password
Mail on Sunday, Martin Beckford, 2016 05 08
London **- It is one of the banes of modern life - you finally come up with a memorable yet secure password for your office computer, only to be told just a few months later that it has expired and you have to find a new one**. But now Britain's security services themselves have decreed that workers may be safer from hackers if they do not have to keep changing passwords. In a new briefing to Whitehall, power stations, banks and the public sector, cyber experts at **CESG** - the information security arm of intelligence agency **GCHQ** - concluded: 'It's one of those counter-intuitive security scenarios; the more often users are forced to change passwords, the greater the overall vulnerability to attack.' The advice continues: 'Most password policies insist that we have to keep changing them. And when forced to change one, the chances are that the new password will be similar to the old one. Attackers can exploit this... New passwords are also more likely to be forgotten, and this carries the productivity costs of

users being locked out... CESG now recommends organisations do not force regular password expiry.'

Row as ex-intelligence chiefs say EU membership protects UK security
BBC News, Staff Writer, 2016 05 08
London - **Leaving the EU would make the UK "less safe", a former intelligence services chief has warned. Former MI6 boss Sir John Sawers told the BBC's Andrew Marr that the UK would be shut out of decisions on the "crucial" issue of data sharing.** But Justice Secretary Michael Gove, who backs the campaign for the UK to leave the EU, said Sir John was "flat wrong". He told the programme many security experts did not think that "Brexit" would harm Britain. 'Wider stability' Security is the latest battleground in the run-up to the referendum on the UK's EU membership on 23 June. Sir John and ex-MI5 chief Lord Evans stepped into the debate with an article in the Sunday Times. Sir John told the BBC that he and Lord Evans, who led MI5 until three years ago, had waited to intervene until after Thursday's elections. He said: "The reason we would be less safe [if the UK voted to leave], is that we would be unable to take part in the decisions that frame the sharing of data, which is a crucial part of counter-terrorism and counter-cyber work that we do these days, and we would lose the abilities of thing like the European Arrest Warrant."

SAS snatch IS chiefs in secret Iraq raids
Daily Mail (UK), Chris Hughes, 2016 05 07
London - **British special forces are leading a secret Coalition mission to snatch Islamic State commanders before a major assault on Mosul in Iraq**. Since the operation began three weeks ago, three mid-ranking IS warlords have been seized in attacks headed by the SAS. Prisoners are being handed over to Kurdish and Iraqi security officials for interrogation. It is part of a plan to unnerve the enemy before an assault on the stricken city in the north. A senior source said: "There are a wide range of activities taking place around Mosul which allows our commanders to shape the dispositions of enemy forces prior to any engagement. "Seizing enemy commanders has always been a key driver in changing the way your opponent thinks, it will unsettle them and may force them to make mistakes. "From our point of view killing the enemy is not always the answer. "If we can get a commander to change sides, as we did in Afghanistan, this can have major influence on people inside Mosul and save lives." A source said: "The SAS are at the heart of this but it is important credit goes to the Iraqis to bolster their standing. " Sources say British security officials are barred from handling or taking part in any interrogations. **However, the Mirror understands officers from MI6 and MI5 are in the area to receive any new information.**

Spy chiefs say quitting EU is security risk
Sunday Times (UK), Richard Kerbaj, Tim Shipman, 2016 05 08
London - The former heads of MI5 and MI6 have warned that leaving the EU could undermine "our ability to protect ourselves" from terrorists. Baron Evans of Weardale, the former **director-general of MI5, and Sir John Sawers, the former head of MI6**, say Brexit could also lead to "**instability on the Continent**", compounding the current "economic difficulties, the migration crisis and a resurgent Russia". In an article for The Sunday Times, the former spy chiefs warn that a vote to leave could damage intelligence sharing because the EU would restrict surveillance powers if the UK were not in the union. They write: "Intelligence work today relies on the lawful and accountable use of large data-sets to reveal the associations and activities of terrorists and cyber-attackers. The terms on which we exchange data with other European countries are set by agreement within the EU. As an EU member, we shape the debate, we push for what we think is the right balance between security and privacy and we

benefit from the data that flows as a result." They conclude: "An agreement reached without us would probably be too restrictive for our needs . . . this could undermine our ability to protect ourselves." Sawers said that he and Evans had not co- ordinated their intervention with Downing Street: "We're not doing it at anybody's behest. We are completely politically neutral."

Downing Street accused of 'manipulating' spy chiefs after they warn against Brexit
The Telegraph (UK), Steven Swinford, 2016 05 08
London - David Cameron has been accused of "manipulating" the former head of MI5 into warning that Britain's national security would be put at risk by a Brexit. Lord Evans, a former director of MI5 and Sir John Sawers, a former head of MI6, said in a joint article that a Brexit would hamper 'our ability to protect ourselves from terrorists'. However Julian Lewis, the Conservative head of the defence select committee, said that Lord Evans had told him privately that leaving the EU would "make no difference" to national security. Speaking in a personal capacity he said: "I had a conversation very recently with one of the two and I was quite impressed by the fact that although he told me he was in favour of remaining in the EU, it would make no difference to our security. "I am very surprised and rather disappointed to see this article has appeared. I find it rather difficult to believe he has changed his mind in such a short period of time. I can only wonder if there's some sort of manipulation going on here."

Return to Table of Contents/ Retour à la table des matières

Australia/ Australie

Two Australians killed in US air strikes, including terrorist recruiter Neil Prakash
ABC (Australia), Andrew Greene, 2016 05 05
Canberra - The Islamic State group's most senior Australian recruiter Neil Prakash is killed in a US air strike on a terrorist stronghold in Iraq, while a separate strike in Syria kills the sister of the radicalised teen who shot dead police accountant Curtis Cheng in Sydney last year. Australia's most wanted terrorist Neil Prakash has been killed in a US air strike on the Islamic State (IS) stronghold of Mosul in northern Iraq. The ABC understands Prakash was among a gathering of IS operatives targeted on April 29, with the United States recently confirming his death and advising Australia. American authorities have also advised the Federal Government that Australian woman Shadi Jabar Khalil Mohammad was killed in a similar air strike near the Syrian city of Al Bab a fortnight ago. Mohammad was the sister of Farhad Mohammad, the teenager who . Prakash's death is considered "significant" by Australian and American authorities because of his highly prominent and influential role as a senior IS recruiter. He was believed to have left Melbourne for Syria in 2013, where he changed his name to Abu Khaled al-Cambodi, and was put on a US kill list.Attorney-General George Brandis and Defence Minister Marise Payne said in a statement that the pair were both active recruiters of foreign fighters on behalf of IS, and had been inspiring attacks against Western interests. **"The latest advice I have from ASIO as of this morning is they assess there are about 110 Australians engaged with ISIL in the Middle East as foreign fighters or otherwise engaged within the ISIL network," Senator Brandis told AM.**

Neil Prakash's death a significant blow to terror recruitment in Australia, Government says
ABC (Australia), Lexi Metherell, 2016 05 05
Canberra - The death of Neil Prakash -- Australia's most wanted terrorist -- is a significant blow to Islamic State's recruitment of Australians, the Federal Government says. The

Melbourne extremist had been a key player in inspiring violent terrorism in Australia. He was killed in a US airstrike in Iraq on Friday night. Rumours of Prakash's death first began in January, but it is now known that he was still alive up until last Friday, when the United States Government said it killed him in an American airstrike. Attorney-General George Brandis told Sky News that Australia cooperated with the US in relation to the identification and location of Prakash. Senator Brandis said the death was significant in the fight against terrorism on home soil and in frustrating Islamic State recruitment. "He was actively involved both in recruitment and in encouraging domestic terrorism in Australia," Mr Brandis said. "He was the principal Australian reaching back from the Middle East into Australia and in particular into terrorist networks in both Melbourne and Sydney." The US also confirmed it had killed the sister of Farhad Jabar, who killed police employee . Shadi Jabar Khalil Mohammad and her husband, who were IS members, died in an airstrike in al Bab, near Aleppo in Syria. Prakash was reportedly involved in foiled terror plots on last year's and this year's Anzac Day commemorations. **Senator Brandis said ASIO advised him that there were still 110 Australian foreign fighters in Iraq or Syria.** Mr West said it is not clear who would fill the void left by Prakash.

ASIO warns of cyber terror risks
The Australian, Cameron Stewart, 2016 05 04
Sydney - ASIO has warned Australia is losing the battle against cyber espionage as spy agencies yesterday received a fresh funding boost to combat both the growing cyber threat and the ongoing spectre of Islamic terrorism. The government will also step up its investment in countering violent extremism with an extra $5 million to set up community support programs to encourage early tip-offs about would-be Islamic extremists. **ASIO, which will receive an extra $24m in funding in 2016-17 on top of a series of major funding increases in recent years, has delivered a stark warning in the budget papers that the scope of espionage and cyber attacks is outstripping the ability to combat them**. "Clandestine foreign actors are causing harm to Australia through espionage, interference and cyber activity that seeks to undermine our political and economic sovereignty," ASIO said. "The gap is likely widening between the scale and scope of harm experienced to Australia's sovereignty, government systems, and commercial and intellectual property, and the ability of ASIO and partner agencies to successfully mitigate that harm." ASIO also warned the terrorism threat in Australia would continue to remain high and that it could provide no guarantee in the current climate that there would not be a terrorist attack here. "The counter-terrorism challenge Australia faces is underscored by events; since the national terrorism threat level was raised on 12 September, 2014, there have been three attacks and eight disruption operations in relation to imminent attack planning in Australia." The budget gives another funding increase to Australia's overseas spy agency ASIS to help in the struggle against Islamic State.

Big guns wheeled out to fight cyber crime
Adelaide Advertiser, Staff reporter, 2016 05 04
Adelaide - Nearly $200 million has been allocated in the Federal Budget to deliver a comprehensive cyber security strategy for Australia. The announcement, which was "vital to our economic and national security", builds on the $38 million announced in the National Innovation and Science Agenda. Over the next four years, the Federal Government will spend $194.9 million to implement the recommendations from Australia's **Cyber Security Review**. These included $51 million for the **Defence Department** to relocate the **Australian Cyber Security Centre**, and $11 million to identify cyber vulnerabilities in Commonwealth systems. The Australian Federal Police will receive $20.4 million and the Australian Crime Commission will get $16 million to increase its capabilities to fight cyber crime. The Education Department

will also receive a share of $3.5 million to open up to six academic centres of cyber security excellence.

Return to Table of Contents/ Retour à la table des matières

New Zealand/Nouvelle-Zélande

$22m for cyber security
The Daily Post (New Zealand), Nicholas Jones, 2016 05 06
Wellington - Seven potentially significant cyber intrusions aimed at New Zealand organisations are being detected by a Government security agency every month. What organisations are protected by the **Government Communications Security Bureau's Cortex cyber security programme is secret, but significant economic targets and vital network utilities are likely to be included**. Cortex is mostly automated, with machines using information and patterns gleaned from previous attacks to scan data and systems for points of weakness and possible intrusions. Its existence was first revealed by Prime Minister John Key before the last election, ahead of Kim Dotcom's "moment of truth" event in Auckland. In a speech in Auckland yesterday, Communications Minister Amy Adams revealed more about the attacks that Cortex encounters. "In a typical month, the GCSB through Project Cortex detects seven potentially significant cyber intrusions affecting one or more substantial New Zealand organisations.

Panama Papers a cyber security warning - PM
Radio New Zealand News, Mohamed Hassan, 2016 05 05
Wellington - The Panama Papers leak is a warning to New Zealand businesses to protect themselves from cyber hacking, Prime Minister John Key says. Mr Key announced today a $22 million fund that will go towards setting up a national security agency aimed at protecting businesses and infrastructure from online attacks. The Computer Emergency Response Team (CERT) was first announced in December, and will be included in this year's budget. $20 million will go towards the agency's operating funds over the next four years, with $2.2 in new capital. It is expected to begin operating in early 2017. Speaking at the Cyber Security Summit in Auckland this morning, Mr Key said New Zealanders needed to start taking the threat of cyber attacks seriously. "This is real, it's happening, and there are people sitting out there who just want to make mischief, and want to get access to that information." He said hackers present a real threat to the government, to businesses and to NGOs. "If we're going to do our jobs properly, we better start realising that we've got to take this issue seriously." Mr Key said it wasn't just up to the government to take action, and directors and chief executives of businesses need to get on board. "We can't make you do that for your businesses." "But we are through the CERT, and through all of the other work that **GCSB** and the police and others do, quite willing to work with you, and help you, and provide the best technology that we can."

Return to Table of Contents/ Retour à la table des matières

International

China/Chine

China's Anbot: future of law enforcement?

South China Morning Post, Stephen Chen, 2016 05 10
Beijing - bombs, making arrests and neutralising threats with an electric shock - robotic officer can do it all, but it's making rights watchers uneasy. China is developing a robotic security officer that can sniff out bombs, grab suspects with a mechanical clamp and deliver a jolt of electricity to neutralise threats. The military researchers behind the project say it will start patrolling public areas such as banks, airports and schools, although a human-rights watcher has questioned whether its ability to carry out commands with no questions asked will be abused. A prototype of "AnBot" - developed by the National University of Defence Technology in Changsha (長沙), Hunan (湖南) - was unveiled at a technology expo in Chongqing (重慶) last month. **"We are very, very interested in AnBot," said a senior official with the China Security Association, a trade organisation run by the Ministry of Public Security**. "It is difficult to gauge the size of the market for police robots at this early stage, but it could easily exceed 10 billion yuan [HK$11.97 billion]," the official said. If manufacturers could bring the price below 100,000 yuan per unit, it would "sell big", he said.

Int'l community calls for peaceful solution to South China Sea issue, opposes internationalization
Xinhua News Agency, Staff reporter, 2016 05 10
Beijing - Countries around the world have voiced their support for a peaceful negotiation on the South China Sea issue between the parties directly concerned, opposing its internationalization. Russian Foreign Minister Sergey Lavrov said recently that any disputes in the South China Sea should be resolved through dialogue and attempts to internationalize the issue must be stopped. "We believe that all countries involved in the disputes should follow the principles of non-use of force, and continue seeking mutually acceptable political and diplomatic solutions," Lavrov said in a joint interview with Chinese, Japanese and Mongolian media in Moscow. He urged external players to stop interfering in the negotiations among the parties directly involved. "I am convinced that they (attempts to internationalize the issue) are completely counterproductive," said Lavrov. "Only negotiations, which China and the ASEAN are pursuing, can bring the desired result, namely, mutually acceptable agreements." The core of the Beijing-Manila South China Sea dispute is a territorial one, caused by the illegal occupation of some of China's islands and reefs since the 1970s by the Philippines, and an issue of maritime delimitation.

Return to Table of Contents/ Retour à la table des matières

Russia/Russie

ISIS claims female Russian spy infiltrated terror network
Fox News, Staff report, 2016 05 10
Washington - Her name was "Elvira," and her treachery cost several ISIS members their lives before the caliphate's spy hunters tracked her down and executed her, according to the latest issue of the Islamic State's Russian-language online magazine. The article in Istok, titled "Elvira Karaeva - Agent of the **Russian Special Services**," focuses on a woman whom ISIS in the Caucasus accused of being an agent of the **Russian intelligence services**. According to the piece, Karaeva worked as a spy for four years, during which she secretly passed along information on the jihadi groups in the Caucasus, including locations and photographs of ISIS fighters. The article notes that although Karaeva was questioned by ISIS's "investigative authorities," she was able to convince them of her innocence. But when the terror

network used a "cunning investigative maneuver," the woman confessed and was later executed by an ISIS member, according to the article.

Terrorists planning attacks on mass May 9 V-Day celebrations detained in Moscow
RT (Russia), Staff report, 2016 05 05
Moscow - A group of citizens from Central Asian countries has been detained by Russia's security agency, the FSB, on suspicion of planning massive terror attacks during Victory Day celebrations, at the behest of Syrian and Turkish terrorist leaders. "We have found a large quantity of weapons, explosives and other terrorist equipment," the Federal Security Service, known by the abbreviation FSB, said in a statement. "The suspects were planning to fire weapons into a crowd, during mass street celebrations on May 9," an FSB source told RIA news agency. The security agency said that the citizens of the former Soviet republics were based in Moscow and were planning to target the capital. A source inside the FSB told the Russian news portal life.ru that the detainees numbered 12, and were residents of a single apartment in suburban Moscow. Among them were nine men from Uzbekistan, one from Kirghizstan, and two Russians. Investigators found evidence of communication with terrorists from Syria and Turkey on their phones, as well as a library of extremist literature.

Return to Table of Contents/ Retour à la table des matières

Europe

Two Turkish journalists sentenced after one survives assassination attempt
Washington Post, Erin Cunningham, 2016 05 07
Istanbul - A Turkish court sentenced two prominent journalists to five years in prison for "divulging state secrets" Friday in a high-profile case that has drawn international scrutiny - just hours after one of the reporters was nearly killed in an assassination attempt outside the courthouse in Istanbul. Can Dundar, editor in chief of Turkey's daily Cumhuriyet newspaper, escaped the attack by an armed assailant unscathed but was then handed the five-year sentence for publishing a report on the government's alleged smuggling of arms to Syrian rebels. His colleague, Ankara bureau chief Erdem Gul, was also convicted for his part in publishing the report. Dundar and Gul were acquitted of separate charges of espionage and conspiring to topple the government. The report, published in May 2015, was based on footage purporting to show Turkish intelligence facilitating weapons transfers to rebels across the border in Syria. The incident, which took place early in 2014, came to light after Turkish paramilitary and police forces halted trucks reportedly transporting the weapons. Rights groups have condemned the proceedings and urged Turkish authorities to drop the charges. The Turkey researcher for Human Rights Watch, Emma Sinclair- Webb, called the trial "monstrous" Friday. Media watchdog Reporters Without Borders blasted the case as "autocratic retribution" from Turkish President Recep Tayyip Erdogan, who was named as a complainant in the suit.

Les questions que pose l'affaire de cyberespionnage de RUAG
Le Temps, Lise Bailat, 2016 05 06
Berne - L'attaque a été longue, de haut niveau, menée depuis l'étranger, et elle a requis une classification secrète de la part du Conseil fédéral. L'entreprise d'armement et de systèmes de défense RUAG, qui appartient à 100% à la Confédération, a été infiltrée par un maliciel étranger de haut niveau pendant des mois. « D'après les premiers éléments disponibles, l'attaque de cyberespionnage menée contre RUAG a commencé en décembre 2014 », indique Renato Kalbermatten, porte-parole du Département fédéral de la défense. Et le logiciel espion utilisé semble si sophistiqué qu'il est impossible d'affirmer aujourd'hui avec 100%

de certitude que l'attaque a pris fin. Selon nos informations, c'est un service de renseignement étranger qui a découvert le pot aux roses et transmis l'information aux espions suisses. En janvier dernier, **le Service de renseignement de la Confédération (SRC) a alerté RUAG ainsi que le Ministère public de la Confédération (MPC),** qui a ouvert une enquête pénale contre inconnu le 25 janvier. Dans le même temps, une tentative d'attaque informatique a eu lieu contre le **Département fédéral de la défense (DDPS**), département de tutelle de RUAG, révélait mercredi le Tages-Anzeiger. Elle a pu être déjouée, selon le conseiller fédéral Guy Parmelin.

Un diplomate succède à un autre à la DGSE
Le Figaro, 2016 05 06
Le directeur de la stratégie de la DGSE, Christophe Bigot, devient ambassadeur de France au Sénégal. Ancien ambassadeur en Israël, il retrouve les chemins de la diplomatie, après un passage par les services de renseignements. C'est un autre diplomate, Martin Briens, directeur de cabinet adjoint de Laurent Fabius au Quai d'Orsay, qui prend la direction de la stratégie à la « Piscine » , surnom donné au service de renseignements extérieurs. (article complet)

La Suisse reste démunie face aux cyberattaques
La Tribune de Genève, Florent Quiquerez, 2016 05 06
Berne - «Les risques de cyberespionnage sont totalement sous- estimés en Suisse. » Pour Corina Eichenberger (PLR/AG), qui préside la Commission de la sécurité du National, l'affaire d'espionnage chez RUAG - important groupe de défense et d'aéronautique - est la preuve qu'il y a toujours plus d'attaques contre les sociétés privées et les administrations publiques. L'affaire a été en partie révélée par leTages-Anzeiger. Le Service de renseignement a informé le Conseil fédéral en début d'année de la présence de logiciels espions sur les ordinateurs de RUAG, entreprise en mains de la Confédération. Le Ministère public a ouvert une enquête pénale. Tout cela a de quoi mettre en état d'alerte le Département de la défense (DDPS): la Confédération partage de nombreuses interfaces informatiques avec RUAG. «On ne peut pas encore dire s'il y a eu des dégâts. L'analyse est toujours en cours», explique Renato Kalbermatten, porte-parole du DDPS, qui ne commente pas non plus l'information selon laquelle l'attaque viendrait de Russie. Ce cyberespionnage, qui aurait commencé en décembre 2014, occupe le DDPS depuis des mois. Quatorze mesures ont été prises pour éliminer les risques de vol de données. Lesquelles? «Top secret. » Le Conseil fédéral annonce aussi la création d'une task force pour examiner si l'informatique de l'administration a subi des dommages et renforcer la sécurité le cas échéant.

Russian Spies Are Reportedly Trying to Stop NATO and Sweden From Hooking Up
Vice News, Ryan Faith, 2016 05 03
New York - The Swedish state security police, or SAPO, is getting pretty worried about a dramatic uptick in Russian espionage activity in Sweden, according to leaks in the Swedish press. And SAPO is hinting that it's **related to the fact that Sweden is gearing up for a May 25 parliamentary debate about ratifying a "Host Nation Support Agreement" that would make it easier for NATO troops to use Swedish territory, ports, and bases in exercises or emergencies.** SAPO sources have told the Swedish press that "Russia has tried to influence the debate on Sweden's security policy choices through public statements," and that this overt activity has been matched by an increase in covert activity. Although SAPO is shying away from making lots of specific statements -- charges of espionage are extremely politically sensitive -- it has indicated that it's tracked people affiliated with Russian intelligence services participating in conferences aimed at blocking further Swedish cooperation with NATO.

This is part of a longer-term increase in the aggressiveness of Russian posturing toward Sweden.On March 19, two days after SAPO released its unclassified annual report, which detailed Russian psychological and disinformation campaigns, Swedish media were hit with a massive cyberattack; the "distributed denial of service" attack blocked the sites of seven major Swedish newspapers. This year's SAPO report also asserts that members of **Russia's civilian overseas intelligence service (SVR) and military intelligence service (GRU) have been active in carrying out an aggressive reconnaissance of civilian and military infrastructure**. Last year's report identified 10 SVR and GRU officers among the 37 Russian diplomats in Sweden; this year's report notes an increase in contacts with Swedish radical right-wing organizations.

Le djihadiste breton préparait un attentat
Ouest-France, Jean-Yves Hinault et Thibaud Grasland, 2016 05 04
Côtes-d'Armor - Originaire des Côtes-d'Armor, il préparait l'attaque du commissariat d'Orléans. Il a été interpellé en décembre dans l'Indre. En 2014, Cüneyt Kolankaya tente de rejoindre la Syrie pour y mener le djihad. Il est arrêté le 8 décembre de la même année par la police turque à la frontière syrienne et expulsé vers la France, où il est entendu par l'antiterrorisme. **Le 13 février 2015, âgé de 19 ans, il est interpellé par la Direction générale de la sécurité intérieure (DGSI) chez sa mère à Saint- Martin-des-Prés (Côtes-d'Armor).** Après sa présentation au pôle antiterroriste de Paris, il est mis en examen pour association de malfaiteurs en relation avec une entreprise terroriste et écroué. « Oussama » arrêté chez son père Dans l'émission Spécial investigation , diffusée lundi soir sur Canal + , on retrouve la trace du jeune homme quelques semaines après. Le journaliste, qui s'est infiltré dans un réseau de djihadistes, révèle que Cüneyt Kolankaya, qui se fait appeler « Oussama » , est resté en détention provisoire cinq mois à la prison de Fresnes, puis est retourné vivre chez son père dans l'Indre.

Dutch children as young as nine being trained in ISIS camps: Intelligence Chief
Newsweek, Jack Moore, 2016 05 03
New York - Dozens of children from the Netherlands are now residing in the Islamic State militant group's caliphate, with some as young as nine training in combat, the country's top intelligence official said on Monday. **Rob Bertholee**, the head of the **Dutch intelligence service,** told a Berlin conference on Monday that 250 Dutch nationals have fled the country to fight for the ultraconservative ISIS cause overseas in both Iraq and Syria. This figure includes some 60 women and 70 children. Bertholee said that Dutch authorities have information that shows children aged nine are being used for military purposes by the group.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Former Mossad chief: State Comptroller report on Gaza conflict 'is very severe'
Jerusalem Post, Yaakov Lappin, 2016 05 10
Jerusalem - Former Mossad Director Maj.-Gen. (res.). Danny Yatom said on Tuesday that a draft State Comptroller report, which examines Israeli political and military decision-making in the lead-up to Operation Protective Edge in Gaza in 2014, is a "very severe" document that points to serious failings. Yatom, who spoke during the launch of his new book, Labyrinth of Power, said, "Hamas dragged Israel into Operation Protective Edge, and on our side, we did not understand this." He added that Israel began dealing with tunnels "after a

big delay, and only after terrorists infiltrated Israel through a tunnel." Last week, a security source told The Jerusalem Post that the Comptroller's report is not as severe as has been described in other reports. He added that "nothing was hidden from cabinet ministers. They were exposed to all the details. This was the case before Operation Protection Edge, and certainly after it."

Shin Bet Head: Palestinian Security Forces Respond to Israeli Tips and Thwart Attacks
Haaretz, Barak Ravid, 2016 05 05
Jerusalem - **Head of the Shin Bet security service Yoram Cohen told the cabinet on Wednesday that when Palestinian security forces receive Israeli intelligence information, they act on it to thwart attacks.** Ministers said Cohen sung the praises of security coordination with the Palestinians, but also said that most of the terrorism thwarted in the West Bank was as a result of Israeli operations. During the meeting, Education Minister Naftali Bennett and Internal Security Minister Gilad Erdan argued with Cohen about talks held with the Palestinians about reducing IDF operations in Area A. Cohen replied that he wasn't specifically addressing the extent of attacks that were thwarted by the Palestinians because the issue had to be viewed in a more complex manner.

Accused Israeli spy released
Jerusalem Post, Ariel Ben Solomon, 2016 05 04
Jerusalem **- A Druse from Israel detained by Syria for allegedly spying for Israel has been released after almost 13 years in jail, according to Israeli media reports.** Berjas Awidat, 47, from Majdal Shams in the Golan, left Israel to study in Syria and disappeared after he was taken in Damascus by the Palestine division of the secret police, said Druse Deputy Regional Cooperation Minister Ayoub Kara. "No one knew what had happened to him until a high level Israeli government official intervened in the case," he said. An important figure in the Israeli government handled the Berjas case for many years and twice succeeded in sending Berjas's mother to Syria, explained Kara. Events in Syria, the situation in the prisons and pressure from relatives and, especially, various entities connected to the case in Israel, brought the situation to the attention of Syrian authorities, which decided to release him in order to decrease tensions with the Druse community, Kara said.

Accused Israeli spy released
Jerusalem Post, Ariel Ben Solomon, 2016 05 04
Jerusalem - **A Druse from Israel detained by Syria for allegedly spying for Israel has been released after almost 13 years in jail, according to Israeli media reports**. Berjas Awidat, 47, from Majdal Shams in the Golan, left Israel to study in Syria and disappeared after he was taken in Damascus by the Palestine division of the secret police, said Druse Deputy Regional Cooperation Minister Ayoub Kara. “No one knew what had happened to him until a high level Israeli government official intervened in the case,” he said. An important figure in the Israeli government handled the Berjas case for many years and twice succeeded in sending Berjas’s mother to Syria, explained Kara. Events in Syria, the situation in the prisons and pressure from relatives and, especially, various entities connected to the case in Israel, brought the situation to the attention of Syrian authorities, which decided to release him in order to decrease tensions with the Druse community, Kara said.

Return to Table of Contents/ Retour à la table des matières

Asia/Asie

Afghan forces facing terrorists supported by neighboring intelligence: Stanikzai
Khaama Press, 2016 05 10
Kabul - **The former acting minister of defense and acting head of the Afghan intelligence Masoom Stanikzai said the Afghan forces are facing threats posed by terrorists who are receiving support from the neighboring intelligence**. Stanikzai was speaking during a gathering in Kabul to introduce the acting NDS chief and acting Minister of Defense. Without elaborating further on which neighboring country's intelligence agency is supporting the terrorists fighting in Afghanistan, Stanikzai said the NDS operatives are always on alert to foil conspiracies against the national stability of the country. Stanikzai called the NDS operatives a 'Silent Force' who are always prepared to fight against the foreign conspiracies. He promised President Mohammad Ashraf Ghani and CEO Abdullah Abdullah and the Afghan people to use all efforts to protect the country against the threats posed by the terror groups.

Military probe underway over alleged N. Korean hacking into navy vessel builder
Yonhap News Agency, Staff reporter, 2016 05 10
Seoul - South Korea's military counter-espionage service has opened an investigation into an alleged North Korean hacking attack on Hanjin Heavy Industries & Construction Co. a key builder of naval warships, officials said Tuesday. "After identifying signs that Hanjin Heavy Industries may have been hacked on April 20, the Defense Security Command is currently leading a security investigation into whether any military secrets were leaked and whether North Korea was involved," official sources said. "North Korea could have been involved, but we are not absolutely sure at this stage," he added. Hanjin is a major naval warship builder, having built the latest frigates and amphibious assault vessels including the ROKS Dokdo (LPH-6111). (Full report)

India building 160-strong lab network to tackle bio-terrorism
Times of India, Chethan Kumar, 2016 05 10
Bengaluru - At a time when even the US has been slammed by experts for failing in dealing with bio-terrorism, India's efforts in creating a network of labs to fight it has taken off well with 35 labs established in the first phase having completed collection of data from more than 1,00,000 patients on various kinds of viruses, bacteria and parasites. In about 18 months, a breakout in even a remote part of India will be known to New Delhi and other relevant centres regardless of the casualty count. The labs will detect and map all known viruses and other agents, while also doing research on unknown agents. National and international reports, including a WikiLeaks cable made public five years ago have pointed to the threats bio-terrorism - - use of infectious biological agents such as smallpox or anthrax virus as weapons of terrorism -- has posed to India. India, according to reports in the public domain, has been on the bio-terrorism radar since the mid-2000s.

Ghani names picks for acting defence minister, spymaster
Pajhwok Afghan News, Azizullah Hamdard, 2016 05 06
Kabul - After a flurry of calls from the parliament, President Ashraf Ghani has nominated his picks for defence minister and spy chief. In two separate decrees issued last night, the president nominated Maj. Gen. Abdullah Khan as acting defence minister. According to a statement from the Presidential Palace, Gen. Khan replaces Masoom Stanikzai the current acting defence minister. Stanikzai has been picked as presidential advisor and acting head of

the **National Directorate of Security (NDS**) - the Afghan spy service. Following his nomination by the president, Stanikzai won a vote of confidence from the parliament on June 6, 2015. Last month, the Wolesi Jirga speaker asked the president to nominate his picks for spymaster and minister of defence.

Afghan forces facing terrorists supported by neighboring intelligence: Stanikzai
Khaama Press, 2016 05 10
Kabul - **The former acting minister of defense and acting head of the Afghan intelligence Masoom Stanikzai said the Afghan forces are facing threats posed by terrorists who are receiving support from the neighboring intelligence**. Stanikzai was speaking during a gathering in Kabul to introduce the acting NDS chief and acting Minister of Defense. **Without elaborating further on which neighboring country's intelligence agency is supporting the terrorists fighting in Afghanistan, Stanikzai said the NDS operatives are always on alert to foil conspiracies against the national stability of the country**. Stanikzai called the NDS operatives a 'Silent Force' who are always prepared to fight against the foreign conspiracies. He promised President Mohammad Ashraf Ghani and CEO Abdullah Abdullah and the Afghan people to use all efforts to protect the country against the threats posed by the terror groups.

Haqqani network terrorist arrested in Kabul before targeting parliament
Khaama Press, 2016 05 09
Kabul - A Haqqani network terrorists have been arrested by the Afghan intelligence operatives before the suspects manage to target the parliament building. The **National Directorate of Security (NDS)** said the terrorist was looking to attack the parliament building with BM12 rockets. No further details regarding the exact location where the terrorist was arrested by the intelligence operatives. This comes as the Afghan intelligence operatives foiled attack plots by the notorious Haqqani terrorist network in Kabul city by arresting 3 suspects in connection to the attack plots on Wednesday. The intelligence operatives foiled at least four large attack plots by Haqqani terrorist network in capital Kabul last month. Haqqani network was formed in the late 1970s by Jalaluddin Haqqani. The group is allied with al-Qaida and the Afghan Taliban and cooperates with other terrorist organizations in the region.

CIA director fears Pakistan poisoned him
Daily Telegraph (Australia), Andrew Marszal, 2016 05 07
Washington - **The CIA director who oversaw the raid that killed Osama bin Laden suspected that he was poisoned by Pakistani spies weeks later, according to a report**. Mark Kelton, the agency's Pakistan chief in 2011, was pulled out of Islamabad suffering from a violent stomach illness two months after the CIA-led raid on bin Laden's compound. CIA officials "continue to think that it is plausible - if not provable" that Mr Kelton's illness was the work of Pakistani spy chiefs, and launched an investigation into the matter at the time, the Washington Post claimed yesterday. **It said the "mysterious" nature of the illness, combined with allegations that Pakistani intelligence had been "linked to numerous plots against journalists, diplomats and other perceived adversaries", prompted CIA suspicions**. Relations deteriorated sharply just 48 hours after Mr Kelton's arrival in Pakistan when Raymond Davis, a CIA contractor, shot dead two Pakistani men in Lahore in February 2011. By the time of the bin Laden raid in May, Mr Kelton was barely speaking with Pakistan's spy chief Ahmed Shuja Pa, CIA officials told the newspaper. No evidence was ever found that Mr Kelton had been targeted, nor that Pakistani authorities had poisoned any US official serving in the country. Mr Kelton, 59, now retired from the CIA, said only that it had not been him who first raised the possibility that he had been poisoned.

Indonesia, Malaysia, Philippines sign maritime security declaration
Jakarta Post, Marguerite Afra Sapiie, 2016 05 06
Jakarta - **Foreign ministers and defense force chiefs from Indonesia, Malaysia and the Philippines signed a joint declaration on maritime security on Thursday, calling on all governments in the region to increase efforts to tackle marine threats**. The leaders called for intensified maritime security following the recent kidnapping of seamen by the Southern Philippines-based Abu Sayyaf militant group, and other armed sea robberies, that have endangered national security in the region. In the joint declaration obtained by The Jakarta Post, the officials agreed to conduct patrols and to render immediate assistance for the safety of all vessels and crew in the three countries' respective maritime areas. The governments will also establish a joint focal point to facilitate the timely sharing of information and intelligence, according to the statement released by the Foreign Ministry.

Ghani names picks for acting defence minister, spymaster
Pajhwok Afghan News, Azizullah Hamdard, 2016 05 06
Kabul - After a flurry of calls from the parliament, President Ashraf Ghani has nominated his picks for defence minister and spy chief. In two separate decrees issued last night, the president nominated Maj. **Gen. Abdullah Khan** as acting defence minister. According to a statement from the Presidential Palace, Gen. Khan replaces Masoom Stanikzai the current acting defence minister. Stanikzai has been picked as presidential advisor and acting head of the **National Directorate of Security (NDS) - the Afghan spy service**. Following his nomination by the president, Stanikzai won a vote of confidence from the parliament on June 6, 2015. Last month, the Wolesi Jirga speaker asked the president to nominate his picks for spymaster and minister of defence.

Ghani assigns Stanikzai as acting NDS chief, Abdullah Khan acting defense minister
Khaama Press, 2016 05 06
Kabul - President Mohammad Ashraf Ghani has appointed Mohammad Masoom Stanikzai as the acting Intelligence, National Directorate of Security (NDS) Chief. According to a statement by the Office of the President, General Abdullah has been assigned for the post of acting minister of defense. The statement further added that Stanikzai will also serve as Ministerial Adviser to President Ghani. Abdullah Khan was previously serving as the Chief of Staff in Afghan National Army Chief of Staff office before he was assigned as acting minister of defense. This comes as President Ghani promised to introduce the nominees for Minister of Defense and National Directorate of Security (NDS) Chief during a gathering in the Afghan parliament late last month. Ghani made the promise during a gathering in the Afghan parliament while announcing the government's stance regarding the peace efforts and fight against corruption.

S. spy chief visits Seoul over N. Korean issues
Yonhap News Agency, Staff reporter, 2016 05 05
Seoul - The top U.S. intelligence official visited South Korea this week and met with top Seoul officials to discuss North Korean issues, officials here said Thursday. Director of **National Intelligence James Clapper arrived in Seoul on Wednesday as North Korea is set to hold its key party congress on Friday, amid lingering concern the country will conduct its fifth nuclear test.** "Clapper visited the Ministry of Defense building yesterday morning in an unofficial visit and met with Defense Minister Han Min-koo," a government official said on the condition of anonymity. The two discussed the possibility of another North Korean nuclear test and other security issues, the official said, without elaborating. Clapper also met with other ranking security and military officials, as well as Gen. Vincent Brooks, the new commander of

U.S. Forces Korea, they said. "The visit is believed to have been made in time for the appointment of Gen. Vincent Brooks," said another government official, noting that they are believed to have exchanged intelligence on recent developments in the North's nuclear activities.

Would-be suicide bomber, accomplice held in Takhar, claims NDS
Pajhwok Afghan News, Pajhwok Report, 2016 05 05
Kabul - A would-be suicide bomber and an accomplice guiding him have been detained in northern Takhar province, the National Directorate of Security (NDS) said on Thursday. A statement from the intelligence agency identified the would-be bomber as Mohammad Ayub and his guide as Mohammad Ibrahim. They were arrested during an operation in Ishkamish district. The suspects planned to carry out a suicide attack in the province, but they were caught before reaching their target, the spy service said, adding the detainees were involved in attacks in Takhar, Baghlan and Kunduz. (Full Report).

Something seriously wrong with counterterror security: Pathankot terror attack
Times of India, Staff Report, 2016 05 04
New Delhi - A Parliamentary panel has rapped the government for its failure to prevent the Pathankot terror attack, saying "something is seriously wrong" in the country's counterterror establishment and the airbase's security was not robust. The panel said it has failed to understand that in spite of terror alert sounded well in advance, how terrorists managed to breach the high-security airbase and subsequently carried out the strike. The committee said it is constrained to note that despite concrete and credible intelligence inputs received from abducted and released SP of Pathankot and his friend and through interception of communication between terrorists and their handlers by the terrorists disclosing that they were planning an attack on a defence establishment, the security agencies were so ill-prepared to anticipate threats in time and counter them swiftly and decisively.

Return to Table of Contents/ Retour à la table des matières

Africa/Afrique

Intelligence Official: Islamic State Growing in Somalia
Voice of America, Harun Maruf, 2016 05 05
Washington - Pro-Islamic State Somali militants have grown in numbers and are receiving financial and military support from Yemen, a top intelligence official told the VOA Somali Service. Abdi Hassan Hussein, the former Director of the U.S.-backed Puntland Intelligence Agency (PIA) said when the pro-IS Somali faction was founded in October last year it had about 20-30 men, but has since set up training camps and recruited more fighters. He said the group's fighters now number between 100-150 fighters. "They have graduated their first units and they have received their military supplies," he said. Hussein led PIA until a year ago when he was replaced. His main job was to detect militant threats and plan counter-terrorism operations. He said Islamic State has welcomed its Somalia branch and has started delivering supplies through their affiliate faction in Yemen. "They received military supplies from Yemen - weapons, uniform, ISIS sent trainers who inspected their bases, and they have started sending financial support," he said. "The weapons' shipment was delivered by sea from Mukallah city in Hadramouth, it has arrived from the Red Sea coast of Somalia in February and March this year." Hussein said the government and African Union troops can't win against al-Shabab or IS factions militarily, and urged them to confront the groups ideologically. "The youth they are

sending are assets, but misguided; they need to be saved from harming the people and harming themselves," he said.

Return to Table of Contents/ Retour à la table des matières

Americas/Amériques

Cuban Five caused no harm to US as they fought against terrorism - Russian lawmaker
TASS World Service, 2016 05 10
Moscow - The activities of the so-called Cuban Five - a group of five Cuban intelligence officers, did not cause any harm to the United States, as were aimed against the terrorist threat, first vice-speaker of the Russian State Duma lower house of parliament, first deputy chairman of the Central Committee of the Communist Party of Russia (CPRF) Ivan Melnikov said on Tuesday at a meeting in Moscow with the Cuban antiterrorists heroes. The five arrived in Moscow on Sunday, May 8 to attend a military parade celebrating Russia's victory over fascism in Moscow"s Red Square on May 9. They were expected to meet with Russian Foreign Minister Sergey Lavrov, parliamentarians, members of the Cuba solidarity movement and state officials. "Now there is much talk in different parts of the world that terrorism has become a major threat to peace. This is true, but only, as always, the Americans apply double standards to all issues, as well as to this issue," he said. "Your activities in the US territory caused absolutely no damage to the US national interests", Melnikov said, adding that members of the Cuban Five were "real antiterrorist fighters." "You were engaged in preventing those terrorist attacks that were aimed against your country, and did this successfully", the State Duma official said.

Leader opposition party in Venezuela assassinated
Fox News Latino, Staff Writer, 2016 05 08
Caracas - **Venezuelan politician German Mavare, leader of the opposition UNT party, died Friday after being shot in the head, an assassination that occurred in the western state of Lara, his organization said.** "The board of the UNT expresses its deepest sorrow for the slaying of colleague German Mavare. We demand justice and an end to violence," was the message posted on the Twitter account of the UNT party, headed by jailed ex- presidential candidate and former governor of Zulia state, Manuel Rosales. The mayor of Iribarren in Lara state, Alfredo Ramos, said on his Twitter account minutes after the incident occurred before dawn Friday: "German Mavare, of the popular urbanization of Carucieña, a tireless fighter for social causes, has just been hit by a bullet in the head." For his part, Luis Florido, an opposition lawmaker of the Voluntad Popular party, said on Twitter: "German Mavare died. A red bullet ended his life. Politics today is high risk. We demand an investigation of the case #NoMoreViolence #Lara".

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

15-06-2016 to/au 21-06-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Security officials gather in B.C.
The Province (Vancouver), Rob Shaw, 2016 06 20
Vancouver - **Top police, intelligence and security officials from Canada and the United States will gather at the B.C. legislature this week to discuss how best to protect politicians inside capital buildings from the growing threat of terrorist attacks**. The conference was organized by sergeant-at-arms Gary Lenz, head of security at the B.C. legislature, who said a discussion is needed on the rapidly changing pace of investigating, responding to and preventing threats against politicians, staffers and tourists inside capital buildings across North America. "The world has changed, security has changed and the people in charge of life, property and security need to also change," said Lenz. adding the goal is to develop standards, policies and expectations for sergeants-at-arms, as well as breaking down silos among agencies that monitor and respond to threats. **More than 43 officials plan to attend, including the western director of Canada's spy agency, the Canadian Security Intelligence Service, and RCMP officers who head up the Parliamentary Protective Service and Integrated National Security Enforcement Teams**. Security officials from legislatures in Scotland, Texas, Virginia and Hawaii are also attending, as well as the first chairman of the New York State Senate Homeland Security Committee, who helped craft modern-day security legislation after the terrorist attacks at the Twin Towers in 2001.

Goodale hopes new spy oversight committee will be 'spontaneous' with reports
CBC.CA, Catharine Tunney, 2016 06 18
Ottawa - Public Safety Minister **Ralph Goodale says he hopes Canada's new spy watchdog committee will file multiple public reports about its findings and concerns about the country's covert security and intelligence activities.** "The law says a minimum once per year, but I would hope the committee would send a report whenever they felt it was necessary," he told Chris Hall in an interview on CBC Radio's The House. On Thursday the federal government introduced new legislation to create a joint oversight committee with robust powers to scrutinize national security matters.. When questioned if a nine people would be enough for the sweeping monitoring he's promised, Goodale pointed out there are already oversight bodies in place including the **Security Intelligence Review Committee that oversees CSIS, and the Civilian Review and Complaints Commission for the RCMP.**

Security supercommittee to report to prime minister
Globe and Mail, Daniel Leblanc, 2016 06 17
Ottawa - A **group of nine MPs and senators will receive extraordinary powers to delve into Canada's national-security secrets**, although questions remain about the government's right to restrict its access to documents or its ability to raise its concerns in public. As promised in last year's election, the Liberal government tabled legislation to create a national security and intelligence committee of parliamentarians to provide oversight of all 17 federal agencies involved in security issues. While composed of parliamentarians, the new committee will report to the prime minister, unlike traditional parliamentary committees. As such, the new committee's annual and special reports will be vetted by the government before they are released to prevent the disclosure of any classified information, which stands to constrain the body's ability to raise red flags with the public. **The committee will have a "broad mandate," Public Safety Minister Ralph Goodale insisted at a news conference**. The seven MPs and two senators will be able to review "any activity" carried out by national- security agencies and "any matter

relating to national security or intelligence," according to Bill C-22. However, the government will be able to constrain certain investigations as ministers will have the right to refuse to provide information that "would be injurious to national security." **The committee will be able to monitor the work of the Canadian Security Intelligence Service, but will be prevented from looking at continuing RCMP criminal investigations or delve into "ongoing defence intelligence activities supporting military operations."**

Spy watchdog mandate covers 'any operation'
Ottawa Citizen, Ian Macleod, 2016 06 17
Ottawa - **Sweeping powers to scrutinize "any issue, any activity, any operation" will be granted to a new committee of parliamentarians to watch over federal spying and other clandestine security and intelligence activities,** the government has announced. The long-promised **Bill C-22**, tabled in the Commons Thursday, proposes the creation of an unprecedented "national security and intelligence committee of parliamentarians" to hold to greater account the nation's two chief spy services and at least 15 other departments and agencies with national security responsibilities. The move fulfils a major Liberal election promise to increase parliamentary scrutiny of national security operations to offset the expansive and controversial counterterrorism powers under the **Anti-terrorism Act of 2015, formerly Bill C-51**, to investigate, detain, arrest, silence or otherwise thwart individuals suspected as threats to the security of Canada.. "They are going to have the ability to look at any issue, any activity, any operation, any document in the government of Canada that relates to security and intelligence matters," Public Safety Minister **Ralph Goodale** told reporters after the bill's unveiling. Current review of the national security apparatus and the handling of public complaints is now siloed within three small watchdog agencies, led by the **Security Intelligence Review Committee** (SIRC), which conducts afterthe-fact reviews of the operations of **CSIS**.

Liberals want to stop MPs from saying too much
Toronto Star Online, Tonda MacCharles, 2016 06 16
Ottawa - **A bill to establish a long-promised parliamentary committee to review Canada's national security agencies will make it a criminal offence for MPs to blab what they learn**, says Public Safety Minister **Ralph Goodale**. It is already an offence under the Security of Information Act for government officials to disclose security and intelligence information and for any person to make unauthorized disclosures, but Goodale suggested there will be additional precautions taken in the act. "These MPs will be undertaking a very serious responsibility," he told reporters. "They'll have to meet certain, very specific security standards. They'll have to swear an oath with regard to the information they obtain. And violation of that oath is a criminal offence and a breach of trust. So the consequences for illegally improperly divulging information that is contrary to the national security of Canada is a serious, criminal offence." The proposed law Goodale will introduce Thursday in Parliament will fulfill a Liberal promise to give **elected MPs the ability to oversee the activities of agencies like the RCMP, the spy agency CSIS, the electronic signals intelligence agency CSE, and border guards at the CBSA.** It is not yet clear whether the Liberal government will allow MPs to oversee in real time the activities and operations of national security agencies, or whether they will operate more as the civilian-led watchdog of CSIS now does -- conducting after-the-fact review of those activities.

Frontières - Ottawa donnera plus d'informations aux Américains... et à l'assurance-emploi
Le Devoir, Marie Vastel, 2016 06 16
Ottawa - **Le Canada traquera bientôt les entrées et sorties de tous ses citoyens à la frontière américaine et refilera ces informations à Washington**. Le tout, sans baliser davantage le partage de ces renseignements. Ce qui fait bondir une fois de plus les groupes de

défense des droits civils. Mais le gouvernement Trudeau modifie en outre ses lois pour partager ces données avec ses propres ministères afin de déceler ceux qui fraudent ses programmes sociaux. Justin Trudeau avait annoncé, de passage à Washington ce printemps, qu'il élargirait bientôt le partage d'informations entre le Canada et les États-Unis. Les données biographiques -- nom, sexe, date de naissance, nationalité, et autres informations figurant sur le passeport -- des ressortissants étrangers et des résidents permanents étaient déjà récoltées à la frontière depuis cinq ans. Elles le seront aussi pour les citoyens des deux pays qui traversent par voie terrestre. Surprise, cependant, dans le projet de loi déposé par le ministre de la Sécurité publique, **Ralph Goodale : l'Agence des services frontaliers pourra également partager ces données avec le ministère de l'Emploi et du Développement social si l'information peut être utile à l'application de la Loi sur l'assurance-emploi ou de celle sur la sécurité de la vieillesse**.

New bill would allow border guards to collect biographic data on those leaving Canada
CBC News, Staff reporter, 2016 06 16
Ottawa - The federal government plans to introduce **a bill today that would allow border guards to collect biographic information from everyone leaving Canada**. The move will implement the final stages of the entry-exit agreement Canada signed under a joint border initiative with the U.S. in 2011. Public Safety Minister **Ralph Goodale** is holding a news conference after question period today. CBCNews.ca is carrying the news conference live at 3:20 p.m. ET. The legislation proposed by Goodale, **titled "An Act to amend the Customs Act,"** is one of three public safety bills the Liberal government plans to introduce this week. A bill on pre-clearance for people crossing the border is expected tomorrow. Addressing reporters in Ottawa, Goodale said **the biographical information collected would not go beyond what Canadians might find on the second page of their passport**: Name, nationality, date of birth, gender and issuing authority of the passport. The **Canada Border Services Agency** currently collects biographical information from everyone entering Canada but does not track when and where a person leaves Canada. This bill will close the gap and provide the federal government with a way to better track who is entering and leaving the country.

Canadians not so eager to weaken our country's anti-terrorism legislation anymore
National Post, John Ivison, 2016 06 15
Column: In the general election campaign, the Liberals were vocal about repealing the "problematic elements" of the Conservative government's anti-terror legislation. In the wake of the carnage in Paris last November, and now Orlando, **it is fair to say there is much less enthusiasm to overturn many of its provisions, particularly those that allow the Canadian Security Intelligence Service to disrupt potential terrorist activity. Ralph Goodale, the public safety minister, will introduce a bill creating an all-party committee of parliamentarians to provide oversight to the expanded national security apparatus before the House rises this summer**, as the Ottawa Citizen's Ian MacLeod reported earlier this month. The government will also review all appeals by Canadians to the no-fly list and create a counter- radicalization office to work in vulnerable communities, as promised in the election platform. Goodale has further said he intends to engage in public consultations on the entire national security framework over the summer, to look at areas where the current legislation might be improved. But, in the wake of ISIL-inspired outrages in Paris and Orlando, there does not seem to be an appetite to roll back the substantive parts of the bill that allow CSIS to use loosely defined disruptive "measures," or attempt to raise the threshold for preventative detention. The reason for that is simple. **When he appeared before parliamentary committees in the spring, CSIS director Michel Coulombe said the powers are being used and have been successful in disrupting terror attacks. "For every terror attack that takes place in Canada and abroad, many more are disrupted," he told the Senate defence**

committee in March. "Threat mitigation measures" have been used "less than two dozen times" in the previous six months, he said. When C-51 was introduced, many civil rights advocates were concerned it would impact adversely on constitutionally protected rights.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

FBI no-fly list revealed: 81,000 names, but fewer than 1,000 are Americans
Washington Times, Stephen Dinan, 2016 06 21
Washington - The **FBI's no-fly list contains about 81,000 names, but fewer than 1,000 of those are "U.S. persons,"** a top lawmaker revealed Monday, giving the outlines of the secretive program on the floor of the Senate. Another list maintained by the FBI, dubbed the "TSA selectee list" because it triggers higher scrutiny but doesn't ban flying, has some 28,000 records, of which fewer than 1,700 are U.S. persons, Sen. Dianne Feinstein said as she argued for denying gun sales to those who appear on the lists, in the wake of the Orlando terrorist shooting. Democrats say those lists and a broader list, the **Terrorist Screening Database**, with about 1 million names, should be used to deny potential terrorists lethal weapons. Mrs. Feinstein has proposed banning those who appear on any of the lists from being able to clear a background check enabling them to purchase a firearm. Republicans argue the lists are too broad, and are riddled with errors that, if followed, would deny law-abiding Americans their Second Amendment rights without due process of law.

Former El Paso FBI chief to lead US Border Patrol (Canada)
El Paso Times, Cindy Ramirez, 2016 06 21
El Paso - An **FBI veteran** who once led the El Paso division **has been named to head the U.S. Border Patrol,** bringing in an outsider to run an agency traditionally led by agents who rise through the ranks. **Mark Morgan**, who briefly led the internal affairs department at the Border Patrol's parent agency, has been chosen to oversee a multibillion-dollar annual budget and about **20,000 agents who patrol the nation's land borders with Canada and Mexico** and its maritime boundaries, the Associated Press reported. "It is my great privilege and honor to be selected to serve with the men and women of the U.S. Border Patrol and to lead this great organization," Morgan said in a statement issued by the U.S. Customs and Border Protection, which oversees the agency.

U.S. Spies: Israeli Agent Jonathan Pollard Could Spill More Secrets--Even After 30 Years Behind Bars
The Daily Beast, Shane Harris, 2016 06 21
Washington - **Jonathan Pollard, the former U.S. intelligence analyst turned spy for Israel, wants the American government to ease up on the conditions of his parole**. In legal briefs, he has argued that Washington should stop monitoring his personal computer and online activities and not force him to wear a personal GPS device that tracks Pollard's movements in New York, where he has been living since his release from federal prison last year. To which the U.S. intelligence community has essentially replied, "Oh, hell no." **In a series of declarations filed late Friday with the U.S. Parole Commission, senior U.S. intelligence officials forcefully argued that Pollard still poses a risk to national security because if left unchecked, he could divulge U.S. secrets**--and even old ones could do harm. "Some of the sources and methods used to develop some of the intelligence exposed by Mr. Pollard not only remain classified but are still in use by the Intelligence Community today," Jennifer L. Hudson, a

senior official in the **Office of the Director of National Intelligence**, said in a written statement. One former official who worked on the damage assessment after Pollard's espionage was discovered said that he was driven not by patriotism for Israel, but by the need to pay for his high-spending lifestyle and drug habit. "It was all about money, and he put most of it up his nose.

Inside the Pentagon's secretive preparations for a 'cyber 9/11'
Army Times, Andrew Tilghman, 2016 06 21
Suffolk - A fictitious scenario was laid out for nearly 1,000 military, government and private sector personnel here at **this year's Cyber Guard exercise**, the nation's largest test of its network defenses. Conducted over nine days in June, the event offered a disturbing look at the type of catastrophe that could unfold during what the government's top officials call "cyber 9/11." "For us, it's not a question of ifit will happen but when," said **Coast Guard Rear Adm. Kevin Lunday, U.S. Cyber Command's director of training.** "The more relevant question is: When it does [happen], will we as a Department of Defense, will we as a nation and with our allies, be ready for it?"

FBI chief Comey stakes out unusually public profile on biggest issues
USA Today, Kevin Johnson, 2016 06 20
Washington - **When President Obama named James Comey to succeed FBI Director Robert Mueller, the popular nominee acknowledged the long shadow cast by the man who in the previous 12 years had led the bureau longer than anyone except J. Edgar Hoover**. "I must be out of my mind to be following Bob Mueller," Comey said in the 2013 White House Rose Garden ceremony. "I don't know if I can fill those shoes, but I know that, however I do, I will be standing truly on the shoulders of a giant." Indeed, Mueller's tenure was widely credited with the post-9/11 transformation of the FBI from a largely reactive law enforcement institution to an intelligence-driven agency bent on preventing new terror strikes. And he did it by shunning the spotlight at virtually every opportunity. By contrast, **Comey, 55, has staked out a public profile that couldn't be more different than his predecessor and the traditional confines of the office itself**. "I've known Jim for a quarter century," said Chuck Rosenberg, director of the Drug Enforcement Administration who also served as Comey's first chief of staff at the FBI. "When he feels like he has something to say, he does so only after careful judgment. And while it may seem like an unusual role for an FBI director, it's not a reflex action. It has nothing to do with self promotion or aggrandizement."

Amid gun scrutiny, government's growing watch lists are in sharper focus
Washington Post, Jerry Markon, 2016 06 18
Washington - The **push by congressional Democrats to bar suspected terrorists from acquiring guns and explosives has focused renewed attention on the government's secretive terrorist watch lists,** which have grown exponentially since the 9/11 attacks and triggered widespread concern among civil liberties groups. Since the mass shooting in a gay nightclub in Orlando on Sunday, Democrats have endorsed various measures to get weapons out of the hands of people on the lists. The Senate is expected to vote Monday on a series of competing gun-control measures that will highlight the continuing partisan divide over the issue. The Orlando shooter, Omar Mateen, had been on the FBI's terrorist watch list but was removed in 2014. His was one of approximately 800,000 names in that database, the most prominent of at least seven overlapping watch lists maintained by at least four federal agencies. The system has grown so large and complex that **Sen. Bob Corker (R- Tenn.), the chairman of the Senate Foreign Relations Committee, said this week that the Senate will vote "with almost no one understanding how these lists are put together**, how they're adjudicated,

how you get off of them." He added: "The terror watch list is not what people think it is . . . and there's 11 different lists."

CIA: Militants Still Able to Stage Attacks
Wall Street Journal, Damian Paletta, Alan Cullison, 2016 06 17
Washington - A **two-year campaign by the U.S. and other countries to defeat Islamic State has failed to disrupt its capability to carry out terrorist attacks, Central Intelligence Agency Director John Brennan saidThursday**. Airstrikes and efforts to cut off its access to cash have been in place since mid-2014, but the group has continued to adjust its strategy to continue operating -- and influencing others. Although the terror group has lost territory in Iraq and Syria, it has still been able to direct or inspire terror attacks in Europe, the Middle East, and the U.S. "The group's foreign branches and global networks can help preserve its capability for terrorism regardless of events in Iraq and Syria," Mr. Brennan said. "In fact, as the pressure mounts on [Islamic State], we judge that it will intensify its global terror campaign to maintain its dominance of the global terrorism agenda."

CIA chief outlines 'blinking red lights' for White House hopefuls
Politico, Ellen Mitchell, 2016 06 16
Washington - The **CIA director told Congress Thursday that cyberthreats, North Korea's nuclear program, and instability across the Middle East and Africa are the top issues he would highlight when briefing President Barack Obama's potential successors on the world's "blinking red lights."** Both Donald Trump and Hillary Clinton are expected to receive classified briefings from intelligence agencies once they officially become the Republican and Democratic presidential nominees, as expected, next month. "Terrorism is going to continue to plague us, and that's related to the cyber issue and how we're going to make sure that FBI and NSA and CIA and others are going to be able to do their jobs to protect this country," **John Brennan** told members of the Senate Select Committee on Intelligence. He added that the whoever is elected in November "needs to use all four years" to take on cyber.

CIA drone strikes plummet in shift to Pentagon
Washington Post, Greg Miller, 2016 06 17
Washington - The **pace of the CIA's drone campaign has plunged this year as part of a renewed push by the Obama administration to shift responsibility for lethal counterterrorism operations to the Pentagon,** current and former U.S. officials said. The agency has carried out at most seven strikes in 2016, putting the spy service on course to take fewer shots from remotely piloted aircraft than in any year since 2007, two years before President Obama took office and made the agency's drone program a pillar of his counterterrorism approach. U.S. officials said several factors have contributed to the sharp drop in the number of strikes, including the staggering depletion of al-Qaeda's ranks in Pakistan, where in 2010 the agency launched 118 attacks. By comparison, the CIA has fired missiles from remotely piloted aircraft only twice this year. But the decline also has been driven by White House decisions to curtail the CIA's lethal role in Yemen and restrict it from even flying armed drones over Syria - instead handing the unambiguous lead for such operations to the U.S. military's elite **Joint Special Operations Command (JSOC**). Officials at the CIA and the White House declined to comment.

FBI Should Crack Smartphones Themselves, Says Cybersecurity Expert
Popular Science, Coby McDonald, 2016 06 17
New York - **When the FBI asked Apple to help crack the San Bernardino shooter's iPhone, the agency was wading into dangerous waters**. That's according to **an essay by Susan Landau, Professor of Cybersecurity Policy at Worcester Polytechnic Institute**, published

today in the journal Science . Landau, who worked as a privacy analyst for Google, writes that the FBI's approach was shortsighted and risked undermining smartphone protections for users across the board while inviting exploitation of the resulting security weaknesses by bad guys. The real problem, Landau says, was the way the FBI wanted Apple to crack the phone. The agency had ordered Apple to create a special update that would disable a security feature normally causing the phone to shut down after ten failed password attempts. If the use of updates to hack smartphones were to become routine, it could lead to misuse by bad actors, she argues. "Some neglect in the process or the collaboration of a rogue employee would make it easy for false requests to be slipped into the update queue." And consumers might wonder if new updates might actually be surveillance tools. If distrust leads users to avoid updates it "would have devastating security effects," she writes.

Former CIA Chief: Trump's Conspiracy Theory About ISIS Is Nonsense
Politico, Michael Morell, 2016 06 17
Comment - **Presumptive GOP presidential nominee Donald Trump, seeking to make the case following the Orlando shootings that the Obama administration was somehow sympathetic to terrorists, resurrected an old conspiracy theory Thursday about the Islamic State**, one that has no place in our public discourse. In a tweet, Trump pointed his followers to an article about the 2012 memo titled "Hillary Clinton Received Secret Memo Stating Obama Admin 'Support' for ISIS." This is, of course, quite a charge against President Obama and his administration at a time when Clinton was still serving as secretary of state. The problem with the charge is that it is simply not true. I know this, since in **my role as deputy director and acting director of the CIA, I participated in nearly every meeting in the Situation Room at the time of the supposed memo regarding the deteriorating situation in Syria**. These included deputies meetings chaired by then-Deputy National Security Adviser Denis McDonough; principals meetings chaired by then- National Security Adviser Tom Donilon; and National Security Council meetings chaired by the president.

House votes down surveillance reform effort
The Hill, Katie Bo Williams, 2016 06 16
Washington - **House lawmakers on Thursday voted down language that would have closed what critics call the "backdoor search loophole" in current surveillance law**. The amendment to the annual defense appropriations bill failed 198-222. Intelligence Committee Republicans had lobbied against the proposed edit in the days leading up to the vote, petitioning colleagues in a Thursday letter to "give our Intelligence Community all of the authorities it needs to detect and stop terrorist attacks."

In Declassified Transcripts, Details of C.I.A. Torture
New York Times, Charlie Savage, 2016 06 16
Washington - After the **Central Intelligence Agency transferred Abu Zubaydah to the American military prison at Guantánamo Bay, Cuba, and he was brought before a panel of officers for a hearing in March 2007, he described in broken English how he had been tortured in the agency's black-site prisons**. He said his body had shaken when he stood for hours, naked and shackled in a cold room and unable to shift his weight to an injured leg. He spoke of his humiliation at having to relieve himself in a bucket in front of other people, "like an animal." And he described being waterboarded until he stopped breathing and required resuscitation. The government disclosed the accounts this week in response to a Freedom of Information Act lawsuit brought by the American Civil Liberties Union, which provided the documents to The New York Times.

Pentagon Unleashes Cyber Effort to Counter Militants on Battlefield
Voice of America, Carla Babb, 2016 06 16
Washington - The **Pentagon has launched a new cyber task force to counter the Islamic State group,** and officials say it is creating advantages both in cyberspace and on the battlefield. The task force, **JTF-Ares**, was developed in May and is in its "initial operation phase," U.S. Cyber Command spokesman Joe Holstead said. The military has carried out several cyber offensive operations against IS militants, which experts say have produced many coalition successes in the last few months. "There's no bang, and there's no explosion, but it does give you a military advantage," said James Lewis of the Center for Strategic and International Studies.

CIA chief: ISIS working to send operatives to the West
Associated Press, Staff report, 2016 06 16
Washington - **CIA Director John Brennan will tell Congress on Thursday that Islamic State militants are training and attempting to deploy operatives for further attacks on the West and will rely more on guerrilla- style tactics to compensate for their territorial losses**. In remarks prepared for the Senate Intelligence Committee, Brennan says IS has been working to build an apparatus to direct and inspire attacks against its foreign enemies, as in the recent attacks in Paris and Brussels -- ones the CIA believes were directed by IS leaders. "ISIL has a large cadre of Western fighters who could potentially serve as operatives for attacks in the West," Brennan said, using another acronym for the group. He said IS probably is working to smuggle them into countries, perhaps among refugee flows or through legitimate means of travel. Brennan also noted the group's call for followers to conduct so-called lone-wolf attacks in their home countries.

Homeland Security Chief: Gun Control 'Part and Parcel' of Agency Mission
Wall Street Journal, Julian Routh, 2016 06 15
Washington - **Homeland Security Secretary Jeh Johnson said Tuesday that gun control is "critical" to public safety and should be part of his agency's mission to protect Americans from "homegrown" terrorism.** In what he said were his first public comments on the issue, Mr. Johnson told CBS News that the government must "minimize" the opportunities for terrorists to obtain guns in the U.S. "We have to face the fact that meaningful, responsible gun control has to be part of homeland security as well, given the prospect of homegrown, home born bound extremism in this country," Mr. Johnson said. "We've seen this now with Orlando and San Bernardino.

Newly released CIA files expose grim details of agency interrogation program
Washington Post, Multiple reporters, 2016 06 15
Washington - The **CIA released dozens of previously classified documents Tuesday that expose disturbing new details of the agency's treatment of terrorism suspects after the Sept. 11, 2001, attacks,** including one who died in Afghanistan in 2002 after being doused with water and chained to a concrete floor as temperatures plunged below freezing. The files include granular descriptions of the inner workings of the CIA's "black site" prisons, messages sent to CIA headquarters from field officers who expressed deep misgivings with how detainees were being treated and secret memos raising objections to the roles played by doctors and psychologists in the administration of treatment later condemned as torture. But the collection also includes documents that were drafted by senior CIA officials to defend the interrogation program as it came under growing scrutiny, including a lengthy memo asserting that the use of often brutal methods had saved thousands of civilian lives.

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

EU referendum: Poll reveals third of Leave voters believe MI5 conspiring with Government to stop Brexit
The Independent (UK), Ashley Cowburn, 2016 06 21
London - **Nearly a third of Leave voters believe Britain's intelligence agency MI5 is in cahoots with the Government to stop Britain leaving the European Union**, according to a new poll. The poll, by YouGov for LBC, also found 28 per cent of all voters believe Thursday's referendum is rigged. A total of 64 per cent of Ukip supporters thought it was likely the referendum would be rigged, compared with just 16 per cent from the party who thought such an idea was "probably false". In total, 21 per cent of those surveyed believed MI5 was working with the UK government to try and stop Britain leaving the EU. Around 40 per cent said this was "probably false" while 39 per cent opted for "don't know".

Remain in EU, say former UK security and intelligence chiefs
The Guardian (London), Richard Norton-Taylor, 2016 06 21
London - Economists can argue forever - or neverendum, as the saying goes now. What is extraordinary is the breadth and depth of the arguments over the pros and cons of EU membership - even entering the realm of spooks. **Former security and intelligence chiefs (who make it clear they are speaking for serving officers) are warning that leaving the EU would hinder their work protecting Britain**. It is as if Brexiteers, including some senior ministers, are dismissing offhand **warnings from MI5 and MI6.** "I do know", said Nigel Inkster, a former director of MI6, "that the intelligence community places enormous value on exchanges" with intelligence agencies of other EU countries, notably over information on suspected terrorists or violent extremists. In the event of Brexit, "I do know the intelligence community would be concerned", he stressed. Existing EU agreements on sharing datesets would have to be renegotiated on a bilateral basis, he said.

Police chief urges companies to step up terror response training
Sunday Times (UK), Mark Macaskill, 2016 06 19
London - **One of Scotland's most senior police officers is urging employers to give staff anti-terrorism training under plans to boost Britain's preparedness for an atrocity**. Up to 1m civilians a year are to be trained in how to help prevent -- and in the worstcase scenario, react to -- a terror attack on British soil. The move signals a step change in the training of civilians, which until now has focused on those working in "high-risk" venues such as stadiums, shopping centres and airports. Under **Project Griffin**, about 100,000 people a year receive anti-terrorism training, but it is hoped to increase this to 1m a year with the launch of a self-help anti-terror manual. The guide aims to help civilians to understand the threat from terrorism, to empower them to recognise and report suspicious activity, and teach them what to do if they are caught up in a terrorist incident. "While being prepared and knowing what to do is vital, it is equally important that as many people as possible who work in busy places are aware of the threat and are better equipped to recognise and report suspicious activity," said **Chief Inspector Ronnie Megaughin, deputy director of the Scottish Business Resilience Centre**.

Local anti-terrorism advisers will provide briefings to trainers from companies and organisations, who will be able to feed the information back to colleagues.

I am a former MI6 chief and a lifelong patriot. Here's why I'm voting Remain
London Daily Telegraph, John Sawyers, 2016 06 17
Comment - I've spent my professional life batting for Britain. **As Chief of MI6, I led a service devoted to defending Britain from attack** . When I was Ambassador at the UN and in Egypt I worked exclusively for British interests. I've always helped implement the policies of the government of the day. But the motivation was to serve our country. Unlike my parents and grandparents, I've been privileged to live my life in an era of peace in Europe. I want the same for my children and grandchildren. The EU helped stabilise continental Europe. France and Germany are reconciled and are now committed partners. Newly democratic countries in the south and east of Europe strove to be part of the EU as it was an anchor point for democracy and the rule of law. Today, however, I am worried by the turn that politics in Europe is taking. Extremist pressures are returning, with echoes of the Thirties. **If Britain leaving causes the EU to crumble , where are the brakes to stop Europe sliding backwards to extremes of Left and Right, inviting renewed conflict ? We would inevitably be drawn in to try to sort it out. We can't pass that on to the next generation. We must defend ourselves against terrorists.** Terror networks operate across borders, and so must we if we are to stop them. The EU provides a valuable legal framework for sharing information and data - crucial tools in the modern era.

Inside the GCHQ doughnut, code breakers face up to our encrypted future
i News (UK), Gordon Corera, 2016 06 16
London - **If you journey beneath GCHQ's "Doughnut", you find yourself in a cavernous computer hall, stretching to 10,000 square metres. Ear protectors are required for visitors to hush what sounds like a constant electronic waterfall** - and the exact names of some of the computers are secret, as is their processing power. Bletchley Park's great innovation while cracking the Nazis' Enigma Code during the Second World War was the melding of human ingenuity with the kind of processing power that only a computer could offer. That remains the model for today's codebreakers. **Inside the "Doughnut", the mathematical heirs to Alan Turing sit in front of screens displaying ones and zeros rather than the pads of paper with letters that made up the Enigma code.** But it is the same task of understanding a system and its weaknesses. "My job is a combination of maths and computer programming and just being crafty at problem-solving," a female twenty- something mathematician explains. "You know why it is important. And that is what spurs you on."

Snowden Disclosure Prompts Backlash in Scotland
The Intercept, Ryan Gallagher, 2016 06 16
Washington - Top **government officials in Scotland are under pressure to explain their knowledge of a secretive police surveillance unit that was exposed in documents leaked by National Security Agency whistleblower Edward Snowden**. On Tuesday, cabinet secretary for justice Michael Matheson was grilled in the country's parliament about the so-called Scottish Recording Centre and its previously undisclosed involvement in covert surveillance operations. As The Intercept revealed last week, the Recording Centre is one of several domestic organizations within **the United Kingdom involved in a top-secret program named MILKWHITE**, which has provided law enforcement agencies with access to "bulk" internet data intercepted by the British eavesdropping agency Government Communications Headquarters, or GCHQ. Prior to the disclosure, few in Scotland knew the Recording Centre even existed -- much less that it has been tapping into GCHQ's troves of data. In recent days,

several Scottish media outlets have picked up the issue, increasing pressure on the government.

Return to Table of Contents/ Retour à la table des matières

Australia / Australie

AFP report leaves unanswered questions on top secret intelligence leak
Sydney Morning Herald, Deborah Snow, 2016 06 18
Canberra - **Independent Tasmanian MP Andrew Wilkie has strongly rejected what he claims is offensive and unfounded "innuendo" levelled against him in a 12-year old Australian Federal Police report into the leaking of an intelligence document on the Iraq War to conservative columnist Andrew Bolt** in 2003. Mr Bolt, a supporter of the Howard government, used the document to undermine the credibility of Mr Wilkie, who by then had left his **job as an intelligence analyst with the top secret Office of National Assessments and become a vocal public critic of the war**. The AFP report, released on Friday after a freedom of information request by Labor, is highly critical of the way the bureaucracy handled Mr Wilkie's highly classified report, which he produced in late 2002 on the eve of the Iraq War. Federal investigators say 84 copies were distributed around the government between December 2002 and September 2003. But only seven of the receiving agencies external to ONA had "handled the receipt, distribution and return of the document in accordance with the ONA handling guidelines."Despite this, the AFP says, "we are prepared to accept only two copies of the report cannot be reasonably be accounted for". One was a copy which went to a since disbanded Defence Department branch.

Hundreds of cases on grid of ASIO
The Australian, Paul Maley, 2016 06 15
Sydney - **There is no such thing as a terrorist watch list, at least not in Australia. Instead, ASIO operates what it calls a "grid" -- a framework for determining the level of surveillance and investigation it applies to any of the hundreds of Islamic radicals who at any one time are of security interest to the agency**. ASIO does not say how many suspected extremists are on the grid. However, the domestic intelligence agency told The Australian yesterday it had more than 400 "high-priority" counter- terrorism investigations on its books. That's more than double the number of serious investigations ASIO was conducting in 2014, - before Islamic State declared its caliphate in Syria and Iraq, an event sources say supercharged extremist sentiment in Australia. ASIO has also said there are about 190 Australians actively supporting Islamic State in some way, although they would almost certainly form part of the 400-odd people being "watched" on the agency's grid. The grid is organised into concentric circles, with subjects moving from the centre, where scrutiny is at its most intense, towards the periphery, where the level of surveillance is gradually scaled down.

Return to Table of Contents/ Retour à la table des matières

New Zealand / Nouvelle-Zélande

NZ military in US for cyber terrorist attack exercise
New Zealand Herald, Staff Writer, 2016 06 19
Wellington - **New Zealand military personnel have jetted into the US for a major cyber terrorist attack exercise alongside other countries of the "Five Eyes" intelligence-**

gathering network. The 16-strong **New Zealand Defence Force (NZDF)** team is joining forces with around 2000 personnel from the Five Eyes partner nations in responding to attacks from a "dynamic and skilled adversary" during Exercise Cyber Flag 16. The large-scale two-week training exercise began on Friday at a United States Department of defence facility in Suffolk, Virginia. To ensure a realistic training environment, participants are using systems that simulate the allied information networks and adversary networks. "Over a two-week period, we will be under constant bombardment from an opposing force that uses a range of tactics," said Wing **Commander Rhys Taylor, Senior National Officer of the NZDF** contingent. While Mr Brownlee would not give specific details about the scale of an expanded cyber security unit, but said it would be "significant"and was likely to work in co-operation with the **Government Communications and Security Bureau (GCSB).**

New Zealand military to join "Five Eyes" cyber attack exercise (Canada)
Xinhua News Agency, Staff reporter, 2016 06 17
Wellington - **New Zealand military personnel are to join a major cyber attack exercise for countries of the "Five Eyes" intelligence- gathering network, the New Zealand Defence Force (NZDF) said** Friday. Sixteen NZDF personnel would join about 2,000 personnel from the Five Eyes nations - - **New Zealand, the United States, Britain, Canada and Australia -- in fending off simulated cyber attacks as part of a training exercise hosted by the U.S**. from June 17 to 30. Major General Tim Gall, Commander Joint Forces New Zealand, said Exercise Cyber Flag 16, being held at a U.S. Department of Defense facility in Suffolk, Virginia, would involve systems that simulated the allied information networks and adversary networks. The teams would respond to the cyber attacks as a coalition, allowing participants to practice interoperability and defence, Gall said in a statement. "Although we are all using the same tools to defend our respective networks, it will be great to learn how other countries are using those tools to defend their systems," he said.

Return to Table of Contents/ Retour à la table des matières

International

China / Chine

Chinese Curb Cyberattacks on U.S. Interests, Report Finds
New York Times, David E. Sanger, 2016 06 21
Washington - **Nine months after President Obama and President Xi Jinping of China agreed to a broad crackdown on cyberespionage aimed at curbing the theft of intellectual property, the first detailed study of Chinese hacking has found a sharp drop-off in almost daily raids on Silicon Valley firms, military contractors and other commercial targets. But the study, conducted** by the iSight intelligence unit of FireEye, a company that manages large network breaches, also concluded that the drop-off began a year before Mr. Obama and Mr. Xi announced their accord in the White House Rose Garden. In a conclusion that is largely echoed by **American intelligence officials**, the study said the change is part of Mr. Xi's broad effort to bring the **Chinese military**, which is considered one of the main sponsors of the attacks, further under his control. As a result, the same political forces that may be alleviating the theft of data from American companies are also responsible for Mr. Xi's stunningly swift crackdown on the Chinese media, bloggers and others who could challenge the Communist Party. "It's a mixed

bag," said Kevin Mandia, the founder of Mandiant, now part of FireEye, which first detailed the activities of a People's Liberation Army cyber-arm, called Unit 61398, that had been responsible for some of the most highly publicized thefts of American technology.

Cybersecurity collaboration to increase
China Daily, Zhang Yi, 2016 06 15
Beijing - **Chinese and US security officials held the second High- Level Joint Dialogue on Cybercrime and Related Issues on Tuesday, pledging to iron out differences and to make fighting cybercrime a part of bilateral cooperation**. The dialogue in Beijing, following the first such conversation in Washington in December, was attended by **Minister of Public Security Guo Shengkun and Suzanne Spaulding, an undersecretary at the US Department of Homeland Security**. Other senior officials from both countries also participated. "Stepping up collaboration on cybersecurity conforms to common interests of both countries. The joint dialogue should be developed into a major channel for communication and cooperation on cybersecurity issues between China and the United States," Guo, who also is a state councilor, said at the dialogue. **US Secretary of Homeland Security Jeh Johnson and Attorney General Loretta Lynch** had been scheduled to attend the meeting, but they withdrew after the mass shooting in Orlando, Florida.

Return to Table of Contents/ Retour à la table des matières

Russia / Russie

Russian Lawmakers Propose Harsher Punishment for Extremism
Moscow Times, Staff report, 2016 06 20
Moscow - **Russian State Duma deputies have proposed an increase in fines and prison sentences for extremist activities,** the RBC news website reported Monday. The amendments to the anti-terrorism bill were approved for a second reading by the Duma's Security Committee. The measures were prepared by United Russia lawmaker Irina Yarovaya and Federation Council member Viktor Ozerov. With the new amendments, inciting hatred or enmity publicly -- via the media or on the Internet -- could carry a fine of up to 500,000 rubles ($7,800). Under the current law, fines of up to 300,000 rubles ($4,700) can be given, RBC reported. The new amendments would allow prison sentences of up to five years, compared to the current maximum of four years. When violence is involved, a fine of up to 600,000 rubles ($9,300) could be given -- compared to a maximum fine of 500,000 rubles under current legislation.

Russia may be behind 'jihadist' cyberattacks
London Daily **Telegraph, Roland Oliphant, 2016 06 20**
Moscow - A jihadist hacking group linked to Isil may be a front for a Russian government cyberwarfare programme against the West, European intelligence chiefs believe. The **Cyber Caliphate**, a hacking collective affiliated to Islamic State of Iraq and the Levant (Isil), came to prominence in April last year when it attacked the French TV5Monde television channel. Jihadist propaganda was plastered over **TV5Monde's Facebook page** and the channel was forced to broadcast pre-recorded programmes. Police linked it to a Russian hacking collective, APT28, raising questions about Kremlin involvement. Now German intelligence services believe Russian secret services may be behind other cyberattacks ascribed to the Cyber Caliphate, Der Spiegel reported.

As Russian Hackers Attack, NATO Lacks a Clear Cyberwar Strategy
New York Times, David E. Sanger, 2016 06 17
Tallinn, Estonia - In **the six months since part of Ukraine's power grid came crashing down, turned off by highly sophisticated hackers, cyberspace allies of President Vladimir V. Putin of Russia have been leaving their mark here in the Baltics and across the sea in Finland and Sweden**. Perhaps to discourage the traditionally neutral Finns and Swedes from growing closer to NATO -- this past week NATO conducted a naval exercise from Finnish territory for the first time -- hackers disabled the **Finnish Ministry of Defense's website**. That was preceded by electronic espionage against a Dutch commission that had concluded that a Russian-made Buk missile brought down a Malaysian airliner two years ago, killing 298 people. And **Germany's intelligence agency, the BND**, recently told American officials that it believed Russian hackers had been behind a cyberattack that destroyed a German steel mill. Here in Estonia, where NATO maintains a center to explore the alliance's cyberspace vulnerabilities and potential responses to attacks, there is a widespread recognition that the Western alliance has yet to develop a strategy to counter Russia's increasingly aggressive action in cyberspace. While there are frequent conferences and papers, there are no serious military plans, apart from locking down the alliance's own networks. **Russia, China and Iran** have increasingly sophisticated offensive cyberforces; NATO has none, and no established mechanism to draw on United States Cyber Command or its British equivalent.

SVR doesn't comment on reports on Russian spy exposed in Spain
Interfax News Agency, 2016 06 16
Moscow—**The Russian Foreign Intelligence Service (SVR) refrains from commenting on the report on a Russian sleeper agent allegedly exposed in Spain.** "We are not commenting on foreign media reports on this matter," Sergei Ivanov, the head of the SVR bureau, told Interfax on Thursday. According to foreign media reports, the first sleeper agent from Russia has allegedly been exposed in Spain. According to the reports, he has worked for 20 years using another person's name and identity. Foreign media reports said the man, named Sergei Cherepanov, lived in Madrid under the name of business consultant Henry Frit.

Russia denies DNC hack and says maybe someone 'forgot the password'
Washington Post, Andrew Roth, 2016 06 15
Moscow - When Russia faces uncomfortable accusations from abroad, the Kremlin normally lashes back with official declarations and scornful comments on state television. But when the Democratic National Committee and cybersecurity experts told The Washington Post that Russian government hackers had stolen an entire database of opposition research on presumptive GOP presidential nominee Donald Trump, officials here met the accusations with little more than a simple denial and a shrug. **"Usually these kinds of leaks take place not because hackers broke in, but, as any professional will tell you, because someone simply forgot the password or set the simple password 123456," German Klimenko, Putin's top Internet adviser, said in remarks carried by the RIA Novosti** state news agency. "Well, it's always simpler to explain this away as the intrigues of enemies, rather than one's own incompetence." "I absolutely rule out the possibility that the government or government agencies were involved in this," Dmitry Peskov, a spokesman for President Vladimir Putin, told journalists in a curt statement.

Russian FSB behind cyberattacks on MH17 investigators in 2015 - German Intelligence
Ukraine Today, Staff report, 2016 06 15
Kiev - **Russian secret services were behind the cyberattack on the servers of the Dutch Safety Board in late 2015**. Hackers, supervised by the FSB, likely attempted to obtain the Dutch report, which named the Russian BUK anti-air system as the weapon behind the airplane

crash. This is according to the German Intelligence. Berlin calls the cyberattacks on the investigators an example of the espionage operations, conducted by Moscow. The German report doesn't indicate, however, if the hackers were successful in their attempt. The Dutch safety board, responsible for the MH17 investigation, also doesn't comment on Russia's alleged involvement in the attacks, according to the Dutch newspaper The Telegraaf.

Russian government hackers penetrated DNC, stole opposition research on Trump
Washington Post, Ellen Nakashima, 2016 06 15
Washington - **Russian government hackers penetrated the computer network of the Democratic National Committee and gained access to the entire database of opposition research on GOP presidential candidate Donald Trump**, according to committee officials and security experts who responded to the breach. The intruders so thoroughly compromised the DNC's system that they also were able to read all email and chat traffic, said DNC officials and the security experts. The intrusion into the DNC was one of several targeting American political organizations. The networks of presidential candidates Hillary Clinton and Donald Trump were also targeted by Russian spies, as were the computers of some GOP political action committees, U.S. officials said. But details on those cases were not available. A Russian Embassy spokesman said he had no knowledge of such intrusions.

Return to Table of Contents/ Retour à la table des matières

Europe

Le terrorisme, casse-tête judiciaire
Le Soir (Belgique), Journaliste maison, 2016 06 21
Bruxelles - La **persistance de la menace djihadiste oblige la Belgique à revoir avec pragmatisme son arsenal juridique**. La **prégnance du risque terroriste a obligé le gouvernement à adapter l'arsenal judiciaire belge**. Depuis plus d'un an, le ministre de la Justice Koen Geens a mis en place une série de mesures pragmatiques pour combler les lacunes d'un Code pénal pas forcément adapté au mode opératoire du terrorisme contemporain. Certaines d'entre elles font débat, qu'elles soient déjà d'application (perquisitions de nuit, possibilité d'écoutes sans intervention d'un juge d'instruction...) ou en projet (allongement du délai de garde à vue à 72 heures). La lutte contre le terrorisme passe aussi par une collaboration judiciaire internationale renforcée, comme l'a rappelé Patrick Dewael, président de la Commission attentats, présente ce lundi à Paris.

Attentats à Bruxelles: trois mois après, la menace terroriste pèse toujours sur la rue de la Loi
RTL Info (France), Journaliste maison, 2016 06 20
Bruxelles - **Trois mois après les attentats bruxellois de l'aéroport national (Zaventem) et du métro Maelbeek, la rue de la Loi reste sous le coup de la menace terroriste**. Retour sur un trimestre de politique fédérale fait de démissions - refusées ou acceptées -, de mesures anti-terroristes, de polémiques et d'opérations policières. Ces derniers jours ont été marqués par les fuites dans les médias sur l'existence présumée d'une menace sur les centres commerciaux et autres lieux publics, le renforcement de la protection de plusieurs personnalités et une importante opération policière de la nuit de vendredi à samedi qui aurait permis de déjouer un projet d'attentat. Le **Premier ministre Charles Michel a appelé au calme et annoncé dans le même temps plusieurs mesures de sécurité complémentaires**. La commission d'enquête prépare ses premières recommandations Un premier train de mesures avait déjà été adopté,

rendant possibles les perquisitions de nuit dans les dossiers antiterroristes, les écoutes téléphoniques dans le cadre de la lutte contre le trafic d'armes, ou encore l'instauration de registres des combattants étrangers.

François Hollande souhaite garantir l'anonymat des policiers
Le Monde, 2016 06 18
Paris - **Quelques jours après le double assassinat de Magnanville (Yvelines), lundi 13 juin, le chef de l'Etat, François Hollande, a voulu donner sans attendre des gages aux forces de l'ordre, meurtries par la perte de deux collègues pris pour cible au nom de l'organisation** Etat islamique (EI). Vendredi 17 juin, lors d'un hommage officiel à Versailles, il a promis que « des mesures seront prises pour garantir leur anonymat, et donc leur protection » . Il entend ainsi éviter que « les policiers et les gendarmes soient identifiés » et « pris pour cibles par les malfaiteurs qu'ils ont mis hors d'état de nuire » . Concrètement, l'exécutif peut vouloir modifier l'article 413-13 du code pénal, qui interdit de révéler l'identité d'un agent appartenant à certains services spécifiques. Cette interdiction est aussi prévue pour les médias à l'article 39 sexies de la loi de 1881 sur la **liberté de la presse et vise, entre autres, les agents de l'unité de coordination de la lutte antiterroriste (Uclat), ceux de la sous-direction antiterroriste (SDAT), de la Direction générale de la sécurité intérieure (DGSI), de l'unité d'intervention de la police nationale (RAID)**, de la brigade de recherche et d'intervention (BRI) ou encore du groupe d'intervention de la gendarmerie nationale (GIGN). « Le président peut vouloir étendre cette liste », théorise la source policière. Et pourrait ainsi obliger les médias à flouter le visage des agents, même s'ils officient sur la voie publique.

State Agency for National Security Chairman Awarded Order of the Star of Italy
Bulgarian News Agency, 2016 09 18
Sofia—Chairman **of the State Agency for National Security (SANS) Dimiter Georgoev has been awarded the Order of the Star of Italy, Officer class, for merits in the development of the bilateral relations and cooperation between Bulgaria and Italy**, SANS said on Friday. The order was handed over by Italian Ambassador to Sofia Marco Conticelli. It is bestowed by decree of the President of Italy on the recommendation of the Minister of Foreign Affairs. Accepting the distinction, Georgiev said that the order is a big recognition for Bulgaria and for the work of SANS.

Bulgaria Sets Up National PNR Unit
Bulgarian News Agency, 2016 09 16
Sofia—**Bulgaria is setting up a National Passenger Name Record (PNR) Unit to counteract terrorism and serious crime, BTA learned from Violeta Ducheva, the project's manager at the State Agency for National Security (SANS).** The unit will start out by recording all air passengers' data. The unit will not have access to passenger data in the air carriers' reservation systems. Air carriers will transfer the PNR to the unit 48 hours before a flight and immediately before the flight, said Ducheva. PNR transfer in advance is already a fact, which enables timely data analysis. PNR were manually processed for certain flights only until recent technological developments made it possible to receive the data in advance, said Ducheva.

Depuis 2012, près d'une dizaine de lois ont renforcé l'arsenal antiterroriste
Le Monde, Journaliste maison, 2016 06 15
Paris - « **Nous avons tiré les leçons des attentats de ces trois dernières années », a martelé le premier ministre, Manuel Valls**, devant les députés, mardi 14 juin. Certains à droite souhaiteraient un nouveau durcissement. Le **premier ministre, Manuel Valls, et son ministre de l'intérieur, Bernard Cazeneuve, n'ont eu de cesse de le répéter, lors des questions au gouvernement à l'Assemblée nationale**, mardi 14 juin. Au lendemain de l'attaque terroriste

contre un couple de fonctionnaires du ministère de l'intérieur, à Magnanville (Yvelines), pas question de répondre par un nouvel arsenal législatif. Pour l'exécutif, tout est déjà en place : « Nous avons tiré les leçons des attentats de ces trois dernières années, beaucoup a été fait, nous nous sommes dotés des moyens d'agir » , a martelé le chef du gouvernement dans l'hémicycle, déroulant ses chiffres sur les hausses d'effectifs et le nombre de lois votées depuis 2012.

Valls prévient que la France sera encore frappée
Agence France-Presse, Journaliste maison, 2016 06 15
Paris - **Manuel Valls a défendu mercredi l'action du renseignement et de l'antiterrorisme en France après l'assassinat d'un policier et de sa compagne lundi soir près de Paris**, tout en prévenant que le pays serait frappé par de nouvelles attaques. Le Premier ministre, qui a écarté l'idée de centres de rétention pour les personnes radicalisées, portée par la droite, a affirmé sur France Inter qu'il n'y avait eu ni "négligence" ni "manque de discernement" dans le suivi du tueur de Magnanville (Yvelines). **"Moi je ne laisserai pas dire qu'il y a eu de la part de nos forces chargées de la lutte contre le terrorisme la moindre négligence ni le moindre manque de discernement, je sais la difficulté de leur tâche", a déclaré M. Valls**, même s'il a reconnu qu'il y avait "toujours un échec" en cas d'attentat. Comme mardi à l'Assemblée nationale, le Premier ministre a de nouveau écarté l'idée de centres de rétention pour les personnes radicalisées n'ayant pas été condamnées, qui seraient "dangereux" et "affaibliraient la lutte contre le terrorisme". Selon lui, la France doit plutôt "poursuivre le travail" engagé par le gouvernement pour "resserrer les mailles du filet" de l'antiterrorisme, en délivrant de nouveaux moyens à la police et au renseignement. Mais le pays "connaîtra de nouveau des attaques", a prévenu le chef du gouvernement.

Report: Chinese hackers target Dutch-German defense company
NL Times (The Netherlands), Janene Peters, 2016 06 15
The Hague - A **group of Chinese hackers for years had access to the systems of a Dutch-German defense technology company, during which time they "definitely" obtained access to technological information and "probably" also had control of the company's network**, the Volkskrant reports based on sources in the intelligence community. According to the newspaper's sources, the company involved is Rheinmetall Defence, based in Ede. The company is one of the world's largest suppliers of defense technology and security systems. Among other thing, the company produces materials for armored vehicles. Delft based digital **security company Fox-IT** discovered the hack when they found unknown malicious software in the company's systems in the autumn of last year. After months of investigation, they managed to identify the hackers as Chinese based on the language settings in the malware, the targets selected ad the working method. The Volkskrant sources stated that the hackers sent English-language emails from fake email addresses to the Ede company's employees. The emails seemed to contain news about the Dutch- German cooperation. The malware was installed once the emails were opened.

Switzerland snubs plans to strip terrorists of nationality
The Local (Switzerland), Staff report, 2016 06 15
Bern - The **measure put forward by Swiss president and chairman of the country's populist Swiss People's Party Toni Brunner was rejected by the Swiss senate** to the tune of 27 votes against and 12 in favour. The move was initially approved by MPs in the Swiss lower house in a vote held three weeks after the Paris attacks of November 2015. But in a debate on the issue held this week Swiss senators said the wording of the proposal was too vague, and insisted the current legislation was effective. **Current rules allow allows for the stripping of Swiss nationality if a person's "behaviour is a serious threat to Swiss interests or**

reputation". The law dating back to 1953 has never been used. However, a Swiss-Italian teenager suspected of joining terrorists in Syria could have his Swiss nationality withdrawn in what would be the first such case in Switzerland.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Former Shin Bet head 'bursts myth' on cyber hackers who attack Israel
Jerusalem Post, Yonah Jeremy Bob, 2016 06 21
Jerusalem - In his first big speech **since stepping down as head of the Shin Bet (Israel Security Agency) last month, Yoram Cohen departed from conventional wisdom Tuesday saying he wanted to "burst the myth of retribution," explaining that Israel always eventually learns who to hold responsible for attempted cyber hacks**. Conventionally, most government and private sector officials say that one of the puzzles of cyber warfare is identifying who initiated a cyber attack. Cohen's statements, made at Tel Aviv University's international cyber conference, indicated that the Shin Bet's abilities to decipher who cyber attacks Israel are more advanced than has been previously known. He headed the Shin Bet from May 2011 until May 2016. The former Shin Bet director listed Israel as facing three main cyber threats: computer network attacks, computer exploitation attacks and social media influence attacks.

Iran Intelligence University calls for applicants
Iranian Labour News Agency (via BBC Monitoring Middle East), 2016 06 18
Tehran— **Iran's University of Intelligence and National Security (UNIS**) has announced its postgraduate student recruitment preferences, offering a range of required topics and competitive bursaries for applicants under the age of 27. According to the latest released booklet outlining different universities' entry subjects, the UNIS announced the following topics of interest for its new cohort of students, including: management of intelligence; protection of intelligence; Iranian security studies; security research; security and criminology; engineering of security and telecommunication; engineering of information and security technology. In addition, the following sub-topics will be taught: coding; cyber security; bioterrorism and crisis management.

Intelligence chief warns of growing gaps between Israel, neighbors
Times of Israel, Judah Ari Gross, 2016 06 17
Jerusalem - Since the Arab Spring in 2011, Israel has gotten stronger, more stable and wealthier than its neighbors. But that's not necessarily something to be proud of -- it's something that should be worrisome, according **to Military Intelligence chief Maj. Gen. Herzi Halevy**. His speech gave a general overview of the region, but did not reveal any information not previously released by the Israel Defense Forces. He **touched on the Syrian civil war, Iran's nuclear ambitions, Hezbollah in Lebanon, Hamas in Gaza, terror in the West Bank and the Islamic State group. Each of these threats has existed for years, but one area of concern Halevy touched on was the growing disparity between Israel and its neighbors**. On the one hand, Israel's status as a strong, stable democracy in the Middle East is something that should be treasured and not forgotten. Economic strife can give rise to religious extremism and terrorism, the Military Intelligence chief warned.

Intelligence minister warns 'megalomanic' Hezbollah chief
Times of Israel, Stuart Winer, 2016 06 17

Jerusalem - **Intelligence Minister Yisrael Katz launched a scathing attack on the Hezbollah terror group's leader, calling Hassan Nasrallah a "megalomaniac" with no concept of reality and warning that Lebanon would be "ruined"** in a future conflict between the IDF and Hezbollah. "Hezbollah continues to be the primary non-state threat, not only to Israel but also to Lebanon," he told the Herzliya Conference, an annual seminar reviewing Israel's security. He added that a conflict with the Lebanon-based Shiite group could be triggered by a minor incident due to "the megalomaniac character of the organization's leader, Hassan Nasrallah, a fanatical personality who lacks any conception of reality except, perhaps, anything to do with protecting his personal security." Hezbollah is believed to have an arsenal of more than 100,000 missiles and rockets, along with weapons systems "that they never had before," Halevy said.

Dam, State Security threaten to further cripple government
The Daily Star, Hussein Dakroub, 2016 06 16
Beirut— The Cabinet will meet Thursday amid lingering differences over the controversial Janna dam project and the State Security agency, two contentious issues that threaten to further cripple the work of an already paralyzed government. The meeting also comes against the backdrop of the resignation of two Kataeb Party ministers in a dramatic development that will further weaken government productivity. **The Cabinet is also expected to address the long-running dispute over the leadership of the State Security agency.** The agency has been plagued by a funding row and a leadership struggle between the agency's head, Maj. Gen. George Karaa, and his deputy, Brig. Gen. Mohammad Tufayli. Karaa is a Greek Catholic, and his duties overlap with those of Tufayli, a Shiite. In effect, the latter has the same powers as the agency's head. This has ultimately caused a sectarian-related issue. All the ministers had agreed in April to task Salam with negotiating a solution to the crisis which has deepened divisions within the Cabinet

Iranian-British Female Spy Arrested in Tehran's Imam Khomeini Airport
Fars News Agency, 2016 06 16
Tehran - The **Islamic Revolution Guards Corps (IRGC) announced in a statement on Wednesday that it has arrested an Iranian-British national at Imam Khomeini International Airport for spying charges**. Nazanin Zaghari was arrested by the IRGC's Kerman Province Intelligence Department at Imam Khomeini International Airport on April 3 while she was trying to leave the country and was later transferred to Kerman for her involvement in a regime change plot, the IRGC statement read.

Counter-terror bill passed into law
Israel National News, 2016 06 15
Jerusalem— The K**nesset passed on Wednesday an anti-terror bill proposed by Justice Minister Ayelet Shaked, with 57 votes in favor and 16 against.**The legislation, which increases the punishments for organizers of terrorism and enables courts to convict terror cell leaders more easily, replaces a series of emergency provisions used since the establishment of the state. According to the law, those involved directly or indirectly in organizing terror cells could face up to 25 years in prison, while leaders of terror cells would face a mandatory life sentence. Terrorists who use chemical, biological, or radioactive weapons during attacks would also face mandatory life sentences. Under the new law the Prime Minister and **Defense Minister will now be able to declare groups terrorist organizations, based upon the recommendation of the Shin Bet security agency** and in consultation with the Attorney General.

Israeli parliament approves contentious anti-terror bill
Xinhua News Agency, 2016 06 15

Jerusalem— The **Israeli parliament approved on Wednesday a controversial anti-terror bill which aims to increase penalties on terror-related moves and qualify more activities as part of its definition of terrorism.** The bill, which has been under discussion by the Knesset's Constitution, Law and Justice Committee since 2010, was recently adopted and advanced by Israel's Justice Minister Ayelet Shaked from the ultranationalist Jewish Home right-wing party. Fifty-seven lawmakers voted in favor of the bill, while 16 lawmakers objected to it. The promotion of the bill in recent months came amid a wave of violence between Israelis and Palestinians, which started in October, claiming the lives of 32 Israelis and 205 Palestinians since. The bill extends the state and its security authorities' powers against potential terror suspects and expands the definition of what qualifies as terrorist-related activities.

Return to Table of Contents/ Retour à la table des matières

Asia / Asie

Park instructs government to exhaustively check terror response capabilities
Yonhap News Agency, Staff reporter, 2016 06 21
Seoul - **President Park Geun-hye on Tuesday instructed her government to "exhaustively" check the country's terror response capabilities, warning that North Korea, with direct or indirect links to international terrorist groups**, could mount attacks against the South. Her remarks came a few days after the **National Intelligence Service** revealed that the Islamic State jihadist group had designated some U.S. military installations here and a South Korean citizen as targets for attacks. "There are concerns over the possibility of the North -- with direct or indirect links to terrorist groups -- launching attacks (against South Korea)," she said during a Cabinet meeting at the presidential office **Cheong Wa Dae**. **"There has continuously been intelligence about terrorist attempts to abduct our citizens**, while the North has been posting videos explicitly threatening to blow up Cheong Wa Dae and the government complex," the chief executive added, underscoring that South Korea is no longer safe from terrorism. Park ordered Cabinet ministers to ensure that the anti-terrorism center, launched earlier this month under the prime minister's office, is equipped with sufficient measures to properly respond to diverse scenarios of terrorist attacks. Over the last five years, South Korean authorities have found and deported some 50 foreigners with links to terrorist organizations. The authorities have also caught two South Koreans who attempted to join such entities.

S. Korea to hold anti-terrorism ministerial meeting
Yonhap News Agency, Staff reporter, 2016 06 21
Seoul - The **South Korean government said Tuesday it will hold a special anti-terrorism meeting amid rising threats from overseas terrorist groups**. The date of the meeting has not been set, but it will be chaired by **Prime Minister Hwang Kyo-ahn** with related ministers to take part in the discussions. The gathering comes as reports indicate the militant Islamic State (IS) group has made threats against South Korea. **South Korea's National Intelligence Service earlier said IS has been calling for terrorist attacks through messaging services by revealing the locations of key military bases and individuals associated with them around the globe.** The spy agency said the list included some U.S. military bases in South Korea, as well as a staff worker of a local civic group. South Korea currently operates an anti-terrorism center under the prime minister's office after the country's first comprehensive anti-terrorism bill went into effect this month. Related to the meeting, the National Assembly's Intelligence Committee said the government aims to come up with countermeasures to cope with the threats made by IS.

Wolesi Jirga approves Stanikzai as spymaster
Pajhwok Afghan News, Khawaja Basir fitri, 2016 06 20
Kabul - The **Wolesi Jirga -- or the lower house of parliament -- on Monday approved Mohammad Masoom Stanikzai as National Directorate of Security (NDS) chief**. Stanikzai was introduced as President Ashraf Ghani's choice for spymaster along with the defence minister-designate to the Wolesi Jirga for the trust vote on June 8. After Stanikzai outlined his programmes to the house, of the 224 lawmakers present, 161 voted in his favour. He has been serving as acting defense minister for the past one year.

Afghan MPs confirm new defence minister, intelligence chief
Agence France-Presse, 2016 06 20
Kabul—**Afghan lawmakers on Monday approved President Ashraf Ghani's nominees for defence minister and intelligence director**, two crucial posts that sat vacant for months as the country struggles to rein in an ascendant insurgency. The confirmations came as attacks left at least 23 people dead across Afghanistan Monday and wounded dozens more, as the Taliban's resurgence continues to raise serious questions about the ability of Afghan forces to hold their own without the support of US-led NATO troops. MPs voted for Abdullah Habibi, formerly a senior official in the defence ministry who holds the rank of army general, to become its new minister. **Mohammad Masoom Stanekzai, a former top official in the government body overseeing the country's peace process who has worked to bring the Taliban to the negotiating table, was named head of Afghanistan's National Directorate of Security (NDS) intelligence agency.**

South Korea spy agency bars 12 waitresses from North from court
Reuters, 2016 05 20
Seoul— A **South Korean court has ordered the spy agency to make 12 North Korean waitresses who defected to the South available to answer whether they defected of their free will,** but the agency said they would not be presented in court. The **National Intelligence Service** is holding the 12 women who fled a restaurant run by the North in China. An official at the service said on Monday only the women's "legal representatives" would attend the court hearing on Tuesday. The court order came after a group of lawyers filed a petition for a hearing to determine whether the 12 were being held against their will.

ISIS threat to U.S. air bases, South Korea intelligence agency warns
CNN.com, Paula Hancocks, 2016 06 20
Seoul - **ISIS has collected information on 77 U.S. and NATO air force facilities around the world and is calling on supporters to attack them, according to South Korea's intelligence agency**. The terror group has also released information on individuals in 21 countries, including the personal details of one employee of a South Korean welfare organization, the **National Intelligence Service** (NIS) said in a statement Sunday. That person is now under protection, the agency said. The NIS says ISIS' hacking organization, the United Cyber Caliphate, collected details of U.S. air force units in South Korea including Osan Air Base, and addresses and Google satellite maps have been released through the Telegram messaging service.

Police seek to legalize private investigators
The Korea Times, 2016 06 19
Seoul—A group of senior and retired police officers have set up an **organization in a bid to legalize private investigators,** according to police, Sunday. This is the first time that former and incumbent police officers are seeking to allow private detectives in Korea, while previously

demands have usually come from the so-called “errand centers,” companies that work for individual clients. According to the **National Police Agency (NPA)**, a notice has been recently posted on the police’s intranet to recruit members for the organization. It is aimed at studying overseas private investigator systems with the final goal of having the National Assembly legalize the profession. “Police cannot intervene actively in many civil cases such as disputes over medical malpractice and insurance, sometimes because of manpower or budget shortages,” according to an officer at Jongno Police Station. “We believe that private investigators would meet the demand by clients in such cases,” he said.

Anti-terror official likely to be Indonesia's youngest top cop
Nikkei Report, 2016 06 18
Jakarta— **President Joko Widodo's recent nomination of Tito Karnavian to lead the Indonesian police has drawn applause from many, with Karnavian's clean track record and long counterterrorism experience bringing hope for reforms amid the growing threat of global terrorism**. Widodo on Wednesday submitted a nomination letter to Parliament, which will hold a "fit-and-proper test" to decide the eligibility of Karnavian -- now the head of Indonesia's anti-terrorism agency -- to replace National Police chief Badrodin Haiti, who will soon reach retirement age. "I'm hoping Commissioner Gen. Tito will be able to enhance the professionalism of the National Police and also improve the quality of law enforcement -- especially against drug crimes, terrorism and corruption," Widodo told reporters Thursday. Karnavian's nomination has surprised many. **At 51, he is the youngest of eight three-star generals on the police force originally considered for the top job**.

Establishing new spy agency would require law revision
Jakarta Post, Marguerite Afra Sapiie, 2016 06 17
Jakarta - The **State Intelligence Law would need to be revised if the Defense Ministry decided to form its own spy body, National Intelligence Agency (BIN) chief Sutiyoso said on Thursday**. "The law states that the actor in defense intelligence is within the Indonesian Military, namely the military's Strategic Intelligence Agency [BAIS]," Sutiyoso told journalists. The Defense Ministry has yet to contact BIN to deliberate the plan, but Sutiyoso warned that the consequences of establishing a new agency could burden the ministry in terms of budget and human resources. He said the central intelligence committee - which gathers all spy bodies in the country including those under the National Police, the Indonesian Military, the Attorney General's Office and numerous ministries - met and coordinated at least once a month.

New spy agency is unnecessary: Vice President Jusuf Kalla
Jakarta Post, News Desk, 2016 06 16
Jakarta - The **Defense Ministry's plan to establish its own intelligence agency is unnecessary, Vice President Jusuf Kalla says on Tuesday**. Even though the government had yet to make comprehensive discussion about the realization of the plan, Kalla asserted that the newly spy agency was in-fact not an urgency in the present. "[The government] haven't discussed anything, but I can assure that we don't need too much agencies in the meantime," Kalla said as quoted by kompas.com. The officials should initially conduct in-depth assessment on the intelligence body planning since it is feared that the newly spy body would overlap with the **National Intelligence Agency** (BIN), Kalla said. Earlier, Defense Minister Ryamizard Ryacudu announced the plan to establish an intelligence body under the Defense Ministry, which aimed to dig deeper on information needed for the country's defense interests.

Iran responds to letter about Indian spy
Pakistan Dawn, Iftikhar A. Khan, 2016 06 16

Islamabad - The **Iranian government has finally responded to a letter written by the interior ministry seeking investigation into Indian intelligence agency RAW's network in Iran**. According to sources, the response was handed over to Interior Minister Chaudhry Nisar Ali Khan by **Iranian Ambassador Mehdi Hunerdoost** who called on him here on Wednesday. According to an official statement, progress in expansion of cooperation in a number of areas, including security, was reviewed during the meeting which also took stock of the situation prevailing in the region. The contents of the Iranian response were not shared with the media. Chaudhry Nisar made it clear that no third country could influence relations between Pakistan and Iran. He stressed the need for strengthening monitoring of the border between the two countries and timely exchange of information.

Return to Table of Contents/ Retour à la table des matières

Africa / Afrique

Dasuki loses bail bid at Appeal Court
Nigerian Tribune, 2016 06 16
Abuja— **The Court of Appeal, Abuja division, has dismissed the appeal of former National Security Adviser (NSA), Colonel Muhammad Sambo Dasuki** (retd), seeking order of the appellate court to compel the Federal Government to allow him to enjoy the bail granted him by an Abuja High Court. The appellate court, in its judgment delivered by Justice Abdul Aboki, held that the appeal lacked merit and substance and consequently, dismissed it. In an unanimous judgment of the full panel of the court, it upheld the submission of the Economic and Financial Crimes Commission (EFCC), which put Dasuki on trial, that it was not in contempt of any court order because the re-arrest of the appellant in December last year, was not at its instance.

Return to Table of Contents/ Retour à la table des matières

Americas / Amériques

Olympic Brazil detects IS radical posts in Portuguese
Agence France-Presse, 2016 06 17
Rio de Janiero—Authorities in this year's Olympic host Brazil detected **users exchanging messages in Portuguese linked to the Islamic State extremist group in an online web forum, intelligence services said Friday**. The warning raised security concerns about the potential existence of sympathizers of the armed group in Brazil, which was previously thought to be relatively free of Islamic extremism. Pre-Olympic jitters had already risen after a French jihadist warned on Twitter after deadly attacks in France last November that Brazil was the "next target." The **Brazilian Intelligence Agency** said in a statement Friday that it "confirms the existence of a group and its way of operating" online with jihadist messages. It said the group was found on Telegram, an online messaging application.

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

29-06-2016 to/au 05-07-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Watchdog condemns lack of diversity among CSIS senior staff
Globe and Mail, Laurent Bastien, 2016 07 02
Ottawa - The **federal government's human-rights watchdog has repeatedly admonished the Canadian Security Intelligence Service over a lack of diversity in its upper echelons**, according to newly disclosed reports. Records obtained by The Globe and Mail show that the Canadian Human Rights Commission has conducted two employment equity audits of CSIS over the past decade and, on both occasions, the spy agency was criticized because it had not hired a sufficient number of visible minorities, people with disabilities and indigenous Canadians. The 2014 and 2011 audits found that none of CSIS's senior managers were indigenous or visible minorities, and only 17 per cent are women, a decrease of 13 per cent since 2009. "Your organization has a lower overall EE [employment equity] result when compared to separate agencies and is therefore considered to be a less successful employer with respect to EE," the commission wrote, urging the agency to close gaps in its hiring practices. One of its main challenges, the commission noted, was to increase the diversity of its managerial staff. Formed three decades ago from a former **RCMP intelligence division**, CSIS is a $500-million-a-year organization with 3,000 employees.

Data encryption hampering police work
Toronto Star, Alex Boutilier, 2016 07 02
Toronto - The **growing popularity of programs that protect online privacy is creating a barrier for police and security agencies' ability to intercept and use data**, documents obtained by the Star suggest. Officials warned **Public Safety Minister Ralph Goodale** in November that encryption - the ability to mask communications so only the intended recipients can make sense of the message - is hindering their ability to use online communications in investigations. "Canadians are increasingly using mobile phone networks, the Internet and other electronic means to communicate and execute transactions with each other," read the documents, heavily censored and stamped "secret." "This has led to a significant gap between the technologies available for criminal exploitation and our means to enforce Canada's laws and keep Canadians safe." The Star requested an interview with Goodale to discuss these issues, but the minister was unavailable over the past two weeks. His office noted that the minister recently addressed the encryption debate in a speech at the University of Regina.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

CIA Chief Blasts 'Stubborn' Kim Jong-un
Chosun Ilbo, 2016 07 05

Seoul--**Central Intelligence Agency Director John Brennan said North Korean leader Kim Jong-un is "exceptionally stubborn and not a very good listener,"** according to Voice of America last Friday.Brennan made the remark at the Council on Foreign Relations in Washington last Wednesday."North Korea remains my top concern in terms of nuclear proliferation, as the country leader Kim Jong-un fails to recognize that the rest of the world won't accept his pursuit of nuclear weapons," Brennan said.He added that the U.S. wishes to help North Korea emerge from isolation and to support the country's people. But he warned that Kim must realize that his pursuit of nuclear weapons and missiles harms the longevity of his rule.(full report).

CIA caught off guard by Islamic State's rise in post-Moammar Gadhafi Libya
Washington Times, Rowan Scarborough, 2016 07 04
Washington - **CIA chieftains were caught off guard by the spiraling Islamic violence in postwar Libya,** suddenly realizing that analysts had never brainstormed what the country would look like and that the White House had not asked. The agency also acknowledged in a classified report that Moammar Gadhafi, Libya's U.S.-deposed dictator, had long suppressed a variety of radical Islamic groups, including al Qaeda, from taking root in his country and endangering North Africa. The CIA views are among the interviews and documents compiled by the House select committee that investigated the Islamic extremist attacks on the U.S. diplomatic mission in Benghazi and on a nearby CIA base on Sept. 11, 2012.

Transgender People Will Be Allowed to Serve Openly in Military
New York Times, Matthew Rosenberg, 2016 07 02
Washington - **Defense Secretary Ashton B. Carter on Thursday removed one of the final barriers to military service by lifting the Pentagon's ban on transgender people serving openly in the armed forces.** "Effective immediately, transgender Americans may serve openly," Mr. Carter said. "They can no longer be discharged or otherwise separated from the military just for being transgender." The decision pushes forward a transformation of the military that Mr. Carter has accelerated in the last year with the opening of all combat roles to women and the appointment of the first openly gay Army secretary.

5 issues the U.S. military must still address about allowing transgender service
Washington Post, Dan Lamothe, 2016 07 02
Analysis: **Defense Secretary Ashton B. Carter repealed the U.S. military's ban on transgender service members Thursday, but the Pentagon still has a number of decisions to sort through in the coming months.** In his remarks, Carter focused heavily on why he thought the repeal was the right thing to do, noting there are presently at least 2,500 transgender troops on active duty. But he also laid out a multi-layered implementation process that requires numerous decisions in coming months by service chiefs and senior civilian officials in the Pentagon alike. They include: 1. Forming rules for restrooms, showers and other day-to-day functions Senior defense officials, speaking on the condition of anonymity to speak frankly, said after Carter's announcement Thursday that commanders will be given wide latitude to decide how to best equip their facilities for transgender service. In many cases, the officials said, that could be as simple as putting up new privacy curtains in some bathrooms or setting specific shower hours for different kinds of troops.

Civilian bomb squad cleared in Pentagon pay error
Washington Post, Dan Lamothe, 2016 07 02
Washington - The **Pentagon has decided that members of its civilian bomb squad will not be obligated to pay back up to $173,000 that it says each of them was erroneously paid since the unit was established in 2008**, a defense official said. The Defense Office of

Hearings and Appeals waived the debts "after completion of the normal waiver-of-debt process," said Air Force Lt. Col. Eric Badger, a Pentagon spokesman. The decision was acknowledged late Wednesday, a day after The Washington Post published an article that detailed how members of the bomb squad faced potential financial ruin after the Pentagon decided in 2015 that it had incorrectly paid them a 25 percent hazardous-duty incentive for years. The waivers were completed despite some members of the bomb squad expecting that their cases would not be heard for several more weeks.

Federal Agencies Continue to Shed Security Clearance Holders
Government Executive, Eric Katz, 2016 06 30
Washington—The **federal government cut the number of individuals holding security clearances by a quarter of a million people in fiscal 2015**, according to a new report, marking the second consecutive year agencies have successfully followed through on an Obama administration goal to trim the cleared population. **The Office of the Director of National Intelligence report showed agencies continuing to reduce what had been a growing population of federal employees and contractors who hold clearances.** The number of people with clearances had ticked up in each of the first three years since ODNI began measuring it in 2011. The total reduction in 2015 continued a multi-year trend of federal agencies doling out fewer new security clearances each year. About 4.2 million individuals held security clearances as of Oct. 1, 2015, down 6 percent from the same time in 2014. The cleared population has fallen by about 17 percent since fiscal 2013. The new approvals for security clearances -- including first-time issuances as well as reinvestigations -- dropped 4 percent to 639,000.

Brexit crisis contributing to 'daunting' US security challenges, CIA director says
The Guardian (London), Staff report, 2016 06 30
Washington - The **US is facing its most daunting national security challenge in a generation after the European Union was plunged into "crisis" by Britain's vote to leave**, the head of the **CIA** warned on Wednesday. **John Brennan** insisted that Brexit would not undermine cooperation with MI6 in the fight against terrorism, but suggested that the EU, a bulwark of peace and stability since the fall of the Berlin wall, would now be preoccupied with the UK's departure. "In the 36 years since I first entered government, I have never been witnessing a time with such a daunting array of challenges to our nation's security," Brennan told the Council on Foreign Relations in Washington. "Notable among those challenges is that some of the institutions and relationships that have been pillars of the post-cold war international system are under serious stress. "Of all the crises the EU has faced in recent years, the UK vote to leave the EU may well be its greatest challenge. Brexit is pushing the EU into a period of introspection that will pervade virtually everything the EU does in the coming weeks, months and even years ahead," he said.

CIA Chief Says Brexit Will Test Europe For Years
Wall Street Journal, Damian Paletta, 2016 06 30
Washington - The **decision by British voters to leave the European Union will test the continent for some time, the head of the Central Intelligence Agency said Wednesday**, warning that "decision-making and forging consensus" in the EU will become "much harder." "Brexit is pushing the EU into a period of introspection that will pervade virtually everything the EU does in the coming weeks, months, and even years ahead," **CIA Director John Brennan** said in remarks at the Council on Foreign Relations. Voters in the U.K. last week approved a referendum measure to leave the European Union, a decision that has shocked global market and allies. It still hasn't been determined precisely how or when the U.K. will exit the EU, and some are suggesting the outcome is reversible, but Mr. Brennan suggested it is only a matter of

time. "No member-state has ever left the Union, so Europe is entering a period of uncertainty as the U.K. and the EU take stock of the situation and begin staking out their negotiating positions," he said. Mr. **Brennan said Brexit, as the country's EU departure is commonly called, won't impede intelligence-sharing arrangements between U.S. and British officials**.

U.S. Probes Chinese Ownership of CIA-Linked Insurance Company
Newsweek, Jeff Stein, 2016 06 30
New York - **Federal investigators are taking a close look at the Chinese ownership of an American insurance company that has been selling legal liability insurance to senior CIA, FBI and other intelligence officials** and operatives for decades. The company, Wright USA, was quietly acquired late last year by Fosun Group, a Shanghai-based conglomerate led by Guo Guangchang, a billionaire known as "China's Warren Buffett" who has high-level Communist Party connections. The links between Guo and Wright USA came under scrutiny by the Treasury Department's Committee on Foreign Investment in the United States, as well as the **Office of Director of National Intelligence**, the coordinating body of all U.S. spy agencies, soon after Fosun announced the purchase of Wright's parent company last November. The FBI has also launched a criminal probe into whether the company made "unauthorized disclosures of government data to outsiders," according to a well-placed source, who like others, spoke to Newsweek on condition of anonymity because the information was sensitive. (The FBI declined to comment, and Fosun denies the FBI has asked it for any documents.)

CIA chief Brennan looks at Turkish attack and sees a warning for Americans
Yahoo News, Daniel Klaidman, 2016 06 29
Washington - Four hours after three suicide bombers killed at least 41 people and wounded hundreds more at **Istanbul's Ataturk airport, CIA Director John Brennan said the attacks bore the grim hallmarks of ISIS and warned that the fanatically violent Islamic terrorist group wants to conduct similar large-scale attacks in the United States**. "I am worried from the standpoint of an intelligence professional who looks at the capabilities of Daesh ... and their determination to kill as many as people as possible and to carry out attacks abroad," Brennan said in an exclusive interview at CIA headquarters with Yahoo News. Brennan credited effective homeland security measures and intelligence for the fact that ISIS has been unable to attack America directly -- the Orlando and San Bernardino shootings were carried out by radicals inspired by ISIS but not under its control -- but he believes the group will keep trying to penetrate American defenses.

Intelligence Community Held 12 Diversity and Inclusion Seminars Last Year
Washington Free Beacon, Elizabeth Harrington, 2016 06 29
Washington - The **intelligence community held 12 seminars on diversity and inclusion last year, including "unconscious bias" training and a women's summit that focused on "emotional intelligence**." An employee resource group on "Islamic Culture" is also offered for employees of the National Security Agency to provide "cultural sensitivity." The Office of the Director of National Intelligence released its annual demographics report this month, which detailed the number of community-wide events the intelligence community held during fiscal year 2015.

CIA taps huge potential of digital technology
BBC News, Gordon Corera, 2016 06 29
London - At **CIA headquarters in Langley, the office of the director of digital innovation sits next to the agency's in-house museum filled with artefacts from its history**. Featuring heavily are gadgets such as early secret cameras and bugging devices that would not appear out of character in a Hollywood film. The line-up makes the point that even though the CIA is an

intelligence agency whose central mission has been to recruit people to provide secrets, technology has always had a crucial role. **Andrew Hallman - who runs the recently created Directorate of Digital Innovation -** has the job of making sure that the new digital world works to the CIA's advantage rather than disadvantage.

US Increasingly Focused on Social Media to Weigh Terror Threats
Voice of America, Chris Hannas, 2016 06 29
Washington - The **United States government has become increasingly focused on the idea of examining social media posts in order to make determinations about who represents a security threat to the country**. The latest example is a proposal from the **Customs and Border Protection arm of the Department of Homeland Security** to ask foreign travelers to disclose information about their accounts on services like Facebook and Twitter. It would appear as an optional question on the form people fill out either upon arrival or presubmit online with information such as their name, address, phone number and the names of countries they have visited since 2011. It would also only apply to travelers from the 38 countries allowed visa-free entry into the U.S. "**Collecting social media data will enhance the existing investigative process and provide DHS greater clarity and visibility to possible nefarious activity** and connections by providing an additional tool set which analysts and investigators may use to better analyze and investigate the case," the proposal says.

The Hunter
The Intercept, Peter Maass, 2016 06 28
Washington - The message arrived at night and consisted of three words: "Good evening sir!" The sender was a hacker who had written a series of provocative memos at the **National Security Agency. His secret memos had explained -- with an earthy use of slang and emojis that was unusual for an operative of the largest eavesdropping organization in the world** -- how the NSA breaks into the digital accounts of people who manage computer networks, and how it tries to unmask people who use Tor to browse the web anonymously. Outlining some of the NSA's most sensitive activities, the memos were leaked by Edward Snowden, and I had written about a few of them for The Intercept. There is no Miss Manners for exchanging pleasantries with a man the government has trained to be the digital equivalent of a Navy SEAL. Though I had initiated the contact, I was wary of how he might respond. The hacker had publicly expressed a visceral dislike for Snowden and had accused The Intercept of jeopardizing lives by publishing classified information. One of his memos outlined the ways the NSA reroutes (or "shapes") the internet traffic of entire countries, and another memo was titled "I Hunt Sysadmins."

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

I Spy: GCHQ reaches out to Mumsnet generation in new recruitment drive
Yorkshire Post, Staff report, 2016 07 04
Scarborough - The **director of GCHQ has announced a multi-million pound investment to transform a Yorkshire base into the North of England's training hub as the spy agency looks to recruit more middle-aged women from the Mumsnet generation.** The £42m package was outlined yesterday by Robert Hannigan, the director of the UK's Government

Communications Headquarters, on a visit to its base on the outskirts of Scarborough. The base is to be the training and skills hub of the northern network of GCHQ, the intelligence and security organisation which monitors radio and signals communications and protects against a wide range of threats, from terrorism and cyber crime to child sex exploitation and hacking. Along with **MI5 and MI6,** there will be an emphasis on recruiting more women, especially those who middle-aged and also mid-career, dubbed "Jane Bonds", and the organisation has used Mumsnet for that purpose. Of the £42m that is being invested in the next four years, £30m will go towards the base's infrastructure - modernising and improving the current environment - and £12m to skills training.

Kincora MI6 agent 'was aware of abuse'
Belfast Telegraph, David Young, 2016 07 02
London - **At least one MI6-run agent was aware of sexual abuse being committed in a notorious Belfast boys' home, according to one of the agency's historic intelligence documents.** A classified MI6 note containing the claim about the Kincora abuse scandal was presented in evidence as a senior ranking MI6 officer was questioned at Northern Ireland's Historical Institutional Abuse inquiry. But the anonymised deputy director of the Secret Intelligence Service (MI6), referred to as officer A as he testified via video-link, rejected any suggestion his organisation was aware of the abuse. He told the inquiry panel that an extensive trawl of MI6's files could find no other documentary evidence to corroborate the 1989 note. "We have found nothing that was written at the same time that justifies that assertion or nothing in our subsequent records that backs up that assertion," he said.

Chilcot 'will blame MI6 chief' for Iraq dossier
London Times, Staff Writer, 2016 07 02
London - **Spy chiefs in office during the Iraq war will be "fed to the wolves" when the Chilcot inquiry delivers its findings next week**, it has been claimed. **Sir Richard Dearlove, the former head of MI6**, will be strongly criticised for intelligence given to Tony Blair that laid the groundwork for the "dodgy dossier" claims about Saddam Hussein's weapons of mass destruction, a source told the Daily Mirror. Mr Blair is also expected to be condemned as Sir John Chilcot reports that the former prime minister sidelined experts and the cabinet in order to make the case for war. The report, which has taken seven years to compile, is also expected to expose a failure by British embassy staff in Washington to pass on misgivings from the CIA about preparations for the reconstruction of Iraq.

Return to Table of Contents/ Retour à la table des matières

Australia/ Australie

Police boost surveillance at Australian airports as experts call for new security strategy
The Australian, Mitchell Bingemann, 2016 06 30
Canberra - **Australian Federal Police have been ordered to increase their presence at the nation's largest airports following yesterday's terrorist attacks in Turkey**. The Office of Transport Security -- which regulates security at aviation and maritime hubs -- briefed airlines and airports following yesterday's attacks at Istanbul's Ataturk International Airport, while the AFP enhanced its surveillance in the publicly accessible areas of Australia's major airports.Australia remains on a "high" level of alert, with ASIO maintaining its national terrorism threat level as "probable". "The Department of Infrastructure and Regional Development has

encouraged industry participants to review security in public areas," a spokesman said. "As aviation is a global industry, the government is also in contact with its international counterparts. This is so we can co-ordinate actions and work to ensure that the aviation sector does not grind to a halt as it is critical for our economy and way of life.

Return to Table of Contents/ Retour à la table des matières

New Zealand/Nouvelle-Zélande

Andrew Kibblewhite : First responder
The Dominion Post, Tracy Watkins, 2016 07 02
Column : Did you want to talk about Five Eyes? **Andrew Kibblewhite**, head of the Department of Prime Minister and Cabinet, is asking the question as I'm packing up, tape recorder already turned off and halfway to my pocket. Oh, yeah. Five Eyes. Kibblewhite and I have just finished a 40-minute interview about security and somehow it never came up. But it was clearly on Kibblewhite's list of talking points. This fact alone speaks volumes about how far the national security apparatus has moved in recent years. Five Eyes used to be the club that dare not speak its name; an elite grouping of world "powers" through which much of the world's heavy duty intelligence passes. It's largely thanks to circumstances of geography and historic alliances that we are there at all, Five Eyes' smallest member. There is another club that used to fall in the same secret category - ODESC, or, to go by its more mundane title, the Officials Committee for Domestic and External Co-ordination, chaired by Kibblewhite. **Kibblewhite is among the new breed of public servant heading these previously invisible agencies. In place of the shadowy faces of the past are the likes of Security Intelligence Service boss Rebecca Kitteridge, and new Government Communications Security Bureau boss Andrew Hampton** - personable, smart and refreshingly open, though critics argue that's just clever window dressing. But Kibblewhite has kept a lower profile during that period. Some of that may be tactical - he has made the headlines previously for unrelated reasons, including his offer to Key to resign when it was revealed he knew about Parliamentary Service accessing a journalist's private emails.

Return to Table of Contents/ Retour à la table des matières

International

China/Chine

Warning to online news sites on social media sources
South China Morning Post, 2016 07 05
Beijing--The **powerful internet censorship body has further tightened its grip on online news reports by warning all news or social network websites against publishing news without proper verification**, according to state media reports. The instruction, issued by the **Cyberspace Administration of China**, came only a few days after Xu Lin, formerly the deputy head of the organisation, replaced his boss, Lu Wei, as the top gatekeeper of internet affairs.No

website is allowed to report public news without specifying the sources, or report news that quotes untrue originsCyberspace Administration of China. Xu is seen as a key supporter of President Xi Jinping.

State Department Report Says Chinese Cyber Attacks 'Ongoing'
Washington Free Beacon, Bill Gertz, 2016 06 29
Washington - **Chinese cyber attacks against American firms are "ongoing" and the use of covert cyber tools and methods by Beijing hackers** led to a statistical decline in cyber activities, according to an internal State Department security report. The report by the State Department-led Overseas Security Advisory Council, or OSAC, a public-private partnership, challenges the findings of a recent study by the private cyber security firm FireEye that says the decline in the number of Chinese-origin cyber attacks indicated China has cut back from large-scale cyber attacks. "While media reporting has emphasized this alleged decrease in malicious activity, cases of Chinese espionage campaigns against the U.S. private sector are ongoing," the report said, adding that "OSAC constituents should remain aware that China is still considered a highly capable and motivated cyber threat actor."

Chinese economic cyber-espionage is diminishing, says U.S. official
Reuters, Staff report, 2016 06 28
Washington - U**.S. Assistant Attorney General John Carlin said on Tuesday that Chinese hacking activity appears to have declined since the Chinese government** vowed last September to stop supporting the hacking of U.S. trade secrets. The assertion supports findings released earlier this month from cyber security firm FireEye that breaches attributed to China-based groups had plunged by 90 percent in the past two years. "Generally, people have seen a change in activity," Carlin said at the Center for Strategic and International Studies think tank in Washington.

Return to Table of Contents/ Retour à la table des matières

Russia/Russie

Former Ukrainian security chief says no chances for NATO membership over short term
ITAR-TASS World Service, Staff report, 2016 07 05
Moscow - **Ukraine has lost an opportunity to get NATO membership over the short term, the former chief of the Ukrainian Security Service (SBU), Igor Smeshko** told the ICTV channel on Monday as he commented on the summit of the North-Atlantic pact that will be held in Warsaw on July 8-9. "Ukraine doesn't have the chances to become a NATO member - in the short term as a minimum," he said. "This country will have to build a combat-ready powerful army of its own." **NATO's Secretary General Jens Stoltenberg** said earlier he expected the latest information on developments in Ukraine from President Pyotr Poroshenko at a session of the NATO-Ukraine commission in Warsaw.

Moscow 'secret police grads' stage luxury car parade, prompt storm of criticism
RT (Russia), Staff report, 2016 07 04
Moscow - A **video showing a group of youngsters thought to be fresh graduates of Moscow's FSB secret police academy out for a joyride in Moscow while packed into 30 Mercedes luxury SUVs worth at least $100,000 has raised more than a few eyebrows**. The **FSB newbies** cruising the streets of the Russian capital in black four-wheel drive G-Wagens

blocked traffic in their lane several times, while honking their horns for no reason. To help a cameraman take some great shots, they formed a long line from time to time, making it difficult for other vehicles to pass by safely. Meanwhile, young men in white shirts keep protruding from the car windows, joyfully shouting and waving to each other while taking pictures and videos on their cell phones. The footage of the parade was later posted on the internet by its participants, as well as several witnesses.

Patrushev discuss int'l security with Israel's Mossad chief
Interfax News Agency, 2016 07 01
Moscow—**Russian Security Council Secretary Nikolai Patrushev has discussed international security with the director of Israeli Foreign Intelligence and Security Agency (Mossad),** the press service of the Security Council's administration told Interfax on Friday. "Russian Security Council Secretary has discussed the issues of provision of international security with the director of Israeli Foreign Intelligence and Security Agency. Nikolai Patrushev and Yossi Cohen have paid special attention to the situation in the Middle East," the press service said. The meeting has been held as part of the Cohen's working visit to Moscow, the press service said.

Russia Says U.S. Diplomat In Moscow Altercation A Spy
Radio Free Europe, 2016 06 30
Moscow— **Russia's Foreign Ministry says a U.S. diplomat who was involved in an altercation with a Russian guard outside the Moscow Embassy was a spy returning from an unspecified intelligence operation**. The June 30 announcement comes amid a slew of complaints by both sides of improper treatment of diplomatic staff in each other's country. The public statements represent a remarkable escalation with echoes of Cold War spy capers between Moscow and Washington. The U.S. diplomat suffered a broken shoulder after being tackled on a sidewalk outside the U.S. Embassy compound in central Moscow on June 6, according to a U.S. official who spoke to RFE/RL about the incident. The guard who was said to have tackled the man was part of the **Russian Federal Security Service (FSB)** division that both guards and monitors the embassy. That led to speculation that the American had been specifically targeted as an intelligence officer, a question raised by The Washington Post, which first reported on the incident.

Russian FSB guard attacked U.S. diplomat outside Moscow embassy
Washington Post, Josh Rogin, 2016 06 30
Column - In the early morning of June 6, a **uniformed Russian Federal Security Service (FSB) guard stationed outside the U.S. Embassy in Moscow attacked and beat up a U.S. diplomat who was trying to enter the compound, according to four U.S. officials who were briefed on the incident**. This previously unreported attack occurred just steps from the entrance to the U.S. Embassy complex, which is located in the Presnensky District in Moscow's city center. After being tackled by the FSB guard, the diplomat suffered a broken shoulder, among other injuries. He was eventually able to enter the embassy and was then flown out of Russia to receive urgent medical attention, administration officials confirmed to me. He remains outside of Russia. The attack caused a diplomatic episode behind the scenes that has not surfaced until now. The **State Department in Washington called in Russian Ambassador Sergey I. Kislyak to complain about the incident, an administration official said.** The motive for the attack remains unclear.. A different U.S. official told me **the diplomat may have been working as a spy in Russia under what's known as "diplomatic cover,"** which means he was pretending to be a State Department employee. Spokesmen for the both the **State Department and the CIA declined to comment** on the incident or whether or not the diplomat was in fact an undercover U.S. spy.

Poutine renforce son arsenal antiterroriste
Le Monde, Isabelle Mandraud, 2016 06 29
Moscou - Les opérateurs Internet et de téléphonie devront conserver tous les échanges pendant six mois A une cadence effrénée avant l'interruption de l'été, les députés de la Douma, la chambre basse du **Parlement russe, ont adopté deux lois antiterroristes controversées que le Conseil de la fédération, l'équivalent du Sénat**, s'apprête à son tour à entériner mercredi 29 juin. " Notre pays et notre société en ont besoin " , a déjà prévenu sa présidente, Valentina Matvienko. Présenté comme une réponse à l'attentat d'octobre 2015 contre un charter russe au-dessus du Sinaï, qui avait entraîné la mort de 224 passagers et membres d'équipage, ce **Patriot Act** version russe soulève l'inquiétude des organisations des droits de l'homme. Réfugié en Russie depuis deux ans, le lanceur d'alerte Edward Snowden a également dénoncé sur Twitter un arsenal " Big Brother " , " qui constitue une violation inapplicable et injustifiable des droits " .

The spying game: The former KGB officers who run Russia today
Russia Behind The Headlines, Yekaterina Sinelschikova, 2016 06 28
Moscow - **Secret Agents, sinister prison basements, widespread wiretapping and mass denouncements: There were always many rumors circulating about the KGB. And Russia's most famous Chekist** (from Cheka, the Emergency Committee, the first Soviet state security organization), President Vladimir Putin, and his work as a spy in Dresden continue to keep many people from sleeping at night. "What did Putin actually do in the late the 1980s in East Germany? " But surveillance was not the only secret unit in the KGB - the newspapers did not write about many of the sectors. "I served in the S administration, 'illegal' surveillance. We had false passports and biographies. There were many of us," says retired KGB Major General Valery Malevany. The structure of this command was never divulged. A Soviet agent could have been an engineer, a librarian or a broker. It was easier with the 'illegals' since they had official diplomatic positions. For example, the first secretary of an embassy was always someone from the **KGB**.

Return to Table of Contents/ Retour à la table des matières

Europe

Attentats : la commission d'enquête propose une profonde refonte du renseignement
Le Monde, Journaliste maison, 2016 07 05
Paris - La **commission d'enquête parlementaire sur les attentats de janvier et novembre 2015 a rendu son rapport mardi, soulignant l'étonnant défaut de coordination du renseignement français**. Au terme de six mois de travail, la commission d'enquête parlementaire sur l'action de l'Etat face aux attentats de janvier et novembre2015 a rendu son rapport, mardi 5juillet. Ce **document de trois cents pages se nourrit notamment des auditions de quatre ministres et des directeurs des services de renseignement.** Un important travail de synthèse qui aboutit à trente-neuf propositions, que le rapporteur de la commission, le député PS Sébastien Pietrasanta, et son président, le député LR Georges Fenech, ont présentées au Monde . Ces propositions balayent plusieurs thématiques allant de l'organisation des secours en situation de crise à la sécurisation du territoire en passant par les failles des services de renseignement.

Attentats : renseignement, terrorisme... Ce qu'il faut retenir du rapport de la commission Fenech
Le Point, Journaliste maison, 2016 07 05
Paris - **Georges Fenech**, à la tête de la commission d'enquête parlementaire, **ne décolère pas contre les "aberrations" du 13 novembre 2015.** Ses propositions. Huit mois après les attentats du 13 novembre qui ont secoué Paris, la commission d'enquête parlementaire vient de rendre ses conclusions. Le député Les Républicains Georges Fenech, président de cette commission, ne décolère pas. Il fustige les « aberrations » découvertes durant les cinq mois d'audition. Aux côtés du rapporteur socialiste Sébastien Pietrasanta, il a présenté un rapport pour éviter de telles « tragédies ». **En voici les principales propositions. Un « commandement unifié » Le 13 novembre 2015, ni le ministre de l'Intérieur ni le directeur général de la police nationale n'ont déclenché la Force d'intervention de la police nationale (la FIPN). La Brigade de recherche et d'intervention (BRI) a donc géré la direction des opérations, « alors que nous avons deux forces d'élite spécialisées :** le Raid, qui, ce soir-là, n'a été que force d'appoint, et le GIGN, qui est resté cantonné quai des Célestins », explique Georges Fenech au . Le député préconise « un commandement unifié en cas d'intervention de nos trois forces d'intervention ». **Renforcer la DGSI Georges Fenech s'étonne que « le travail de la Direction générale de la sécurité intérieure [DGSI]** s'arrête à la frontière parisienne ». Ainsi, la recherche de Saïd Kouachi, l'un des tueurs de , avait connu des difficultés à cause de rupture entre les services de la préfecture de police de Paris et la DGSI.

Terrorisme : les propositions chocs de la commission Fenech
Le Figaro, Paule Gonzalès avec Jean-Marc Leclerc, 2016 07 05
Paris - **Pour éviter un nouveau 13 novembre, le président de la Commission d'enquête parlementaire sur les attentats de 2015 propose une révolution dans les structures spécialisées**. «Devant le Bataclan, le 13 novembre, les policiers de la BAC, arrivés les premiers, voulaient au moins que les militaires de l'opération Sentinelle, arrivés sur place, leur prêtent leurs fusils d'assaut Famas, puisque les militaires n'avaient pas le droit de tirer. Et ils ont essuyé un refus!» Le député Les républicains **Georges Fenech**, président de la Commission d'enquête parlementaire sur les attentats de 2015 en France, ne décolère pas contre les «aberrations» mises à jour au fil de ses cinq mois d'auditions. Voici ce qu'il propose, avec le rapporteur socialiste Sébastien Pietrasanta pour éviter de telles «tragédies».

French lawmakers propose intelligence overhaul after 2015 attacks
DPA News Agency, 2016 07 05
Paris—**France's intelligence services should be overhauled**, a parliamentary inquiry commission tasked with assessing possible security flaws recommended Tuesday. The commission was set up in the wake of terrorist attacks that hit the country in 2015. The commission said that counter-terrorism activities should be re-organized around a national agency directly under the authority of the prime minister, French newspaper Le Monde said. It also recommended measures to bolster cooperation between police and military intervention forces, and to streamline intelligence services.The head of the parliamentary group, **Georges Fenech**, said Tuesday on social media that the commission's report conclusions had been adopted unanimously and that a body was set up to monitor the implementation of the proposals. Speaking to broadcaster BFM-TV, Fenech had pointed specifically to the case of Said Kouachi, one of the Charlie Hebdo shooters, who was under Parisian surveillance until it was lifted when he left Paris. The **case was then taken up by French intelligence agency DGSI.**

Former Ukrainian security chief says no chances for NATO membership over short term
ITAR-TASS World Service, Staff report, 2016 07 05
Moscow - **Ukraine has lost an opportunity to get NATO membership over the short term, the former chief of the Ukrainian Security Service (SBU), Igor Smeshko** told the ICTV channel on Monday as he commented on the summit of the North-Atlantic pact that will be held in Warsaw on July 8-9. "Ukraine doesn't have the chances to become a NATO member - in the short term as a minimum," he said. "This country will have to build a combat-ready powerful army of its own." NATO's Secretary General Jens Stoltenberg said earlier he expected the latest information on developments in Ukraine from President Pyotr Poroshenko at a session of the NATO-Ukraine commission in Warsaw.

CIA arrested wrong man but jailed him anyway
McClatchy News Service, Matthew Schofield, 2016 07 04
Berlin--By January 2004, when German citizen **Khaleed al-Masri arrived at the Central Intelligence Agency's secret prison in Afghanistan, agency officials were pretty sure he wasn't a terrorist**. They also knew he didn't know any terrorists, or much about anything in the world of international terror. In short, they suspected they'd nabbed the wrong man. Still, the agency continued to imprison and interrogate him, according to a recently released internal CIA report on al-Masri's arrest. The report claims that al-Masri suffered no physical abuse during his wrongful imprisonment, though it acknowledges that for months he was kept in a "small cell with some clothing, bedding and a bucket for his waste." Al-Masri says he was tortured, specifically that a medical examination against his will constituted sodomy. **The embarrassing, and horrifying, case of al-Masri is hardly new. It has been known for a decade as a colossal example of CIA error in the agency's pursuit of terrorists during the administration of President George W. Bush**. But the recently released internal report makes it clear that the CIA's failures in the al-Masri case were even more outrageous than previous accounts have suggested.

German spy chief says can't rule out Istanbul-style attacks at home
Reuters, 2016 07 02
Berlin—**Attacks by Islamist militants pose the biggest security threat for Germany and events like the shooting and bombing in Istanbul this week could happen in Germany, the head of the domestic intelligence agency (BfV)** told a Saturday newspaper. Three suspected Islamic State suicide bombers killed 44 people at Istanbul's main airport on Tuesday, the deadliest in a string of attacks in Turkey this year. "We can't rule out attacks like those in Istanbul also happening in our country," **Hans-Georg Maassen** told German newspaper Frankfurter Allgemeine Zeitung.

Security Service calls for 700 MHz band to remain state-owned
Esmerk Swedish News, 2016 07 01
Stockholm—The **Swedish Security Service (Säpo) has expressed concern regarding the possible outsourcing of the 700 MHz band by the Swedish Post and Telecom Authority** (PTS). The 700 MHz band will be used for mobile broadband for private consumers. Säpo has responsibility for security protection of telecom connections and the service concluded that it will be hard to maintain security without a secure system.

Russian Federal Security Service officer is charged for espionage in Lithuania
Lithuanian News Agency, 2016 07 01
Vilnius—The Organised Crimes and Corruption Investigation Department at the Prosecutor General's Office of Lithuania has submitted an **espionage case to Vilnius County Court.** A **defendant in the case is identified by initials N. F., the citizen of the Russian Federation**

who at the time was a senior operational officer at the intelligence section of the Russian Federal Security Service's Kaliningrad Regional Office. The Russian citizen is accused of espionage, forgery of documents, the use of forged documents and multiple illegal crossings of the Lithuanian border. N. F. is accused of acting as a foreign intelligence officer in an organised group and attempting to recruit Lithuanian citizens during meetings in several foreign countries from October 2011 to the end of 2014 to spy against Lithuania, collect and transfer information to a foreign intelligence agency and actively organising such activities and paying money for information.

Turkish intelligence warned of potential Istanbul airport attack around 20 days ago: Report
Hurriyet Daily News, Staff report, 2016 06 30
Istanbul - **Turkish intelligence units sent a warning letter to related state institutions about a potential attack by the Islamic State of Iraq and the Levant (ISIL) jihadist group targeting Istanbul around 20 days ago**, before the city's main airport was hit in a deadly terror attack late on June 28, a senior Turkish journalist based in Ankara has reported. Speaking during a live broadcast on June 29, Dogan TV's Ankara representative Hande Firat stated that intelligence units sent a warning letter to all state institutions about a possible attack on Istanbul. "Intelligence units sent a warning letter to the top of the state and all its institutions in early June, around 20 days ago, about Istanbul," Firat said.

Rinkevics warns of foreign intelligence services' increased activity
Latvian News Agency, 2016 06 30
Riga—**Intelligence activity of countries that are not NATO and EU members increases ahead of major events and Latvian security agencies have to be prepared for this, Foreign Minister Edgars Rinkevics (Unity) said** on Latvian Radio today.Asked if foreign intelligence services had been stepping up their activities ahead of the upcoming NATO summit in the Polish capital Warsaw, the Latvian minister said that countries that are not NATO and EU members always want to learn more about forthcoming talks and decisions that could influence their own decision making."In recent years, because of the events in Ukraine, the activity of many countries' intelligence services and their interest in decision makers have only increased.

How a Czech 'super-spy' infiltrated the CIA
The Guardian (London), Benjamin Cunningham, 2016 06 30
Prague - On a cold February night in 1986, **Berlin's Glienicke Bridge became the scene of the cold war's last ever prisoner exchange - a dramatic hand-over involving a Soviet dissident and Karel Koecher**, the **only foreign agent ever known to have infiltrated the CIA.** Koecher was a Czech citizen who had been living undercover in the US for 21 years. Alternately codenamed Rino, Turian or Pedro, he had moved to America in 1965 to establish himself as a mole within the CIA. Koecher's KGB case officer, Colonel Alexander Sokolov, would later call him a super-spy. According to files held by Czech secret police, his wife, Hana Koecherova, codenamed Adrid, had distributed secret messages on Koecher's behalf during their decades abroad but was never charged with espionage. For years she had been a New York City diamond dealer.

Germany girds for potential spike in Islamic State attacks in Europe
Reuters, Staff report, 2016 06 28
Berlin - The **German government voiced concern on Tuesday that Islamic State could step up attacks in Europe** as it loses territory in Iraq and Syria, and said its domestic intelligence agency is training to respond to a large-scale assault. Interior Minister Thomas De Maiziere welcomed gains made by a U.S.-led coalition against Islamic State (IS) in Iraq and Syria, but

said they were not diminishing the risk of attacks in Europe. "On the contrary, we fear that Islamic State will externalize, transfer its activities to Europe, especially because of military losses in the region," the minister, a member of Chancellor Angela Merkel's conservative Christian Democratic party, told reporters. Germany has been on high alert for possible large-scale militant incidents - potentially including military- style weapons - since the IS attacks in Paris last November and Brussels in March, **Hans-Georg Maassen, the head of the BfV domestic intelligence agency**, told the same news conference.

Germany puts a (long) leash on its spooks
Deutsche Welle, Staff report, 2016 06 28
Berlin - The **German government is moving to tighten rules on its foreign intelligence service, the Bundesnachrichtendienst (BND), following a series of revelations that it was acting independently of any government oversight, spying on allies, international organizations and helping the US National Security Agency (NSA) without it ever being appropriately monitored by any parliamentary watchdog**. In a cabinet meeting on Tuesday, Angela Merkel's administration agreed to a new draft bill that would see legal guidelines imposed on spying on European Union citizens, as well as an external committee to oversee the agency. But the bill is actually a diluted version of what had been originally planned and recommended by the parliamentary committee, building in a number of exceptions to allow the BND to spy on targets within the EU.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

IRGC Intelligence Official: Iran Seriously Pursuing Fate of Kidnapped Diplomats
Fars News Agency, 2016 07 05
Tehran - **Head of the Islamic Revolution Guards Corps (IRGC) intelligence unit Hossein Ta'eb underlined that Iran is seriously pursuing the fate of its four diplomats who had been abducted by Phalange forces in Northern Lebanon** in 1982. "The relevant bodies are seriously pursuing the issue until attainment of final results," Ta'eb told FNA on Monday. "We are not yet disappointed at obtaining results as we pursue the case," he added. In relevant remarks yesterday, Son of former Iranian charge d'affaires in Beirut Seyed Mohsen Moussavi underlined that evidence and documents indicate that the four diplomats abducted in Lebanon are still alive and imprisoned in Israel.

Syria intelligence chief visits Rome
Now Lebanon, Albin Szakola, Amin Nasr, 2016 07 05
Beirut - A leading pro-regime newspaper has reported that a **top Syrian intelligence chief sanctioned by the EU recently made a secret visit to Italy.** "A high-level Syrian security delegation visited Rome last week, where they met with senior Italian security officials," Al-Watan reported Sunday. The newspaper--which is owned by Bashar al-Assad's influential cousin Rami Makhlouf--cited a "Western diplomatic source in Beirut" as saying that **Syrian General Intelligence Directorate chief Major General Mohammad Deeb Zaytoun headed the delegation.** "Zaytoun, who was accompanied by a number of officers, made a two-day visit in Rome during which he met with his [Italian] counterpart and a number of security officials," the source told the newspaper.

Iran officials urges intelligence body to find sender of "threatening" messages
BBC Monitoring Caucasus, 2016 07 02
Tehran - **Some Iranian officials and journalists have called on the Ministry of Intelligence and the Cyber Police to investigate the source for "threatening messages" recently sent to journalists**. On 30 June, a message was sent to over 700 political activists and journalists, warning them to stop cooperating with foreign media. "Warning: Any kind of connection or cooperation with hostile elements [presumably referring to the foreign media] residing in foreign countries via email, secured portals or any other communication devices is considered as an offence that will be brought to prosecution. You should cut your relation. This message is the final security warning," it read. Vice-Speaker of the parliament Ali Motahhari called on the **Ministry of Intelligence and FATA (Persian acronym for the Cyber Police)** to investigate the case and find the sender of the message.

Return to Table of Contents/ Retour à la table des matières

Asia/Asie

Japan, Italy to cooperate on counterterrorism after Dhaka attack (Canada)
Kyodo News, 2016 07 05
Tokyo--**Japan and Italy agreed Monday to cooperate on counterterrorism in the wake of a terrorist attack in Dhaka** which resulted in the deaths of 20 hostages, including nine Italians and seven Japanese, the Japanese Foreign Ministry said. Foreign Minister Fumio Kishida and his Italian counterpart Paolo Gentiloni also affirmed in telephone talks to cooperate in dealing with the aftermath of the deadly attack at a restaurant in Dhaka on Friday evening, the ministry said. Noting that the Group of Seven leaders agreed in their summit in May in central Japan on efforts to fight terrorism and violent extremism, the ministers agreed on close coordination to that end, it said. Italy will succeed Japan as the chair of the G-7 grouping Britain, **Canada**, France, Germany, Italy, Japan and the United States next year.

Pakistan denies ISI's role in Dhaka carnage
Dawn (Pakistan), 2016 07 05
Islamabad—The **Foreign Office on Monday denied that Pakistan's premier intelligence agency ISI was behind the Dhaka carnage and described the allegations as "baseless and unfounded".**"These are highly regrettable, irresponsible and provocative stories being carried in the Indian media. They are utterly baseless and unfounded. Pakistan strongly rejects such allegations," FO spokesman Nafees Zakaria said in a statement. He was reacting to media reports that ISI had links with the militant group Jamayetul Mujahideen Bangladesh, the group that carried out the weekend attack in an upscale cafe in the Bangladeshi capital in which 20 hostages, mostly foreigners, were killed by the terrorists.

Indian agencies had alerted Bangladesh
Deccan Herald, 2016 07 04
Kolkata—In a **move that could cause diplomatic unease, Indian intelligence agencies claim that they repeatedly warned Dhaka about an "imminent" terror strike.** The seed of the inputs can be traced back to the October 2014 blast at Khagragarh in Burdwan district of West Bengal. Sources said inputs were passed on to Bangladesh as recent as June 14 after investigating officials observed some pro-Islamic state youths who were using Facebook and Twitter to exchange notes. "Our agencies deciphered these coded missives, mostly

photographs, to realise that Dhaka's diplomatic zone would be under attack," an official said. Sources said **Rajinder Khanna, chief of Indian counter-intelligence agency RAW**, had sometime in early June notified his counterpart in Bangladesh about an "imminent attack". However, Indian agencies are not willing to comment on the measures taken by Dhaka. "It is an internal matter and we shouldn't comment on it, but the last few alerts had specific information. We also know that US agencies shared similar alerts with Dhaka," the source said.

NIS arrests two men for spying for Pyongyang
Korea JoongAng Daily, 2016 07 03
Seoul - The **National Intelligence Service (NIS) arrested two South Korean men on espionage charges and is questioning them about alleged anti- state activities they planned to carry out**, the NIS reported to lawmakers Friday. In a briefing to members of the parliamentary intelligence committee Friday, the NIS revealed that it arrested one espionage suspect in an Internet cafe in Dongjak District, northern Seoul, in May as he was writing an email to a contact in North Korea describing domestic affairs. The NIS didn't elaborate on the suspect's report or his identity except saying that he was in his late 40s or early 50s. The NIS reported it arrested another man in Ansan, Gyeonggi, around the same time on charges of violating the national security law.

S. Korea draws up detailed antiterrorism plans
Yonhap News Agency, 2016 07 02
Seoul—**South Korea's antiterrorism center under the Prime Minister's Office on Friday drew up a detailed plan on tackling possible terrorist attacks in the country**, amid rising concerns that international radical groups may target Asia's fourth-largest economy as well. Under the plan, the country will make a four-step alert system depending on the circumstances, while designating an "antiterrorism squad" composed of special forces under the military, police, and the Ministry of Public Safety and Security. "There is a possibility that North Korea will abduct our citizens overseas, or conduct attacks by hiring international terrorism organizations," Prime Minister Hwang Kyo-ahn said. "All related organizations must make efforts to have no blind spots when it comes to preventing terrorism." The government has been speeding up its efforts to bolster antiterrorism capabilities, especially as the **National Intelligence Service** revealed last month that the Islamic State jihadist group had designated some U.S. military installations here and a South Korean citizen as targets.

Defense and Security to be Focus in K/L Expenditure in APBN-P 2016
Iindonesian Government News, 2016 06 30
Jakarta—Ministry/Institution (K/L) expenditure budget in the Revised State Budget (APBN-P) 2016 will **focus on defense and security expenditur**e. This aims to strengthen national security stability. "The focus of ministry/institution's expenditure in APBN-P 2016 is defense and security expenditure, which aims to strengthen security stability," explains Minister of Finance Bambang P.S. Brodjonegoro in the press conference on APBN-P 2016 and Tax Amnesty on Wednesday (29/06) at the Djuanda Hall, Ministry of Finance, Jakarta. Minister adds, budget increase will also touch K/L that are deal with terrorism and narcotics eradication. "**The beneficiaries, other than Ministry of Defense and POLRI, are BNPT (National Antiterrorism Agency), BNN (National Narcotics Agency), BIN (National Intelligence Agency**), and other institutions related to terrorism and narcotics eradication," he says.

NDS creating subversive spying network in Punjab
The Nation, Jawad R. Awan, 2016 06 29
New Delhi—Tracing NDS footprints in the Punjab, **the security services have spotted Afghan intelligence agency's bids to create a subversive spying network in the province through**

their refugees, The Nation learnt through sources in the security agencies. Against the backdrop of possible encirclement of Pakistan by Kabul, New Delhi and some western powers in the region, Afghanistan's key intelligence service has made bids to erect a network of its agents in the Punjab. The probable network is aimed to launch subversion in the relatively calm province for multiple purposes of which CPEC routes can be the major target, they added. **Inter-Services Intelligence** (ISI), in some key operations, hunted down subversive spy rings of **National Directorate of Security (NDS)** from Taxila, Attock, Rawalpindi and Tarnol, Islamabad. Weapons and explosives were also recovered in the intelligence-led operations to create havoc on Pakistani soil.

Return to Table of Contents/ Retour à la table des matières

Africa/Afrique

State Spies Put Catholic Bishop Mtumbuka, Malawi Activists Under Surveillance Over 'Regime Change' Agenda
Nyasa Times, 2016 07 04
Lilongwe, Malawi—The **dreaded National Intelligence Bureau (NIB) has put on surveillance Bishop Dr Martin Mtumbuka of Karonga Diocese of the influential Catholic Church and other activists following its intelligence gathering** that the bishop has joined the underground movement discussing a regime change agenda in Malawi, Nyasa Times understands. The state spies are following His Grace Bishop Mtumbuka after its intelligence notes claim the Public Affairs Committee (PAC) has successfully convinced him to join the movement that has been discussing the possibility of having President Arthur Peter Mutharika removed from power before the next general elections slated for 2019.

Avengers, Tompolo disown alleged bombers in DSS custody
Vangard News, Emma Amaize, 2016 07 03
Abuja - The **Niger Delta Avengers, NDA, yesterday, denied that two suspects, Christian Oluba, alias Sensor, and Selky Kile Torughedi, arrested by the Department of Security Service, DSS**, in connection with foiled attacks on oil facilities in the Niger Delta, were its members. In addition, fugitive ex-militant leader, Government Ekpemupolo, alias Tompolo, allegedly identified by Torughedi, according to the DSS, as the person that sent him to kill a serving army officer, Major M.B Yahaya, said the claim was a farce. The DSS, had, last Friday, said it arrested Torughedi, described as a close associate of Tompolo in Calabar, Cross River State, after he had carried out reconnaissance on the home of Yahaya in Kaduna, while Sensor was seized as he was allegedly perfecting plans to carry out attacks on oil and gas pipelines, including storage points. The security agency said both suspects were members of the NDA and that it foiled fresh plans by militants to attack oil pipelines in the region by arresting the masterminds.

DSS foils NDA's planned bombing of oil pipelines
Vangard News, Soni Daniel, 2016 07 02
Abuja - The **Department of State Security Service, DSS, has recorded a major success against criminals posing serious challenges to the nation through attacks on oil installations and kidnap of prominent Nigerians for pecuniary gains**. The DSS said last night that it foiled fresh planned attacks on vital oil facilities in the Niger Delta region by arresting the masterminds of the onslaughts before they were able to carry out their nefarious actions. A

statement made available to Saturday Vanguard in Abuja by the security agency and signed by Tony Opuiyo, said the DSS also arrested no fewer than 15 kidnap kingpins from various parts of the country, including the man who kidnapped the Personal Assistant to the Transport Minister, Igo Chinda. The DSS said all the arrests were made in the month of June through what it called 'series of special tactical operations', which led to the decimation of the criminals' hideouts.

Niger Delta: Buhari, Osinbajo meet service chiefs
The Sun (Nigeria), 2016 07 01
Abuja—**President Muhammadu Buhari and Vice President Yemi Osinbajo yesterday held a closed door meeting with Service Chiefs and other heads of security agencies in the country.** The meeting reportedly reviewed military operations in the Niger Delta region and the ongoing anti-terrorism war in the North-East. Those who attended the meeting included the Chief of Defence Staff, Gabriel Olonisakin; Chief of Army Staff, Tukur Buratai;Chiefof Air Staff, Air Marshal SadiqueAbubakar;Chief of Naval Staff,Ibok-Ete Ibas; **Director General of the Department of State Services, Lawal Daura; Director General, National Intelligence Agency, Mr. Ayo Oke;** and theacting Inspector General of Police, Mr. Ibrahim Idris.

Return to Table of Contents/ Retour à la table des matières

Americas/Amériques

Brazil has 'total confidence' in Olympics security
Agence France-Presse, Staff report, 2016 06 29
Rio de Janeiro - **Brazil has "total confidence" that it can ensure security for more than half a million tourists and athletes attending the Rio Olympics this August**, a senior official said Wednesday. Andrei Rodrigues, secretary for major events at the justice ministry, said that a heavy police presence on the ground and **international cooperation on intelligence gathering would overcome potential terrorist threats and the danger of violent crime**. "I have total confidence in our preparations for the security of the Games," Rodrigues told reporters a month ahead of the August 5-21 Olympics, which he described as "the biggest event on the planet."

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

06-07-2016 to/au 12-06-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Demoralized RCMP want union to force change
Ottawa Citizen, Kathryn May, 2016 07 11
Ottawa - **Most rank-and-file RCMP officers don't believe Canada's national police force will survive without unionization** but they have firm ideas about what they want and expect from a new unionized workplace. A report on a major consultation of rank-and-file RCMP found they have "intense and emotional" feelings about the force. Their chief frustration is management who they mistrust and feel doesn't listen to them and their top concerns revolve around wages and benefits, working conditions and protection against "unfair or arbitrary treatment." Alain Jolicoeur, a former senior bureaucrat who led the consultation, recently told a Senate committee that he was taken aback by the "intensity of feelings" among the pro-union and anti-union forces but more favoured unionization than were against.

RCMP legal fund used to finance union drive
Ottawa Citizen, Kathryn May, 2016 07 11
Ottawa - **As Canada's Mounties prepare to choose their first-ever union, two rival factions are warring over the propriety of a loan one side received to finance its organizing drive**. The debate is casting a shadow over the historic public-sector organizing drive, set in motion by a Supreme Court of Canada decision, and considered the biggest in 50 years. At the centre of the dispute is the RCMP's multimillion-dollar legal fund, which took the unusual step of approving a loan - of undisclosed value -- to one of the groups vying to become the force's first bargaining agent. The loan dispute throws a spotlight on the differences that have divided the force for nearly 20 years on how to manage labour relations - a division that paved the way for a landmark top court ruling giving the RCMP the right to unionize.

Government documents suggest Snowden 'altered' the cyberspace discussion
Toronto Star, Alex Boutilier, 2016 07 09
Ottawa - It's not a matter of if there will be another **Edward Snowden**, it's a matter of when, according to internal government documents obtained by the Star. **Global Affairs officials warned ministerStéphane Dion in November an event on the scale of Snowden's disclosures about Internet surveillance is inevitable.** "Incidents similar to the Snowden disclosures and the Sony hack will happen again and we can expect that sudden events will affect international debates on cyberspace," the document reads. The briefing note, prepared for Dion in November and obtained under access to information law, suggests that Snowden's disclosures about western mass surveillance "altered the tone" of the international discussion on cyberspace. In 2013 Snowden, a former employee of the **U.S. National Security Agency (NSA),** pulled back the curtain on mass surveillance online, detailing the capabilities of the "Five Eyes" countries - Canada, the United States, the U.K., Australia and New Zealand - to monitor activity online. While Canada has long advocated for an open and free Internet, suggestions that the nation's spy agency the **Communications Security Establishment** (CSE) has engaged in mass online surveillance have complicated that narrative.

Mounties revamp witness protection
Canadian Press, Jim Bronskill, 2016 07 08
Ottawa - The **RCMP is retooling its witness protection program following a secret internal review that called for changes to enrolment decision-making and better reporting on the**

program's impact. The changes come less than two years after a fullscale overhaul of the program prompted by high-profile controversies. The federal witness program, administered by the RCMP, is seen as a key tool in the fight against terrorism and organized crime. It shields people who help authorities by providing everything from short-term protection to permanent relocation and identity changes. Protectees may be victims, informants, witnesses or others threatened with intimidation or violence.

Mounties refusing to join 'red serge' community events in protest over working conditions
CBC.CA, Alison Crawford, 2016 07 07
Ottawa - **Members of the RCMP across Canada are taking part in quiet protests over what they say is unsustainable under-staffing and an overall morale problem within the force**. Some Mounties are refusing to volunteer for so-called "red serge duty" where they march in parades and appear at events such as fairs, festivals and sporting events in their ceremonial red uniforms and Stetson hats.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

U.S. intel warns: ISIS not desperate, just 'adapting'
CNN.com, Barbara Starr, 2016 07 11
Washington - **Recent raids against ISIS targets have given the U.S. intelligence community a better understanding of how the terror group is structured and organized** and about its plans for attacks outside areas it controls in Syria and Iraq, according to a senior administration official. They also have made it clear that for some time ISIS was planning to focus on those attacks around the world, although there were no clear indications of when and where that would have provided actionable intelligence to prevent them, **the senior official** said. "We were aware they were moving this way," the official said. "It's not like we didn't see it coming." The official declined to say where the intelligence came from, but a spokesman for the U.S.-led coalition in Iraq and Syria recently revealed the Syrian Arab Coalition (SAC) -- Arab fighters in northern Syria that the U.S. supports -- had collected a significant amount of ISIS intel in raids in northern Syria.

Two Russian diplomats are expelled after U.S. official is jumped in Moscow
Washington Post, Carol Morello, 2016 07 09
Washington - The **United States last month expelled two Russian diplomats as a response to a Russian police guard tackling a U.S. diplomat outside the American Embassy in Moscow**, the State Department said Friday. The diplomats were declared persona non grata on June 17, spokesman John Kirby said. That was less than two weeks after the incident that sparked the diplomatic row. The June 6 scuffle between the police officer and the diplomat was captured on security footage and broadcast on Russian television last week. It shows a man emerging from a taxi and walking briskly up the embassy steps. He is just outside the door when a guard jumps out of a gatehouse and wrestles him to the ground. Even with the patrolman on top of him, the diplomat pushes with his feet and, while on his back, manages to get inside the door to the embassy, which is U.S. territory and inviolate.

U.S. Says Kremlin Harasses Diplomats
Wall Street Journal, Felicia Schwartz, 2016 07 08

Washington - **The U.S. has grown increasingly concerned about the Kremlin's harassment of U.S. diplomats**, the State Department said on Thursday in criticism that coincided with the release of a video appearing to show a Russian police officer attacking a U.S. official outside the U.S. Embassy in Moscow. The video on Russian television station NTV shows a man getting out of a taxicab and walking up the stairs of the U.S. Embassy, when a door swings open and a man described as a Russian police officer tackles him, throwing him to the ground. In the footage, the officer pinned the other person, described as a U.S. diplomat, who is seen attempting to slide across the ground outside the embassy to make his way inside. State Department spokesman John Kirby said he couldn't confirm the authenticity of the video but said he didn't have any reason to doubt it.

F.B.I. Director Testifies on Clinton Emails to Withering Criticism From G.O.P.
New York Times, Eric Lichtblau, Michael D. Shear, 2016 07 08
Washington - The F.B.I. director, **James B. Comey Jr., defended himself Thursday against an onslaught of Republican criticism for ending the investigation into Hillary Clinton's emails, but he also provided new details that could prove damaging to her just weeks before she is to be named the Democrats' presidential nominee**. At a contentious hearing of the House oversight committee, Mr. Comey acknowledged under questioning that a number of key assertions that Mrs. Clinton made for months in defending her email system were contradicted by the F.B.I.'s investigation. Mr. Comey said that Mrs. Clinton had failed to return "thousands" of work-related emails to the State Department, despite her public insistence to the contrary, and that her lawyers may have destroyed classified material that the F.B.I. was unable to recover. He also described her handling of classified material as secretary of state as "negligent" -- a legal term he avoided using when he announced on Tuesday that "no reasonable prosecutor" would bring a case against her.

Man Says He Was a Spy; Now He Fears Deportation (Canada)
The New York Times, Benjamin Weiser, 2016 07 07
New York— One evening in February, a man entering the subway at Barclays Center in Brooklyn was detained by the police for using a discounted student MetroCard -- his daughter's, it turned out. It was, he would say later, a stupid mistake that would lead to absurd consequences: The man, **Blerim Skoro**, a citizen of Kosovo, now sits in jail, facing potential deportation. But Mr. Skoro was no mere hapless fare-beater. "I was working for U.S. government," he told a United States asylum officer in May, explaining his past life overseas and why he was now afraid of being sent back to Kosovo, a transcript shows. **"I was trained for Washington. I was a spy."** He says he posed as a willing operative and insinuated himself with members of Al Qaeda in the Balkans, secretly supplying the Central Intelligence Agency with information about plots and the people behind them. **After the C.I.A. cut ties with him in 2010**, he says, **he eventually returned to the United States via Canada** -- illegally, he admits -- and last year, with the help of a lawyer, met separately with the F.B.I. and counterterrorism officials with the New York Police Department, trying unsuccessfully to offer clandestine assistance in the fight against the Islamic State.

WH rejects call to block Clinton from receiving classified briefings
The Hill, Jordan Fabian, 2016 07 06
Washington - The **White House on Wednesday brushed aside House Speaker Paul Ryan's (R-Wis.) call to block Hillary Clinton from receiving classified intelligence briefings as punishment for the FBI's probe into her use of a private email server while secretary of State**. White House press secretary Josh Earnest said it's a "longstanding tradition" for major party presidential nominees to receive such briefings -- and indicated that practice is almost certain to continue. "What the **Office of the Director of National Intelligence [DNI]** has

indicated is that they expect those briefings to move forward after the party conventions," Earnest said. "And the expectation that the DNI has is that they'll provide the same information to both candidates," he added.

Behind James Comey's Big Gamble
Politico, Garrett M. Graff, 2016 07 06
Analysis - Whether or not the **FBI Director James Comey** would speak publicly about the Hillary Clinton email server investigation had been a matter of debate throughout the spring on the seventh-floor corridor that denotes the executive offices inside the J. Edgar Hoover Building on Pennsylvania Avenue, according to those close to the FBI director. During the winter, as the long-running investigation unfolded, the FBI did not expect to make any sort of public statement regarding its investigatory conclusions. That role historically has fallen to the Justice Department; the FBI rarely--if ever--makes public remarks regarding prosecutorial recommendations. But even weeks before Attorney General Loretta Lynch's ill- conceived and seemingly compromising tarmac run-in with former President Bill Clinton in June, **Comey and his leadership team had come to understand that the public credibility of the century-old law enforcement agency would hinge on its handling of the politically touchy email investigation**. The decision to hold Tuesday's news conference came after bureau leaders decided that the FBI couldn't simply conduct its investigation behind closed doors and then kick the decision across Pennsylvania Avenue to what's known as "Main Justice." Instead, to defend the FBI's independence and future credibility and avoid the perception that its investigation had been politically influenced, he had to publicly account for its own work.

Clinton's email could have been hacked, FBI says
Washington Post, Karen DeYoung, 2016 07 06
Washington - The **FBI investigation into Hillary Clinton's private email server found no evidence that her communications were hacked while she was secretary of state**, but it made clear that "hostile actors" here and abroad could have done so. **Clinton "used her personal email extensively while outside of the United States," FBI Director James B. Comey said**, including "in the territory of sophisticated adversaries." It was "possible" that they accessed her account, he said. But "given the nature of the system and the actors potentially involved, we assess we would be unlikely to see such direct evidence."

James Comey's Rebuke of Hillary Clinton Fits a 3-Decade Pattern
New York Times, Michael S. Schmidt, Eric Lichtblau, 2016 07 06
Washington - Shortly after Hillary Clinton was interviewed on Saturday by agents at the F.B.I.'s headquarters, its director, **James B. Comey,** heard from his deputies that Mrs. Clinton had been truthful and forthcoming in the three-and-a-half-hour meeting. Mr. Comey, who had been regularly briefed on the progress of the yearlong investigation into Mrs. Clinton's email account as secretary of state, **had known for some time that his agents had not uncovered enough evidence to charge her or anyone else with a crime**. Now, with the interview done, he told his deputies, according to F.B.I. officials, that he wanted to move forward with a plan he had been working on for months to explain the findings from such a politically contentious investigation to the public. And he did not wait to do it. At 11 a.m. on Tuesday, Mr. Comey walked into a conference room on the first floor of the F.B.I.'s headquarters, where he stood behind a lectern for 15 minutes and laid out in clinical detail how Mrs. Clinton's use of the account was "extremely careless." But, he said, the bureau would recommend to the Justice Department that she not be charged with a crime because his investigators had found no clear evidence that Mrs. Clinton had intentionally broken the law. The careful approach to publicly explaining his thinking fit a pattern for Mr. Comey, who, throughout his three decades as a law enforcement official, has refused to shy away from politically fraught issues.

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

From GCHQ to Google: the battle to outpace hackers in the cyber race
London Daily Telegraph, Staff report, 2016 07 11
London - **Law enforcement and corporations are still losing the fight against cyber criminals, the National Crime Agency admitted this week**, reporting that the "accelerating pace" of criminal ability is outpacing the country's defences. "You've got the perfect storm of increasingly sophisticated cyber attacks and high adoption of cloud infrastructure," says Alexis Scorer, a director at technology dealmakers GP Bullhound who specialises in technology. No amount of money will help overcome one of the greatest difficulties in the security industry though: the lack of skilled people. **By 2019 there will be a global shortfall of 1.5 million security professionals, according to ISC Squared**, a security certification and industry education body. And the numbers could in fact be significantly higher, given that there are already more than 1 million cybersecurity positions unfilled worldwide, according to a 2015 Cisco report. **Heading up the government's move to train more cyber defenders is spook agency GCHQ, which sponsors academic bursaries, runs summer camps and training days, holds competitions and has created a cyber excellence accreditation for top universities and masters programmes.** The intention is to spot talent in children and nurture them through their education, with the end goal being a career in the industry. "It's an interesting departure from our day to day work, but we have a role to play in this," says Chris Ensor, a technical director for GCHQ's information security arm.

Spies warned invading Iraq would inspire terrorists
Sunday Telegraph (UK), Robert Mendick, 2016 07 10
London - **Britain's spy chiefs warned Tony Blair just weeks before the invasion of Iraq that he would be putting the UK at risk of increased terror attacks**. A top-secret report released to the Chilcot inquiry spells out how al-Qaeda was planning to use the invasion to target Britain. The intelligence report also warned of the danger of Iraq's chemical and biological weapons falling into the hands of terrorists. Setting out the increased risk of attack, the Joint Intelligence Committee wrote in February 2003: 'The threat from al-Qaeda will increase at the onset of any military action against Iraq. They will target Coalition forces and other Western interests in the Middle East. "Attacks against Western interests elsewhere are also likely, especially in the US and UK, for maximum impact. "The worldwide threat from other Islamist terrorist groups and individuals will increase significantly."

Spies keen to please No 10 were fooled by lying sources
London Times, Sean O'Neill, 2016 07 09
London - **On the first anniversary of the September 11 attacks, MI6 produced a dramatic intelligence report on the threat from Saddam Hussein**. The information, from a new source, showed that Iraq was making and planning to use chemical and biological weapons. For Tony Blair, in his search to justify Britain's participation in an invasion of Iraq, this was as close as it would get to the silver bullet. The next day, September 12, 2002, Sir Richard Dearlove,head of MI6, was in Downing Street to brief the prime minister on the source and his information. These were heady times for Sir Richard and his agency. **The Secret Intelligence Service** (SIS), commonly known as MI6, had been in the Whitehall wilderness since the end of the Cold War, but that had changed when Osama bin Laden struck in New York and Washington.

15 secretive orders 'allow spy agencies to collect communications data'
Press Association, Staff report, 2016 07 08
London - **Fifteen secretive orders are in force allowing British spy agencies to collect large volumes of communications data**, it has been revealed. The measures were issued by Home and Foreign Secretaries on behalf of **MI5** and **GCHQ** using a little-known legal provision between 2001 and 2016. A report published on Thursday by the Interception of Communications Commissioner's Office (IOCCO) disclosed that there were a total of 23 "extant" section 94 directions within the scope of its oversight. They were all given by the Home Secretary or Foreign Secretary at various times between 2001 and 2016 on behalf of MI5, GCHQ, the three intelligence agencies collectively **- MI5, GCHQ, and MI6** - or the Metropolitan Police's counter-terrorism command.

Blair: I should have challenged intelligence chiefs
London Times, Zachary Spiro, 2016 07 07
London - **Tony Blair expressed regret today that he did not challenge incorrect intelligence assessments about Saddam Hussein's supposed weapons of mass destruction, but still insisted that he was right to overthrow the dictator**. "I can regret the mistakes and I can regret many things about it but I genuinely believe, not just that we acted out of good motives, and I did what I did out of good faith, but I sincerely believe that we would be in a worse position if we hadn't acted that way," he told the BBC Radio 4 Today programme. Mr Blair denied that he had not challenged the intelligence reports more rigorously because he wanted to believe what they were telling him about Saddam's supposed Weapons of Mass Destruction (WMD) to justify going to war.

Exposed: MI5, GCHQ have 15 secret bulk data collection warrants in force
RT (Russia), Staff report, 2016 07 07
London - **Fifteen "secret warrants" are in force to enable British intelligence services to collect bulk data about online and phone traffic, the Interception of Communications Commissioner's Office (IOCCO) has revealed.** The number of orders imposed on telephone and internet companies under Section 94 of the Telecommunications Act has been published for the first time by the surveillance watchdog. A further eight warrants are in place to provide for emergency services, civil contingencies and to protect security personnel. The directions were acquired by the government's electronic monitoring agency **GCHQ** and the national security service MI5. The watchdog says all Section 94 directions are subject to secrecy restrictions, which severely limits what it is able to say about the directions and the actions taken as a result of them.

MI6 must learn how to tell a spy from a fabricator
London Times, Ben Macintyre, 2016 07 07
Column - **Chilcot focuses closely on the MI6 report from September 11, 2011 heralding a "significant breakthrough" after recruiting a spy in Iraq** with "phenomenal access" who might be the "key to unlock" Saddam's biological and chemical weapons programme. In the words of Chilcot, Britain's spymasters already held the "ingrained belief" that Saddam was concealing weapons of mass destruction. The new spy merely fed into that certainty. The highly placed source reported that Iraq had accelerated production of chemical and biological agents, built new facilities across the country and "was concentrating its efforts on the production of anthrax". A second "high impact" report from the same source, circulated by MI6 two weeks later, stated that sarin and other nerve agents were being stored in "hollow glass spheres". But this Iraqi source was a fake who, like Wormold, was spinning his fiction out of whatever came to hand, in his case Hollywood movies. All intelligence services are vulnerable to the danger of

imagining the truth and then luring the available information towards it. **The Iraq defector codenamed "Curveball" by the CIA claimed to have worked in one of Saddam's mobile biological weapons labs and provided key "evidence" in the build-up to the Iraq War**. Rafid Ahmed Alwan was finally revealed to be a taxi driver who had spun his engineering knowledge into a devastatingly damaging con trick.

Spy chiefs were too eager to please with flawed weapons intelligence
London Times, Sean O'Neill, 2016 07 07
London - **Britain's spy agencies bolstered Tony Blair's desire to go to war in Iraq with "flawed intelligence", the Chilcot report concludes**. It paints a picture of intelligence chiefs who appeared all too eager to please the prime minister with information on Saddam Hussein's access to weapons of mass destruction (WMD), which was discredited and withdrawn within two years. **Sir Richard Dearlove, former chief of MI6, and John Scarlett, head of the joint intelligence committee in the months before the invasion, are criticised**. Both had an "ingrained belief" that Saddam had WMD stocks, the inquiry found, and no effort was made to examine the possibility, which turned out to be true, that those weapons had been destroyed after the first Gulf War. Sir John Chilcot said yesterday:

The Rock movie plot 'may have inspired MI6 source's Iraqi weapons claim'
The Guardian (London), Peter Walker, 2016 07 07
London - An **allegation in an MI6 report about Iraq's supposed chemical weapons capability before the 2003 war to remove Saddam Hussein appeared to have been lifted from a Hollywood film, according to the Chilcot report**. A section of the inquiry's findings about the build-up to the conflict in the autumn of 2002 found that MI6, formally known as the Secret Intelligence Service or SIS, feared a source might have taken inspiration from The Rock, a 1996 thriller starring Sean Connery and Nicolas Cage. The report details how MI6 sent information to "a small number of very senior readers", including Tony Blair and the then foreign secretary, Jack Straw, on 11 and 23 September 2002. **Based on what MI6 called "a new source on trial with direct access", this alleged that Saddam's government had accelerated the production of chemical and biological agents,** and in particular that chemical agents might be carried in glass containers. After some discussion on the reliability of the new source, in early October MI6 was questioned directly about this idea.

MI5 officers 'bound' to report abuse if evidence uncovered, Kincora inquiry told
Belfast Telegraph, Staff report, 2016 07 06
Belfast - A **retired MI5 officer has insisted the Security Service would have been duty bound to take action if it uncovered evidence of abuse at Kincora boys' home**. The officer, known as 9347, was giving evidence to the Historical Institutional Abuse (HIA) inquiry, which is examining claims that intelligence agencies covered up the crimes committed by a paedophile ring in the east Belfast home in order to blackmail some alleged high- profile abusers. Three senior care workers **Joseph Mains, Raymond Semple and William McGrath were convicted for abusing boys at Kincora in 1980**, but it has long been alleged that other more prominent figures, including politicians, judges, civil servants and police officers, were also involved. It has also been claimed that McGrath, who had links to a shadowy Protestant paramilitary organisation known as Tara, was working as an MI5 agent.

None of MI6 and MI5's senior officials are from BAME backgrounds
The Guardian (London), Alice Ross, Owen Bowcott, 2016 07 05
London - **None of the senior officials in MI5 or MI6 are from minority ethnic backgrounds, according to diversity figures released by parliament's intelligence and security committee.** Details of the more than 16,000 spies and personnel in Britain's intelligence

apparatus have been released in the committee's annual report. The overall budget of the Single Intelligence Account - which covers expenditure on MI5, MI6 and the government monitoring service GCHQ - rose to £2.63bn last year. In the previous year, it was £2.48bn; in 2010, it stood at £2bn. The smaller agencies, Defence Intelligence, the National Security Secretariat, the Joint Intelligence Organisations and the Office for Security and Counter-Terrorism, cost £1.16bn in 2014-15. The latest figures show that 27% of senior roles in MI5 are held by women but none by those from black, Asian or minority ethnic (BAME) backgrounds. For MI6, 20% of its senior officials are women but none are from BAME backgrounds. Within GCHQ, 18% of its senior staff are women and 2% from a minority ethnic background.

Spy agencies 'produced flawed information on Saddam's WMDs'
The Guardian (London), Ewen MacAskill, 2016 07 06
London - The Chilcot report identifies a series of major blunders by the British intelligence services that produced "flawed" information about Saddam Hussein's alleged weapons of mass destruction (WMDs), the basis for going to war. **The intelligence community emerges from the report with its reputation and some of its most senior staff badly damaged.** The report singles out for criticism Sir John Scarlett, the chairman of the joint intelligence committee (JIC), an umbrella group that pulls together the work of the main intelligence agencies, mainly the findings of the overseas service, MI6. The then MI6 chief, Sir Richard Dearlove, also comes in for criticism. In one of the most damning sections, the report concludes that Tony Blair presented the assessments of the spy agencies to parliament with a "certainty" not justified by the intelligence that had been gathered.

Return to Table of Contents/ Retour à la table des matières

Australia/ Australie

Terrorist trap sprung
The Herald-Sun, James Dowling, 2016 07 05
Sydney—Would-be terrorists are being caught up in airport stings as they try to join extremist groups overseas. **Security agencies secretly cancel the passports of would- be foreign fighters**, allowing them to go to the airport where they are intercepted, questioned and have their electronic devices scanned for information. Even if they are not charged, the airport stops can lead to an **intelligence windfall**. Australian Federal Police deputy commissioner Neil Gaughan revealed the tactic while giving evidence in an application for a control order last month. The **AFP** is trying to place a number of conditions on **Harun Causevic**, who had terrorism charges dropped against him after he was arrested during the Anzac Day raids last year. Mr Causevic — whose passport was cancelled — made similar humanitarian searches. He also searched for information about the **AFP and ASIO**.

Return to Table of Contents/ Retour à la table des matières

New Zealand/Nouvelle-Zélande

It costs to keep tabs on twitter
The Press (Christchurch), 2016 07 08
Auckland— **Government department has revealed it spends $35,000 of taxpayers' money a year on social media monitoring tools, while others are happy using free software**. But

the departments you would expect to be the biggest spenders on social media monitoring - our Government spy agencies - are keeping mum on just how much they pay for such technology. Information released under the **Official Information Act** showed the Ministry for Primary Industries paid US$25,000 (NZ$35,000) a year in licensing costs to use a web-based social media monitoring tool called Crimson Hexagon. The **country's two spy agencies, the Government Communications Security Bureau and the Security Intelligence Service refused to provide information on their use of social media monitoring tools or services, citing national security**.

Return to Table of Contents/ Retour à la table des matières

International

China/Chine

ICIT Report: Despite pact with U.S., China continues to steal intellectual property
SC Magazine, Bradley Smith, 2016 07 12
New York - A **new report released today from the Institute for Critical Infrastructure Technology (ICIT) warns that China's five-year plan for the years 2016-2020 is heavily reliant upon the digital theft of Western nations' intellectual property,** despite the 2015 Sino-U.S. pact to eliminate cyberattacks against corporate assets. Entitled China's Espionage Dynasty: Economic Death by a Thousand Cuts, the paper looks to paint a comprehensive portrait of China's cyberspy program through the aggregation of reports from the U.S. government, cybersecurity firms and independent sources. The ICIT will present its findings in Washington D.C. on July 28 before an audience of federal agencies and critical infrastructure private-sector organizations. In September 2015, the U.S. and **China publicly agreed not to digitally spy on each other for commercial gain**. "While it is possible that China has reduced its targeted attacks against American organizations, it seems more likely that it restructured its cyber operations to assert greater control over its operatives," the report concludes. In other words, the report states, China may have reined in its most obvious threats, while continuing to infiltrate Western businesses with more advanced, virtually undetectable advanced persistent threat (APT) attacks.

Ye Xuanning, son of national founding father, led PLA intelligence wing
South China Morning Post, 2016 07 11
Beijing-- **Ye Xuanning, a son of a founding father of the People's Republic of China and who led a national military intelligence department, died yesterday at 77, mainland media reported**. Ye died of an unspecified illness in Guangzhou in Guangdong province, according to Shanghai-based ThePaper.cn. Although Ye did not rise as high as his elder brother Ye Xuanping, who was provincial governor during the early years of market reforms from 1985 to 1991, he became an important figure in the People's Liberation Army. Ye was in charge of the Liaison Department of the General Political Department for seven years until 1997, when he retired from the military at the rank of general. The liaison wing was responsible for collecting and analysing intelligence, with events in Taiwan being a chief concern.

Return to Table of Contents/ Retour à la table des matières

Russia's FSB Didn't Open Espionage Case Against Opposition Figure Navalny
Sputnik (Russia), Staff report, 2016 07 12
Moscow - The **Russian Federal Security Service (FSB) confirmed it had not opened a criminal case against Russian opposition figure Alexei Navalny on espionage allegations**. The document with the FSB's confirmation was attached to the civil lawsuit case filed by Navalny against Russia's state-run broadcaster VGTRK, which on April 10 aired a preview of a documentary on its show Vesti Nedeli, claiming that Navalny had received money from the UK intelligence service MI6, a RIA Novosti correspondent reported from the court. The request to attach the response from the FSB to the case was filed by Navalny.

Russian Spy In the Cotswolds Who Sent Her Report Back to Moscow Via Her Washington Line
Mail on Sunday, Anne McElvoy, 2016 07 10
Moscow - On aa hot summer's day in wartime, a dapper young woman with a broad smile pushes a bicycle along a quiet lane deep in the Oxfordshire countryside. With her is a nervous-looking man with intense brown eyes. Passers-by notice the couple holding hands. Yet far from being innocent star-crossed lovers, they are two of the Cold War's most important spies, serving Stalin's military intelligence network and betraying some of our vital nuclear secrets to Moscow. The 'romance' is a cover for controller and agent. **The woman is Sonya, the code name of Ursula Kuczynski, of the GRU (Soviet military intelligence) - a German-born illegal living undercover with her British-born husband Len, also a Soviet spy**. She sends secrets back to Moscow with the help of a specially adapted washing line. The man is **Klaus Fuchs**, also a German immigrant. He is a gifted physicist, working on the Tube Alloys project. At the heart of it is the manufacture of pure uranium-235. Tube Alloys would go on to become the basis of the Manhattan Project in Los Alamos, New Mexico, which developed the first nuclear weapon. Its betrayal by Fuchs gave Moscow a leap forward worth at least two years in its nuclear programme. **New material unearthed from MI5 and East German files confirms that both before and after the war, many of Britain's nuclear secrets were betrayed by Fuchs, with Sonya as his controller.**

Russia Expels American Diplomats in Response to U.S. Move
The Wall Street Journal Online, Nathan Hodge, 2016 07 09
Moscow— The Russian **Foreign Ministry said Saturday it had expelled two U.S. Embassy employees amid a feud between Moscow and Washington** over the treatment of American diplomatic personnel. In a statement Saturday, Russian Deputy Foreign Minister Sergei Ryabkov said two U.S. Embassy employees had been declared persona non grata, saying the **two Americans had been conducting "activities incompatible with diplomatic status" in Russia.** Mr. Ryabkov said the move followed the expulsion of two Russian diplomats by the U.S. "The U.S. government demanded the departure of two employees of the Russian Embassy in Washington, D.C., without presenting any specific complaints against them," Mr. Ryabkov said. "And the State Department at a high level asked us not to make this fact public." Saturday's announcement follows official U.S. expressions of concern about alleged Russian harassment of U.S. diplomats. The State Department complained about the treatment of diplomatic personnel public this week after the release of a video on Russian national television that appeared to show a Russian police officer tackling a U.S. official outside the U.S. Embassy in Moscow. Russian Foreign Ministry spokeswoman Maria Zakharova claimed the U.S. official involved in the June **incident was a spy**.

Russian Media Blames U.S. Diplomat for Embassy Incident, Despite Video
Moscow Times, Staff report, 2016 07 08
Moscow - State-**run television channel NTV has aired the video of a Russian FSB guard attacking a U.S. diplomat outside the U.S. Embassy in Moscow, placing the blame on the American man**. The NTV program "Incidents" presented the video as an attack of an "American spy on a Russian policeman." The video commentary closely resembles the remarks of Maria Zakharova, the Russian Foreign Ministry's official spokesperson. The low- quality footage shows a uniformed Russian **Federal Security Service (FSB) guard attack a U.S. diplomat** as he tries to enter the U.S. Embassy. Lunging at the man, the guard appears to be the aggressor in the altercation. Regardless, The NTV correspondent narrates the video in contradiction with the visuals: The diplomat is said to be a spy wearing a suspicious knitted hat over his face -- dashing to get inside the embassy.

Infamous Russian Double Agent Dies In U.S. -- Reports
Moscow Times, Staff report, 2016 07 08
Moscow - A **Russian double agent who fled to the U.S. has died, the Interfax news agency reported Thursday, citing unnamed sources. Alexander Poteyev, a former colonel in Russia's Foreign Intelligence Services (SVR**), handed state secrets to American authorities before fleeing to the U.S. He was subsequently sentenced in absentia to 25 years imprisonment for treason in 2011. The SVR have so far refused to comment on the reports of the former colonel's death, the RBC newspaper reported.

Poteyev to stay on intl wanted list until his death officially confirmed – source
Interfax News Agency, 2016 07 07
Moscow— **Former intelligence service officer and defector Alexander Poteyev, who was sentenced in Russia in absentia to 25 years in prison for high treason, will remain on the international wanted list and will not be removed from it until reports about his death are officially confirmed**, a source familiar with the situation told Interfax. "In the absence of official documents on his death, he is listed as being alive and, consequently, cannot be removed from the international wanted list," he said. Sources told Interfax earlier on Thursday Russia was verifying information that ex-Russian Foreign Intelligence Service officer Poteyev, who had fled to the U.S, had died.

Law enhancing legal regulation of counterterrorism activity
Russian Government News, 2016 07 07
Moscow— **Vladimir Putin signed Federal Law On Amendments to the Federal Law On Counterterrorism and Certain Legislative Acts of the Russian Federation as concerns Introduction of Additional Measures to Counter Terrorism and Guarantee Public Security**. The Federal Law aims to enhance legal regulation of counterterrorism activity. The Law makes amendments to the federal laws On Counterterrorism, On Transport Security, and On Security of Fuel and Energy Sector Facilities. The amendments clarify the grounds for carrying out counterterrorist operations, strengthen the binding nature of antiterrorist commissions' decisions in the Russian regions, defines the powers of local government bodies in this area, and sets out cooperation procedures when investigating information on the threat of unlawful intervention in the operation of transport and energy sector infrastructure. In particular, the provisions of the Law introduce a ban on using the basic components of combat and service firearms in production of certain categories of civilian arms and devices similar in their construction model to arms. The provisions clarify the definition of financing terrorism, establish the right of federal executive bodies responsible for security and the **Russian Federation Foreign Intelligence Service** to receive for free information systems and (or) data bases from state bodies and state extra-budgetary funds, and set additional demands on telecommunications providers and

organisers of information dissemination in the internet and on organisation of transport and logistics activity.

Putin Tasks FSB With Decrypting Russian Messaging Apps
Moscow Times, Staff report, 2016 07 07
Moscow - **Russian President Vladimir Putin has tasked Russia's Federal Security Service (FSB) with finding the encryption keys needed to monitor the country's online messaging**, the Meduza news website reported Thursday. The FSB have been given two weeks to find the keys, which will make it possible to implement controversial new anti-terror legislation. Alexander Bortnikov, head of the FSB, has been charged with overseeing the task, Meduza reported. Increased government surveillance forms part of the anti-terrorism package authored by ultra-conservative United Russia deputy Irina Yarovaya. The legislation requires all internet messaging platforms which employ additional encryption to supply the FSB with information on how to decode all messages on the platform. If companies do not apply, they can be fined up to 1 million rubles ($15,000), Meduza reported.

Return to Table of Contents/ Retour à la table des matières

Europe

Terrorisme: les sombres prédictions du directeur de la DGSI
Le Figaro, Christophe Cornevin, 2016 07 12
Paris - **Patrick Calvar, le patron du renseignement intérieur en France, est «persuadé» que Daech va faire évoluer son mode opératoire en France pour éviter «d'aller à l'assaut avec la mort à la clef».** Il craint notamment que l'organisation terroriste passe «au stade des véhicules piégés et des engins explosifs». Les terroristes de Daech qui ont endeuillé le pays en mitraillant les terrasses et le Bataclan, puis en menant des attaques kamikazes au Stade de France en novembre dernier pourraient encore intensifier leurs frappes en changeant de méthode. Cette sombre hypothèse est celle de Patrick Calvar, directeur général de la sécurité intérieure (DGSI). Dans une audition menée à huis clos le 24 mai dernier à l'Assemblée nationale par la commission d'enquête relative aux moyens mis en oeuvre par l'État pour lutter contre le terrorisme depuis le 7 janvier 2015, ce professionnel incontesté l'assure: **«Je suis persuadé qu'ils passeront au stade des véhicules piégés et des engins explosifs, et ainsi qu'ils monteront en puissance». «Ils vont finir par projeter des commandos dont la mission consistera à organiser des campagnes terroristes sans nécessairement aller à l'assaut avec la mort à la clef.»** «Pour cela, il leur faut des artificiers et organiser toute une logistique, c'est-à-dire s'installer sur notre territoire, acquérir tous les produits», poursuit Patrick Calvar.

Sources humaines, chiffrement... les lourds défis de la DGSI
Le Figaro, Christophe Cornevin, 2016 07 12
Paris - Confrontée à la fois à une menace extraordinairement complexe et à une recomposition du paysage du renseignement français depuis quelques années, la **Direction générale de la sécurité intérieure (DGSI) doit à la fois être le fer de lance de la lutte antiterroriste tout en menant une profonde métamorphose pour accompagner sa montée en puissance**. Là réside peut-être l'un de ses principaux défis. « La croissance en effectifs, sur une période de cinq ans, sera de près de 40 % » , a déclaré le 24 mai à l'Assemblée Patrick Calvar, patron d'un service dont les effectifs, de 3 000 agents aujourd'hui, ont déjà été musclés par trois plans de recrutements avant de franchir la barre des 4 000 en 2018.

Les trois failles de l'antiterrorisme selon le patron de la DGSI
Ouest-France, Journaliste maison, 2016 07 12
Paris - **Les services du renseignement intérieur sont confrontés à trois défis majeurs dans la lutte antiterroriste, a estimé le 24 mai leur patron Patrick Calvar devant la commission d'enquête parlementaire sur les attentats de 2015 en France**. Son audition, à huis clos, a été rendue publique ce mardi. Les limites du contrôle judiciaire Pour la commission, le cas de Samy Amimour, assaillant du Bataclan qui a pu aller en Syrie en 2013 malgré une mise en examen et une interdiction de sortie du territoire, est « emblématique des défaillances du contrôle judiciaire » . **Pour ne pas porter « atteinte aux droits de la défense » , les services ne peuvent « plus suivre ni intercepter les gens les plus dangereux dès lors qu'ils sont mis en examen ; à moins, s'ils sont impliqués dans un autre projet, qu'une autre enquête soit ouverte »** , a expliqué M. Calvar, directeur général du renseignement intérieur (DGSI), interrogé sur le suivi d'Amimour. « Il s'agit d'un angle mort » , a-t-il estimé, ajoutant qu' « il appartient à un contrôle judiciaire de permettre le suivi de l'intéressé ».

Renseignement : pas touche aux documents secrets du Squale !
Le Point, Mélanie Delattre avec Christophe Labbé, 2016 07 12
Paris - La **justice n'aura pas accès aux documents classifiés retrouvés chez Bernard Squarcini, l'ancien patron du renseignement intérieur**. L'histoire d'un maître espion rattrapé par la justice aurait pu faire un bon polar. Sauf qu'elle est bien réelle et qu'elle concerne l'ancien directeur du renseignement intérieur de Nicolas Sarkozy. **Bernard Squarcini actuellement visé par plusieurs enquêtes. Au départ, il y a ce courrier reçu par le juge Serge Tournaire.** Dans la lettre adressée au magistrat, un fonctionnaire de police évoque des écoutes téléphoniques dont il aurait été victime alors qu'il enquêtait sur le Wagram, un cercle de jeu parisien tenu par des Corses. Plusieurs policiers du service des courses et jeux auraient fait l'objet de « zonzons » de la part de la Direction centrale du renseignement dirigée à l'époque par Bernard Squarcini, lequel était réputé proche d'un des deux clans se disputant le contrôle de l'établissement.

A Genève, le chef de l'armée évoque la cybersécurité
Tribune de Genève, Journaliste maison, 2016 07 12
Genève - André Blattmann était hier l'invité du Club suisse de la presse à Genève. **L'armée suisse est bien protégée contre les cyberattaques, estime son chef, André Blattmann**. Mais après l'affaire Ruag, la lutte contre cette menace potentielle envers des infrastructures critiques restera prioritaire. Plus de 30 000 ordinateurs sur le réseau de l'armée ont été contrôlés après l'attaque qui a visé l'entreprise d'armement de la Confédération, a déclaré hier devant la presse à Genève le chef de l'armée. **Sans qu'aucun virus ne soit trouvé. « L'armée est bien protégée et c'est mon but pour le futur. »**

German spooks monitored EU, NATO government members, report says
DPA News Agency, 2016 07 11
Berlin— New details have emerged on the scale of spying by Germany's foreign intelligence in previous years on members of EU governments and NATO countries in a parliamentary committee report seen by dpa. A "low two-digit number of people" belonging to foreign governments were spied on until October 2013, including heads of states and governments, ministers and members of their offices, as well as members of military institutions, it said. The focus of espionage by the Bundesnachrichtendienst (BND) was on diplomatic representations of EU and NATO member states around the world, making up more than two thirds of all 3,300 targets.

New head of German intelligence service officially installed
dpa News Agency, Staff report, 2016 07 07
Berlin - **Germany's BND intelligence service is "as important today as hardly ever before in history"** German Chancellor Angela Merkel's chief of staff, Peter Altmaier, said on Wednesday as he **officially installed Bruno Kahl, 53, as the new head of the service**. Altmaier stressed the service's increased importance given the heightened threat from international crises, terrorism and cyberattacks. Former senior civil servant Kahl said Wednesday he would work hard to rebuild the trust that had been lost in the service among the German population and the country's international intelligence partners. **Kahl pledged on Wednesday that he would continue his predecessor's moves towards transparency for the service.**

Raid, BRI, GIGN... Les forces d'intervention d'élite peuvent- elles vraiment fusionner ?
FranceTv Info (site web), Journaliste maison, 2016 07 07
Paris - La **commission d'enquête sur l'action de l'Etat face aux attentats parisiens**, qui a présenté ses conclusions mardi, soulève cette épineuse question. Ils sont vêtus de noir, cagoulés et casqués, lourdement armés et parfois protégés par un bouclier. Les hommes des forces d'intervention spéciales françaises se ressemblent à s'y méprendre. A **un détail près, leur écusson. Les uns arborent le parachute blanc du GIGN, les autres la panthère noire du Raid ou la gargouille à l'oeil rouge de la BRI.** La différence entre ces trois unités d'élite ne se limite pas à leur blason, loin de là. Leur histoire, leur savoir-faire et leur périmètre d'intervention les caractérisent.

Bulgaria's Govt OKs Controversial Anti-Terror Bill
Sofia News Agency, Staff report, 2016 07 06
Sofia - The **government of Bulgaria has adopted draft legislation that gives law enforcement and security agencies rights to curb civil liberties in case of a terror emergency**. Apart from giving sweeping powers to the military, police and other officials in case the highest alert is triggered, the bill also sets up a National Counter-Terrorism Center with the security and **counter-intelligence body DANS (State Agency for National Security).** The Bulgarian Armed Forces will be included in a national counter-terrorism plan and will intervene when a threat is detected or in the event of a terror act, when they will also help deal with the aftermath. Institutions, schools and kindergartens will be obliged to develop and apply anti-terror measures, according to the proposal.

Antiterrorisme : " Il y a eu des failles de nos services "
Le Monde, Hélène Bekmezian, 2016 07 06
Paris - Les **responsables de la commission d'enquête parlementaire pointent du doigt les faiblesses du renseignement pénitentiaire**. A l'issue d'un travail qu'ils ont voulu " au-delà des clivages politiques ", le président et le rapporteur de la commission d'enquête " relative aux moyens mis en oeuvre par l'Etat pour lutter contre le terrorisme depuis le 7 janvier 2015 " présentent leurs conclusions, dans leur rapport adopté mardi 5 juillet. Au terme de votre enquête, êtes-vous en mesure de dire si les attentats du 13 novembre auraient pu être évités ? Y a-t-il eu des failles? Sébastien Pietrasanta (PS, Hauts-de-Seine), rapporteur. Il est facile de réécrire l'histoire quand on connaît la fin. **Même les Etats-Unis n'ont pas pu éviter le terrible attentat d'Orlando malgré les moyens immenses dont ils disposent**.

Doubts weigh on France's push for a more-unified intelligence system
Washington Post, James McAuley, 2016 07 06
Paris - On Tuesday, **French lawmakers announced the results of a six-month inquiry into their nation's intelligence services**, still reeling from two deadly terrorist attacks in 2015. The

major recommendation of the committee: **Create a unified intelligence structure better equipped to prevent future attacks**. In January 2015, extremists attacked the editorial offices of the satirical publication Charlie Hebdo and, two days later, a kosher supermarket on the outskirts of Paris. On Nov. 13, militants with ties to the Islamic State killed 130 people in coordinated attacks across the city. In both cases, the inquiry's leaders acknowledged Tuesday, the perpetrators were previously known to authorities. Some were under judicial surveillance at the time, while others had prior convictions.. **Georges Fenech, a conservative member of France's National Assembly who spearheaded the inquiry, placed the bulk of the blame on what he called the country's overly complicated intelligence apparatus**, an overlapping structure of various agencies that are not always in contact with one another.

French Inquiry on Terror Urges Changes to Intelligence Agencies
New York Times, Aurelien Breeden, 2016 07 06
Paris - A **parliamentary committee examining two devastating terrorist attacks in France last year called on Tuesday for the nation's intelligence agencies to be streamlined and merged, finding widespread failures** in the collection and analysis of information that could have helped prevent the attacks. Among 40 proposals, **lawmakers urged the government to merge some of France's overlapping and sometimes competing agencies and to create a new national agency -- like the National Counterterrorism Center that the United States established after the Sept. 11, 2001, attacks** -- reporting directly to the prime minister. It also urged the government to set up a shared antiterrorism database; to better monitor prisons, where radicalization of inmates is a major problem; and to tighten the sentencing of convicted terrorists. The nonpartisan committee included lawmakers from France's two largest parties, the Socialists and the center-right Republicans. It offered the most definitive account so far of the 2015 attacks, and of the intelligence failures preceding them, but was more limited in scope than the 9/11 commission. It did not have access to classified documents, **although it held several closed-door meetings with intelligence and security officials.** Judicial and criminal investigations into the attacks are continuing. While the recommendations are not binding, they are likely to add to the pressures confronting President François Hollande, a Socialist, who is expected to pursue re-election next year despite abysmal popularity ratings.

Terrorisme : les propositions de la commission Fenech
Le Figaro, Paule Gonzalès avec Jean-Marc Leclerc, 2016 07 06
Paris - **Pour éviter un nouveau 13 novembre, le président de la commission d'enquête parlementaire sur les attentats propose une révolution dans les structures spécialisées**.
Sécurité « Devant le Bataclan, le 13 novembre, les policiers de la BAC, arrivés les premiers, voulaient au moins que les militaires de l'opération « Sentinelle » , arrivés sur place, leur prêtent leurs fusils d'assaut Famas, puisque les militaires n'avaient pas le droit de tirer. Et ils ont essuyé un refus ! » Le député les Républicains **Georges Fenech**, président de la commission d'enquête parlementaire sur les attentats de 2015 en France, ne décolère pas contre les « aberrations » mises au jour au fil de ces cinq mois d'auditions. **Son but : « Comprendre comment les auteurs des pires attaques terroristes que l'Hexagone ait connues depuis l'après-guerre ont pu se déplacer à leur guise, alors qu'ils étaient, dans leur quasi-totalité, fichés, surveillés, condamnés ou sous le coup d'un mandat d'arrêt. »**

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Abadi Sacks Top Baghdad Security Officials
Asharq Al-Awsat, Hamza Mustafa, 2016 07 11
Baghdad - **Only one day after accepting the resignation of Interior Minister Mohammed Salem al-Ghabban, Iraqi Prime Minister Haidar al-Abadi sacked a number of high-ranking officials responsible for security in Baghdad, including the head of the Baghdad Operations Command**. Minister Ghabban resigned after the Karrada terrorist bombing that killed 300 and injured over 200 civilians. A statement issued by Abadi's office said that the prime minister had dismissed the head of the Baghdad Operations Command Abdul Amir al-Shammari and commanders of military operations, security services and intelligence in the capital. Minister Gabban told Asharq Al- Awsat newspaper that the **security of Baghdad falls under the responsibility of Baghdad Operations Command.** Abadi didn't announce any alternatives for both positions of Interior Minister and head of Baghdad Operations Command.

911 now includes all security agencies
Arab News, Staff Report, 2016 07 06
Riyadh - **Maj. Gen. Abdul Rahman bin Mohammed Al-Saleh, chief of National Security Operations Center at the Ministry of Interior, said that the unified security operations center, 911, now includes all the relevant security agencies for emergencies**, such as security patrols, traffic, road safety, and Civil Defense. He stressed that it facilitates the coordination between the relevant parties and prevents duplication or conflict of jurisdiction. Saleh said during a phone interview on Al-Ekhbariya TV channel that the new program now includes major partners such as the Saudi Red Crescent Society, the Ministry of Health, Ministry of Water, Environment and Agriculture, and the Ministry of Transport, along with many other bodies such as government secretariats.

Return to Table of Contents/ Retour à la table des matières

Asia/Asie

Two Koreans indicted after spying for Pyongyang
Korea JoongAng Daily, 2016 07 13
Seoul—**Prosecutors on Monday indicted two South Koreans for making reports on domestic affairs to be sent to North Korea and for writing documents extolling the Communist regime**. One of the two indicted suspects is a 52-year-old man surnamed Kim who was arrested at an internet cafe in Seoul on May 24. Another suspect is Kim's accomplice, a man surnamed Lee, 54, who was apprehended in Ansan, Gyeonggi, on the same day. The **National Intelligence Service** reported earlier this month that Kim was arrested as he was trying to send his espionage reports in an email to his contact in North Korea. The NIS took the unusual step of showing recorded footage of the apprehension to members of the parliamentary intelligence committee on July 1 to prove they had taken legal due process for the arrest, such as showing an arrest warrant issued by a court. The **Seoul Central District Prosecutors' Office reported Tuesday that the two men were suspected of having contacted North Korean agents** dispatched by the clandestine 225th Bureau under the Workers' Party of Korea in Pyongyang in March 2014 and last August.

Japan to add more terrorism analysts after Dhaka attack
Nikkei Report, 2016 07 12
Tokyo— The **Japanese government decided Monday to ramp up an anti-terrorism unit's intelligence-gathering capabilities in response to the recent incident in Bangladesh**. The information collection and analysis unit draws staffers from the foreign and defense ministries as

well as the **National Police Agency and the Cabinet Intelligence and Research Office**. It now has about 20 people stationed abroad, with another 20 or so traveling overseas from Tokyo to gather information. The unit will strengthen its presence in the Middle East and Asia, though the scale of the expansion has yet to be determined.

Dhaka attack exposes shortcomings in Bangladesh's security apparatus
Times of India, IndraniBagchi, 2016 07 07
Dhaka - The **Bangladesh government came in for some sharp responses from the foreign diplomatic community over the terror attack in Dhaka** area last week. At a briefing for foreign diplomats by the foreign office here, among expressions of sympathy and solidarity, the Sheikh Hasina government was at the receiving end of some home truths. **Most important is a concern by some countries that if foreigners' security cannot be guaranteed**, it would affect foreign investment in Bangladesh's crucial garment and textile industry. Certainly the Japanese and Europeans would be affected. **Countries like US have offered assistance in counterterrorism and tech-intelligence cooperation**. However, Dhaka has been wary of accepting many of them for several reasons like Washington has in the past tried to pressure Hasina to come to a political "understanding" with Khaleda Zia of BNP. Hasina has refused to give in to the pressure.

Malaysia must share intelligence resources with other nations to tackle IS threats
New Strait Times, Beatrice Nita Jay, 2016 07 07
Putrajaya - The **terror attacks by the Islamic State (IS) is a new phenomenon faced by Malaysia which needs exchange of intelligence with various countries, said Defence Minister Datuk Seri Hishammuddin Hussein**. "This attack requires us to share intelligence with authorities from Belgium, France as well as Saudi Arabia. "We are used to Al Qaeda and Jemaah Islamiah but the threat posed by IS is different from what we faced before. These are things that we must not take for granted," said Hishammuddin at the Hari Raya open house hosted by Prime Minister Datuk Seri NajibRazak, today.

Helal appointed defence minister deputy for strategic intelligence affairs
Pajhwok Afghan News, Pajhwok Report, 2016 07 07
Kabul - **HilaluddinHelal has been appointed Defence Minister assistant to the strategic intelligence department in the rank of General in line with presidential order**, a statement from the Presidential Palace said on Thursday. The Strategic Intelligence post has been newly created in the hierarchy of ministry of defence. Earlier, **Helal served as commander in the air force and deputy security in charge in the Ministry of Interior (MoI)**. He completed higher education in military and remained a brave military officer in the past. Helal also served as Wolesi Jirga member from Baghlan.

Former, current lawmakers acquitted of detaining intelligence agent
Yonhap News Agency, 2016 07 06
Seoul--A **Seoul court acquitted four former and current opposition lawmakers Wednesday on charges of illegally detaining an intelligence agent before the last presidential election**. Rep. Lee Jong-kul of the Minjoo Party of Korea and three others who were formerly affiliated with the party were indicted in 2014 on charges of unlawfully detaining the female agent in her home in Seoul for about 35 hours in December 2012. The agent allegedly took part in the intelligence agency's operation to influence public opinion on the internet ahead of the critical vote. The Seoul Central District Court found the defendants not guilty, saying the agent, identified only by her surname Kim, was not held in captivity as she could have left the house if she wanted.

Diplomats dismayed by security lapses
Bangladesh Daily Star, Rezaul Karim, 2016 07 06
Dhaka - **Expressing serious concern over the systematic attacks and gradual escalation of terrorism and violent extremism, foreign diplomats in Dhaka today stressed the need for more effective security steps**. They also expressed their dismay over militants' targeting foreigners in Bangladesh, especially those who had come to Bangladesh with intent to help the country in socio-economic development, poverty alleviation, infrastructure development and business. Taking part in a discussion at a diplomatic briefing arranged by the foreign ministry at State Guesthouse Padma in the morning, the diplomats called for conducting transparent investigation, maintaining the international standard, into the July 1 terrorist attack on the Holey Artisan Bakery in Gulshan. **A source who attended the meeting said an ambassador told the discussion that the Bangladesh government did not follow up with the intelligence information** on terrorism it was provided by other states as warnings.

Return to Table of Contents/ Retour à la table des matières

Africa/Afrique

FG appoints new CDI
The Sun (Nigeria), 2016 07 09
Lagos—The Federal ederal Government yesterday **appointed a new Chief of Defence In-telligence (CDI) for the armed forces. He is Air Vice Marshal Mohammed Saliu Usman.** He takes over from Ma-jor General John Sarduana Davies, who had been acting since January this year, when the former CDI, Air Vice Marshal Monday Morgan retired. According to the Armed Forces Stat-utes, the position of **Chief of Defence Intelligence** (CDI), which is the apex in the intelligence community, is ro-tational among the services. With the Army and the Navy serving their terms of three years, it fell on the Air Force but AVM Morgan who got appointed when President Muhammadu Buhari assumed office in 2015, was caught up with (ROD), 'run out date' and had to retire.

Bujumbura rejette un rapport de Human Rights Watch accablant ses services secrets
Panapress, 2016 07 11
Bujumbura, Burundi— Le **gouvernement burundais a rejeté** en bloc, lundi, **un récent rapport de «Human Rights Watch» (Hrw) sur de «graves abus» imputables aux agents du pouvoir** qui ont frappé des opposants en détention «à coups de marteau et de barres en acier, leur ont planté des barres en acier aiguisées dans les jambes, ont versé du plastique fondu sur eux, ont noué des cordes autour des parties génitales des hommes et leur ont envoyé des décharges électriques" entre avril 2015 et avril 2016. Le rapport d'enquête soutient encore que «certains détenus qui ont été torturés ou blessés se sont vu refuser des soins médicaux et de nombreux détenus ont été maintenus dans des cachots malodorants et dépourvus de fenêtres ».«Des **agents du service national de renseignement** traitent certains opposants présumés, à leur siège ainsi que dans les lieux secrets, de façon effroyable parce qu'ils savent qu'ils peuvent le faire en toute impunité au lieu que le gouvernement devrait faire cesser la torture immédiatement», peut-on encore lire dans le rapport daté du 7 juillet dernier. Le gouvernement burundais s'offusque aussi du fait que Hrw ne mentionne «nulle part dans ce rapport», les réfugiés burundais enrôlés et entraînés au Rwanda, «dont des enfants mineurs», pour attaquer le Burundi.

Burundi intelligence services torture detainees, report says
Associated Press, 2016 07 07

Kampala— **Human Rights Watch says Burundi's intelligence services have tortured scores of suspected government opponents at their headquarters and in secret locations**. The rights group reported Thursday that abuses often have been carried out in collaboration with members of a pro-government youth militia group known as the Imbonerakure. Burundi has been chaotic since April 2015, when President Pierre Nkurunziza announced plans to seek a third term that he ultimately won. Hundreds of people were killed as security forces tried to quell protests.

Israel and Kenya to boost security partnership in terror fight
Business Daily (Kenya), 2016 07 05
Nairobi— **Kenyan security troops are set to benefit from increased training, equipment and intelligence sharing with Israel** to boost their combat capability in the war against terrorism. President Uhuru Kenyatta said Tuesday that visiting Israeli Prime Minister Benjamin Netanyahu had pledged this in their bilateral meeting to further help strengthen Kenya's army. Nairobi already receives military support from Tel Aviv. Mr Netanyahu is on a three-day state visit to Nairobi. "We have established partnership in fighting terrorism and we will benefit from strategic intelligence," said Mr Kenyatta in a televised joint briefing at State House. Kenya has recently suffered a spate of deadly bomb and gun attacks on civilians and soldiers by Somalia-based Al Shabaab militants who are demanding removal of Kenyan troops from the horn of Africa State. **Israel boasts of Mossad**, the country's intelligence agency, which gathers information to pre-empt terror attacks.

Return to Table of Contents/ Retour à la table des matières

Americas/Amériques

Parrilli slams 'psychopath' Stuiso after ex-spymaster lets rip at CFK
Buenos Aires Herald, 2016 07 12
Buenos Aires—**Former spymaster Antonio "Jaime" Stiuso played down his role in covert intelligence operations during the last decade and levelled explosive accusations against Cristina Fernández de Kirchner** and her administration in a rare interview published yesterday. The former **Operations chief of the Intelligence Secretariat (SI, formerly SIDE),** who fled the country after becoming one of the most sought-after witnesses in the investigation into the death of AMIA special prosecutor Alberto Nisman, claimed that the former Victory Front (FpV) adminstration had operpation a parallel intelligence system that persecuted him. His statements were denied later in the day by former Federal Intelligence Agency (AFI) chief Oscar Parrilli, who occupied the head of the intelligence agency following Stiuso's removal.

An extensive intelligence background
Buenos Aires Herald, 2016 07 12
Buenos Aires—**Antonio "Jaime" Stiuso**, 62, is a **former operations chief of Argentina's domestic intelligence service previously called SIDE** and later the Intelligence Secretariat (SI). A communications expert, Stiuso joined the SIDE in 1972 aged 18 and remained at the organization throughout the last military dictatorship (1976-1983) when it carried out sweeping clandestine surveillance operations on the domestic population. After the return to democracy, Stiuso rose through the ranks of the secretariat to become Operations chief. **He remained at the pinnacle of the organization until his sacking by the Fernández de Kirchner administration in December 2014.** In the weeks following the death of AMIA special prosecutor Alberto Nisman in January, 2015, soon after Stiuso's departure from the

government, the former spy chief fled the country, prompting CFK to accuse the United States of hiding him during her final address to the United Nations General Assembly last year.

Honeymoon in hell: U.S. newlywed jailed in Venezuela as possible spy
Miami Herald, Jim Wyss, 2016 07 08
Caracas - **Joshua Holt, a former missionary from Utah, traveled to Venezuela on June 11 with one plan in mind: marry the woman he'd fallen in love with and take her and her two girls back to the United States**. Instead, **Holt and his wife, ThamaraCaleño, are being held by military intelligence - - and may face charges of terrorism, espionage and illegal possession of weapons after authorities** found two automatic rifles and a hand-grenade in their apartment. But his real crime, said a woman who was present when he was detained, was being a U.S. citizen. And she claims that she and four others saw security forces plant the weapons in the apartment to frame the 24-year-old man. "The only reason they have him is because he's a gringo," said the woman, who asked the Miami Herald not to use her name for fear of retaliation. "I don't care what color his eyes are, what color his hair is, where his passport says he's from -- he's innocent and his human rights are being violated."

Rio Olympics: Brazil vows to be ready in case terror strikes
CNN, Tiffany Ap, 2016 07 07
Rio de Janeiro— Rio de Janeiro has long had a reputation for dangerous favelas, with muggings and kidnappings not uncommon. But authorities are stepping up measures to tackle a different kind of security threat altogether when the Rio Olympic Games begin August 5. **Wary that the international sporting event is a potential prime target for terrorists, Brazilian forces have been working with specialist French SWAT teams** to simulate attack scenarios. In one drill, Brazil special forces and a police dog chase down an armed gunman to thwart a possible attack on Rio's subway system. The dramatic display is meant to reassure journalists that a country with limited experience in handling terrorism is ready for the unthinkable. "There is not a specific threat," said Lt. Gen. Luiz Linhares with the Brazilian Ministry of Defense. "You have to screen for a great (spectrum) of threat." **Brazil's intelligence agency** reported in April that the number of those influenced by ISIS ideology had increased in recent months but insisted there was no threat to the Olympics.

Brazil to strengthen intelligence services
Agencia Brasil, via BBC Monitoring Americas, 2016 07 04
Rio de Janiero-- After 17 years of waiting, the **National Intelligence Policy (PNI)** becomes effective today (30) with the publication of the full text of presidential decree 8,793/16. In an exclusive interview granted to Agencia Brazil, the **incumbent general director of the Brazilian Intelligence Agency [Abin], Wilson Trezza, and the future occupant of the office, intelligence officer Janer Tesch, said that, by approving the PNI, President Michel Temer shows his commitment to strengthen intelligence activity** in Brazil. "We still do not have much to say about Temer's administration because he only took office recently, on 12 May. But he has expressed his commitment to strengthen the intelligence activity, and this decision to approve the PNI is a demonstration that that commitment will materialize," Wilson Trezza said. After eight years as Abin director general, Trezza will hand over his position, in the coming days, to Janer Tesch, who has been an intelligence agent for more than three decades. "I am a professional, with a career of almost 32 years now.

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

20-07-2016 to/au 26-07-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Recruiting changes rile RCMP ranks
National Post, Douglas Quan, 2016 07 25
Vancouver--**An association that represents some of Canada's Mounties says members have "grave reservations" about the RCMP's recent decision to ease entrance requirements, including allowing permanent residents to apply**. **The Mounted Police Professional Association of Canada (MPPAC)** said Sunday management has caved in to political correctness and the "knee jerk" changes amount to lowering standards. "Essentially we face operational security issues as well as serious repercussions in service delivery if we hire people to meet political vs. operational criteria," the association said in a statement through spokesman Rob Creasser.

B.C. judge to rule whether couple was entrapped by police in terrorism sting
Globe and Mail, Sunny Dhillon, 2016 07 23
Ottawa - **John Nuttall and Amanda Korody** were high. In June, 2013, the Muslim converts were at a hotel in the Okanagan city of Kelowna, where they were supposed to be working on a **terrorist plan** to kill revellers and first responders during an attack at the **British Columbia Legislature grounds on Canada Day**. But the husband and wife, heroin addicts who had rarely ventured far from their Surrey basement suite and subsisted on welfare payments, spent much of their time smoking marijuana and playing video games. **The plot was international news**. The couple were found guilty by a jury in June, 2015, of conspiring to murder persons unknown and making or possessing an explosive substance - in both cases for the benefit of or at the direction of a terrorist group. But their convictions have not been entered. **Mr. Nuttall and Ms. Korody have argued that they were victims of police entrapment** and, a year after those arguments began, Justice Catherine Bruce of the B.C. Supreme Court is to deliver her decision at the end of this month. The court heard that the RCMP began looking at Mr. Nuttall after the **Canadian Security Intelligence Service** told the force in early 2013 that he had tried to purchase potassium nitrate, which can be used in explosives.

Darktrace repêche un ancien agent du SCRS
Direction informatique (site web), Dominique Lemoine, 2016 07 20
Toronto - **Darktrace s'implante au Canada avec l'ouverture d'un bureau à Toronto et nomme à la tête de sa direction au Canada un ancien agent de renseignements au service du Canada (SCRS)** et de l'Angleterre (MI5), **David Masson**. Cette multinationale se spécialise en produits de cybersécurité pour les entreprises. Elle a été fondée en 2013 à Cambridge en Angleterre et elle serait née d'une collaboration entre des mathématiciens de l'Université Cambridge et d'anciens agents du MI5, le service de renseignement responsable de la sécurité intérieure au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord.

Electronic spy agency mum on foreign info-sharing that could lead to torture
Canadian Press, Jim Bronskill, 2016 07 20
Ottawa - **Canada's electronic spy agency won't say how often it shares information that could lead to someone being tortured in an overseas prison**. The **Communications Security Establishment** - which monitors threats from foreign terrorists and spies - **has censored documents that spell out the figures, even though the RCMP and Canadian Security Intelligence Service have revealed such numbers in the past.** The reticence

prompted Amnesty International Canada to say "much greater transparency" is needed from the Ottawa-based CSE. "At stake is Canada's compliance with crucial international human rights obligations to prevent torture and ill- treatment," said **Alex Neve**, Amnesty's Canadian secretary general. The secretive CSE has been thrust into the national spotlight in recent years due to leaks by Edward Snowden, the former spy contractor who worked for the National Security Agency, CSE's American counterpart. It is also among a handful of Canadian agencies, including the RCMP, CSIS, the Canada Border Services Agency and National Defence, bound by a government instruction that allows it to share information with foreign partners - even when it means someone could be abused as a result of that exchange. **Public Safety Minister Ralph Goodale** said earlier this year the Liberals will review the "troubling set of issues" raised by the foreign-sharing policy, enacted by the previous Conservative government. Records obtained by The Canadian Press under the Access to Information Act offer a glimpse into how the CSE handled such cases in the first three months of 2015. The quarterly report to **CSE Chief Greta Bossenmaier, l**abelled Top Secret and for Canadian Eyes Only, told her the number of cases that required a "mistreatment risk assessment" and the level of risk associated with passing the information to others. But those details were deleted from the publicly released version of the document. The report says there were "no known instances" of a recipient country's non-compliance with conditions attached to information-sharing during the three months. But little else was disclosed. The CSE faces "unique considerations" it must weigh when discussing details of assessments, said **Christopher Williams**, a senior spokesman for the intelligence agency. "With this in mind, we are not able to release the specific number you have requested without risking revealing insight into our capabilities."

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

Why Experts Are Sure Russia Hacked the DNC Emails

NBC News, Josh Meyer, 2016 07 26

New York - **Many U.S. officials and cyber security experts in and out of government are convinced that state-sponsored Russian hackers** are the ones who stole 20,000 emails from the Democratic National Committee and leaked them to the public just in time to disrupt the Democrats' national convention in Philadelphia. Here's why the experts are so confident the Russians did it: * GEOGRAPHY: At least one of the hacker groups attacking the DNC appeared to cease operations on Russian holidays, and its work hours aligned with a Russian time zone, **cybersecurity company FireEye** concluded in a report. * LANGUAGE: The hackers also left an obvious digital fingerprint, one cybersecurity expert said, perhaps on purpose: a signature in Russia's Cyrillic alphabet. * FORENSIC EVIDENCE: After a different batch of hacked Democratic emails was released last month, a wide spectrum of cyber-security experts concluded that it was the work of Russian intelligence agencies through previously known proxy groups known as COZY BEAR or APT 29, and FANCY BEAR or APT 28.

White House to Issue New Policy for Cyberattack Responses

Wall Street Journal, Damian Paletta, 2016 07 26

Washington - **The White House as soon as Tuesday is expected to issue a new directive on how the government should respond to significant cyberattacks**, two people familiar with the matter said, aiming to end confusion about the responsibilities of agencies involved in security breaches. The new presidential policy directive is a response to the rapid escalation of cyberattacks by criminals and foreign governments that have stolen information from U.S.

companies, citizens and government offices. The policy has been in the works for months, but it will be released at a time when there is an acute focus on the damage caused by cyberattacks. Hackers last year broke into the **Democratic National Committee's network and WikiLeaks** began releasing some internal party emails several days ago. Some of the emails humiliated top DNC officials and led to an uproar at the party's convention in Philadelphia and the resignation of DNC chairwoman Debbie Wasserman Schultz.

WikiLeaks' Julian Assange: 'No Proof' Hacked DNC Emails Came From Russia
NBC News, Alex Johnson, 2016 07 26
New York - **WikiLeaks founder Julian Assange told NBC News on Monday that "there is no proof whatsoever" that his organization got almost 20,000 hacked Democratic National Committee emails from Russian intelligence** --adding it's what's in the emails that's important, not who hacked them. In a Skype interview with Richard Engel for "NBC Nightly News," Assange rejected that it hadn't even been proven that it was WikiLeaks that published some email messages that have been analyzed in outlets like The New York Times. Three cybersecurity experts have told NBC News that the DNC's servers were hacked by Russian intelligence. But Assange said Monday that DNC servers have been riddled with security holes for years and that many sets of documents from multiple sources are now in public hands. "The emails that we have released are different sets of documents to the documents of those [that] people have analyzed," he said.

F.B.I. Examining if Hackers Gained Access to Clinton Aides' Emails
New York Times, David E. Sanger, 2016 07 26
Washington - The **F.B.I. investigation into the suspected state- sponsored Russian theft of emails and documents from the Democratic National Committee's computer networks** has expanded to determine if aides and organizations considered close to Hillary Clinton were also attacked, according to federal officials involved in the investigation. But so far, a sampling of senior Clinton aides at the Democratic National Convention in Philadelphia found none who said they had been notified by the F.B.I. or private investigators that their private emails had been compromised. At this point, law enforcement officials say, there is evidence only of attempts to gain access to those associates through "spear-phishing" attacks, often crude efforts to get someone to click on an email that releases malware into the computer. The committee has said that **Russia hacked** into its computers and has been supported in its assertion by several private cybersecurity firms, including Crowdstrike, the company that investigated the committee's breach. Federal officials say their investigation has been underway since the spring, when the committee notified the F.B.I. of the intrusion. The **committee's suspicions were triggered by what appeared to be a relatively clumsy attack by the G.R.U. In the course of investigating that attack**, the F.B.I. discovered an earlier, more sophisticated attack on the committee by the F.S.B., which is often in competition with the G.R.U.

Preclearance at Foreign Airports Seen as a Necessity to Fight Terrorism (Canada)
New York Times, Ron Nixon, 2016 07 25
Brussels - The **Department of Homeland Security is pushing to increase the number of American law enforcement personnel stationed at airports abroad to screen passengers before they board planes to the United States**, officials say. The effort would be designed to extend the United States' border security to foreign airports as part of new initiatives to reduce the risk of potential terrorists entering the country. Under a smaller program already in place, called **Preclearance** and run by United **States Customs and Border Protection**, officers are based at foreign airports where they collect fingerprints and photos and check travel documents before allowing passengers to board a plane traveling to the United States. The proposed

expansions are mostly for airports in Europe, including the one here in Brussels, which was the site of terrorist attacks in March. The **agency has more than 500 people stationed at 15 foreign airports, including facilities in Canada, Bermuda, the Bahamas, Aruba, Abu Dhabi and Ireland. Ralph Goodale, Canada's minister of public safety,** said the preclearance program has been "tremendously beneficial for both of our countries." He added that it provides an effective way to move people quickly across the border between Canada and the United States, and enhances security between the two countries. Preclearance began in 1952 in Toronto, primarily as a way to streamline the customs process for passengers arriving at American airports from Canada.

FBI Suspects Russia Hacked DNC; U.S. Officials Say It Was to Elect Donald Trump
The Daily Beast, Shane Harris and Nancy A. Youssef, 2016 07 25
Washington—The **FBI suspects that Russian government hackers breached the networks of the Democratic National Committee and stole emails** that were posted to the anti-secrecy site WikiLeaks on Friday. It's an operation that several U.S. officials now suspect was a deliberate attempt to influence the presidential election in favor of Donald Trump, according to five individuals familiar with the investigation of the breach. The **theory that Moscow orchestrated the leaks to help Trump, who has repeatedly praised Russian President Vladimir Putin and practically called for the end of NATO**, is fast gaining currency within the Obama administration because of the timing of the leaks and Trump's own connections to the Russian government, the sources said on condition of anonymity because the investigation is ongoing and developing quickly. "The release of emails just as the Democratic National Convention is getting underway this week has the hallmarks of a Russian active measures campaign," David Shedd, a former director of the Defense Intelligence Agency, told The Daily Beast. Shedd said that additional leaks were likely, echoing an opinion expressed by U.S. officials and experts who said that the release of emails on Friday may just be an opening salvo. An **FBI spokesperson** said in a statement Monday that the bureau was investigating the breach but declined to comment on whether political motivation was part of the inquiry. The theft of information, which at the time reportedly consisted of opposition research and the DNC's files on Trump, seemed to be part of a longer campaign of spying by the Russians in order to glean insights into the next president. **Director of National Intelligence James Clapper also said in May that there were indications both presidential campaigns had been targeted by foreign hackers**.

Snowden Posts Document Alleging US Policy to Hack Foreign Political Parties
Sputnik (Russia), Staff report, 2016 07 25
Washington - The **US intelligence community allegedly authorized the hacking of foreign political parties**, according to a 2010 national security document posted by whistleblower and former National Security Agency contractor Edward Snowden on Monday. The document, originating from the **Director of National Intelligence** and dated July 16, 2010, purported to identify "foreign-based political organizations" allegedly targeted by US intelligence. "Our government specifically authorized the hacking of political parties. Mistakes were made," Snowden said in a Twitter message. Among them were Egypt's Muslim Brotherhood and National Salvation Front, the Pakistan Peoples Party, the Lebanese Amal group and the Indian Bharatiya Janata Party.

9/11 defense lawyers: Judge let U.S. secretly destroy CIA 'black site' evidence
Miami Herald, Carol Rosenberg, 2016 07 25
Guantanamo Bay - **Defense lawyers for the alleged 9/11 plotters said for the first time Sunday that the government destroyed a secret CIA prison with secret permission of the trial judge**, and they learned of it only after the fact. Defense attorneys have been complaining

about a mysterious destruction of evidence episode in a cloaked manner since May. Prosecutors have said they did nothing wrong but declined to explain with any specificity. After a closed session Friday, during which the judge apparently agreed some details were no longer classified, the defense lawyers laid out what they knew in a Sunday roundtable. It did not appear that the "torture chamber," as defense attorney Cheryl Bormann called it, was razed, lawyers said.

Clinton campaign -- and some cyber experts -- say Russia is behind email release
Washington Post, Tom Hamburger, Ellen Nakashima, 2016 07 25
Washington - A **top official with Hillary Clinton's campaign on Sunday accused the Russian government of orchestrating the release of damaging Democratic Party records to help the campaign of Republican Donald Trump** - and some cybersecurity experts agree. The extraordinary charge came as some national security officials have been growing increasingly concerned about possible efforts by Russia to meddle in the election, according to several individuals familiar with the situation. Although other experts remain skeptical of a Russian role, the hacking **incident has caused alarm within the Clinton campaign and also in the national security arena.** Officials from various intelligence and defense agencies, including the National Security Council, the Department of Defense, the FBI and the Department of Homeland Security, attended the White House meeting Thursday, on the eve of the email release. If the accusation is true, it would be the first time the Russians have actively tried to influence an election in this manner, analysts said.

Spy agencies struggle to spot threats from lone, mentally ill attackers
Reuters, Mark Hosenball, 2016 07 24
Washington - **Recent attacks on civilians in the U.S. and Europe have exposed a gap in the intelligence community's efforts to track suspected extremists and prevent mass killings**, a half dozen American, British and French counterterrorism officials told Reuters. The **attacks have a common theme of being carried out by actors with an apparent history of mental illness - but few if any direct links to extremist groups**, the officials told Reuters. From both a legal and a strategic perspective, counterterrorism investigators globally are focused on plots by established violent groups with known ideologies, such as Islamic State. In the U.S., laws designed to protect citizens from intrusive government spying can limit investigations of individuals unless they have provable ties to foreign terror groups. Counterterrorism officials told Reuters that the assailants in a recent spate of mass killings all had histories of apparent mental illness.

Israeli spy Jonathan Pollard seeks easing of parole conditions in US court
Deutsche Welle, Staff Writer, 2016 07 23
Berlin - **Jonathan Pollard** served 30 years in prison for stealing hundreds of secret and top-secret documents and selling them to Israel. He **was paroled in November but is still considered a security threat -** so he wears a tracking device. But as Pollard's attorney Eliot Lauer argued for an easing of some restrictions on Friday, US District Judge Katherine Forrest cautioned that her authority was limited. "The information [Pollard stole] is ridiculously stale, and it's the type of information that no human being could reasonably recall," Lauer told Forrest, referring to the 30-year-old documents. He said Pollard was being denied a job at an investment firm because of the computer monitoring.

A reality check on the Middle East from America's spy chief
Washington Post, David Ignatius, 2016 07 22
Column - **America's top spymaster offered contrarian assessments of some key issues: warning against "hyping" the threat posed by the Syrian al- Qaeda affiliate (terrorist**

group) Jabhat al-Nusra, cautioning against Obama administration plans to share intelligence with Russia on Syrian targets and questioning Turkish claims that last Friday's coup attempt was organized by a cleric living in the United States. National Intelligence Director **James Clapper** made the characteristically blunt comments in an interview Wednesday. He expanded on a warning he made in an interview in May that the United States can't by itself "fix" the problems of the turbulent Middle East. Clapper's skeptical view is shared by President Obama and has reinforced the administration's wariness about committing military force in Syria. Clapper began the wide-ranging discussion by questioning the recent "groundswell" of concern about Jabhat al-Nusra.

How the Real Edward Snowden Helped Write the Ending to Oliver Stone's 'Snowden'
The Daily Beast, Jen Yamato, 2016 07 22
Washington - The **NSA's worst nightmare made his San Diego Comic- Con debut by way of video chat, moments after the first public screening of Oliver Stone's Snowden**. "The FBI actually gets a copy of this talk because we're going through Google Hangouts, which unfortunately has a sort of built-in surveillance capability," joked **Edward Snowden**, his face peering down on a theater full of critics and journalists. He joined Stone and stars **Joseph Gordon-Levitt and Shailene W**oodley from Moscow, his home for the foreseeable future, "live--from the internet." Snowden tracks the NSA analyst as he wrestles with the decision to blow the lid off of the U.S. government's top-secret global surveillance program, an act that made him persona non grata in America and changed history.

Russian Agent Sentenced for Illegally Exporting US High-tech Gear
Voice of America, Staff report, 2016 07 22
New York - A **federal court in New York on Thursday sentenced an admitted agent of the Russian government to 10 years in prison and ordered him to forfeit $500,000 in profit he'd gained from his criminal activity**, which focused on acquiring and secretly shipping abroad high-tech microelectronics for Russian military equipment. **Alexander Fishenko** pleaded guilty to all 19 charges brought by the Department of Justice. U.S. officials said a company that Fishenkohad founded shipped $50 million worth of electronic products to Russia between 2002 and 2012, all in defiance of a government licensing system meant to control such exports. "These commodities have applications and are frequently used in a wide range of military systems," U.S. officials said, "including radar and surveillance systems, missile guidance systems and detonation triggersUltimate recipients of the electronic components acquired by Fishenko's companies, known as **ARC and Apex**, included a research unit for the Russian internal security agency **FSB**, a Russian entity that builds air and missile defense systems, and another that produces electronic warfare systems for the Russian Ministry of Defense.

CIA Chief Hedges When Asked if U.S. Saw Turkey Coup Coming
Wall Street Journal, Damian Paletta, 2016 07 20
McLean Va. - **Central Intelligence Agency Director John Brennan said intelligence officials were well aware of strains within Turkey and sizable opposition to President RecepTayyip Erdogan, but he wouldn't say whether they foresaw an attempted coup last week**. Mr. Brennan, speaking Tuesday evening to an audience at the Intelligence and National Security Alliance, described the setting U.S. officials were in Friday night when the attempted coup was unfolding. "The first thing you do when you have a situation like that is you try to ascertain the facts, and a lot of time...it's very very difficult because a lot of information is coming in and it is hard to distinguish between rumors," he said.

Lawmakers push TSA to strengthen Amtrak passenger security
The Hill, Melanie Zanona, 2016 07 20
Washington - A **pair of House lawmakers is backing a bill that would prod the Transportation Security Administration (TSA) into implementing all the requirements of a decade-old law aimed at addressing terror threats on Amtrak**. The legislation was crafted in response to a recent watchdog report that found the TSA has "limited regulatory oversight processes" to strengthen passenger security at Amtrak, because the agency has not complied with all of the recommendations mandated by Congress following the 9/11 terrorist attacks.

US intel bulletin warns of persistent threat from 'Western female violent extremists'
Fox News, Matthew Dean, 2016 07 20
Washington - The **U.S. intelligence community is warning law enforcement agencies around the country of persistent terror threats posed by radicalized Western women. In a Joint Intelligence Bulletin - or JIB -** distributed Tuesday and obtained by Fox News, the FBI, Department of Homeland Security, and National Counterterrorism Center note a "continued trend of Western female violent extremists... engaging or attempting to engage in plotting against targets in the West, including their home countries." The information was circulated after a review of recent arrests, as well as observations made following successful and disrupted plots. The **agencies find that extremist-sympathizing Western women "are likely to continue" to follow persistent calls by terror groups like ISIS and Al Qaeda to plot and/or carry out lone wolf-style terror attacks in their home countries or other Western nations**. Additionally, FBI, DHS and NCTC warn of the women's potential role in carrying digital surveillance of potential targets over the Internet through a practice known as "doxing." Doxing leverages publicly available information on the web to plot attacks against specific individuals or locations.

Spies among us: Get a peek at their playbook
CNN, Thomas Patterson, 2016 07 20
Washington— Spies are living among us. **In the United States alone, one expert estimates that there are about 100,000 foreign agents working for at least 60 to 80 nations -- all spying on America**. "That's not paranoia -- that's a good guess," said **Chris Simmons, a retired counterintelligence supervisor for the U.S. Defense Intelligence Agency, appearing on CNN's "Declassified."** It all sounds very much like the exciting Hollywood dramas set during the Cold War with Soviet spies pretending to be harmless citizens -- like **F/X's popular TV series "The Americans."** **Evgeny Buryakov**, 41, posed as an employee in the Manhattan office of a Russian bank. He entered the United States and stayed as a private citizen, the Justice Department said. Buryakov gathered "intelligence on the streets of New York City, trading coded messages with Russian spies who send the clandestinely collected information" to **Russia's foreign intelligence agency, the SVR**, Bharara said. According to court documents, Buryakov was "receiving taskings from Moscow." He reportedly was sentenced to 2.5 years in prison and ordered to pay a $10,000 fine.

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

MI6 casts aside its veil of secrecy to show schoolchildren that anyone can become a spy
London Daily Telegraph, Ben Farmer, 2016 07 26

London - **MI6 has welcomed its first school trip as it tries to broaden its recruiting pool for spies and dispel the perception that staff are only chosen via a "tap on the shoulder"** at Oxbridge. Seven pupils from some of the most deprived areas of Wales met the chief of the intelligence agency after winning a careers trip to London. The Secret Intelligence Service wants to attract a wider range of recruits as it fears potentially successful candidates may not think of a career with them. **Sources said an ever broader pool of spies and skills is needed to meet the range of security threats Britain now faces**. A senior intelligence official said: "The Service wants to encourage people from all walks of life, irrespective of their religious or ethnic background, to understand they can have a fulfilling career working for MI6. The world of modern espionage requires a wide range of skills, and we need to broaden our recruitment to every corner of society to ensure we get the best people available to make sure we can defend the nation from a wide range of threats." The schoolchildren who visited MI6 last week were not told of the visit to the service's headquarters on the banks of the Thames until an hour beforehand.

Judge appointed 'surveillance tsar' after police spy row
London Times, Neill Johnston, 2016 07 26
London - A **leading judge has been appointed as the country's new "surveillance tsar" after a controversial row over police spying. Lord Bracadale**, who presided over the trials of Nat Fraser and Tommy Sheridan, is now being urged to "vigorously protect" the interests of the public and journalists. The appointment comes after police were found to have spied on one of their own officers in an effort to uncover the source of media leaks, and was wel-comed by opposition parties after more than a year of delay in filling the role. Liam McArthur, a Liberal Democrat MSP, said: "The fact that a commissioner is now in place will mean nothing unless he vigorously protects the interests of journalists and others who have had their communications data intercepted unlawfully.

MI5 may be stirring Corbyn strife
Daily Telegraph, Ben Riley-Smith, 2016 07 23
London - **Len McCluskey the Unite leader, has claimed Britain's intelligence agencies may be responsible for the bullying and abuse directed towards critics of Jeremy Corbyn**. The union boss, a loyal supporter of the Labour leader, said the security services had a history of "dark practices" and suggested "Right-wingers" in disguise may be responsible for the actions attributed to the Labour leader's supporters.

Boris Johnson once outed MI6 spy 'for a laugh'
Politics.co.uk, Adam Bienkov, 2016 07 20
London - There was some nervousness in the Foreign Office when it was announced that **Boris Johnson had been made foreign secretary.** Part of Johnson's new role involves overseeing **MI6**. This is a highly sensitive and delicate task which some within his department worry he is unsuited for. It now appears there is good reason for them to feel uneasy.In 2001, while editor of the Spectator, Johnson published a piece suggesting that a former **friend and colleague had worked for the secret service. On the front page of the magazine, Johnson splashed the headline "Who was Smallbrow?" Inside, Boris published an article naming Agent Smallbrow as then Sunday Telegraph editor Dominic Lawson.** The allegation was based on a controversial book by renegade spy Richard Tomlinson which had been published in Russia. Tomlinson claimed that Lawson had provided cover for **MI6 agents working in Eastern Europe**.

MI5 monitored protesters at RAF bases in the 1980s
The Independent (UK), Gavin Gordon, 2016 07 21

London - **Peace protesters demonstrating against the deployment of US nuclear missiles at British air bases in the 1980s were kept under close watch by MI5**, newly released government papers suggest. Files released by the **National Archives** in Kew, west London, indicate that peace camps set up around the bases involved were monitored by the security service for evidence of infiltration by "subversive organisations".

GCHQ and Leamington charity aim to inspire girls to take up a career in cyber security
The Courier (Leamington Spa), Staff report, 2016 07 20
Leamington Spa - **National security experts at GCHQ are working with a Leamington charity to offer a free cyber security course for teenage girls this summer**. The Smallpeice Trust is running the CyberFirst Futures residential course with GCHQ at Birmingham University from August 1 to 4, during which participants will gain an insight into the next generation of cyber security tools. **The course will also test their skills in dealing with modern and advanced cyber defence scenarios. Open to 16 and 17-year-old girls, those taking part in the four-day course will work closely with experts from GCHQ, the Smallpeice Trust and academia, gaining an insight into the importance of cyber security and getting first-hand experience of defending against a cyber-attack. Chris Ensor from GCHQ** said: "We want to develop a diverse, continuous flow of people with the right skills and knowledge to help protect the UK against future cyber-attacks.

Return to Table of Contents/ Retour à la table des matières

Australia/ Australie

PM's tough new plan to keep terrorists behind bars
The Australian, Brendan Nicholson, 2016 07 26
Sydney - **Malcolm Turnbull wants new counter-terrorism measures in place urgently to discourage radicals in Australian jails from continuing their calls for jihad.** The Prime Minister announced yesterday the government would legislate for the continued detention of convicted terrorists who had served their sentences and who still posed a ¬serious threat to society, and for courts to impose control orders on children as young as 14. The Australian has been told Mr Turnbull was concerned about terrorists actively trying to spread their message in jails and encouraging violence outside them.

Government moves towards indefinite detention for some terrorists in push for new anti-terror laws
ABC (Australia), Louise Yaxley, 2016 07 25
Canberra - **Australia is taking a step towards indefinite detention for some convicted terrorists, with the Federal Government pushing for legislation in every state so terrorists could be kept in jail after their sentences expire if a court says they would reoffend**. Prime Minister Malcolm Turnbull has written to state and territory leaders asking them to quickly agree on laws that could keep terrorists in jail if the threat is assessed as serious. Federal Attorney-General George Brandis said he wanted laws similar to those in some states which keep sex offenders in jail after they have served their sentence if they still posed a serious risk to the community. He argued it would only apply to very high risk offenders who show no signs of rehabilitation when they are near the end of their sentence. **'Measure will only apply to most serious category of offender 'State leaders were briefed by ASIO's Director General last**

December at Mr Turnbull's first council of Australian Governments meeting and agreed to the idea, then endorsed the next step in April.

PM rushes to pass strict terror laws
The Advertiser, Jackson Gothe-Snape & Rob Harris, 2016 07 25
Canberra - **New laws to keep convicted terrorists behind bars - potentially for life - if they remain a danger to the community, must be fast-tracked, amid an increase in global terror threats**, Prime Minister **Malcolm Turnbull** says. He spoke to state Attorneys-General yesterday to invite them to gather within weeks because he wants to enact a national regimen by the end of the year. In a follow-up letter sent overnight, Mr Turnbull said the laws would cover only "high-risk terrorist offenders" and would "contain appropriate procedural protections and safeguards". "This is a significant public safety and security issue and governments must do all we can to protect the community from individuals posing a high risk of reoffending," he said.

Agencies to focus on 'lone wolves'
The Australian, Brendan Nicholson, 2016 07 22
Canberra - **Malcolm Turnbull has ordered Australia's counter- terrorism agencies to urgently develop a strategy to prevent rapidly radicalised terrorists carrying out Nice-style attacks in public areas.** The government has been advised that the threat of an attack by "lone-wolf" terrorists using a truck or knife and potentially causing scores of casualties could last for decades. Senior sources have told The Australian the **Prime Minister is particularly concerned that while it would be hard for a terrorist to obtain a cache of automatic weapons here, an attack using a vehicle as a weapon could cause devastating casualties**. Mr Turnbull has called in **counter-terrorism co-ordinator Greg Moriarty** and directed him to quickly identify lessons for Australia arising from the Bastille Day attack in Nice.

Security services doing good job: Stratfor
Australian Associated Press, Max Blekin, 2016 07 22
Canberra - **The lack of large-scale terror attacks in the US and Australia show security services are doing a good job, a US private sector intelligence group says**. Terrorist group Islamic State's call to adherents to conduct "lone wolf" attacks was a response to police pressure and an admission of weakness. In an analysis of "lone wolf" terrorism, **Stratfor security analyst Scott Stewart** says organised terror groups are more effective at mounting large attacks as they contained skilled operatives. But they were also more likely to attract attention of counter-terrorism services. "Judging from the lack of such attacks, at least in North America and Australia, they are doing a good job," Mr Stewart said. Based on sheer numbers, both are more likely to encounter grassroots terrorists than officers of the **Australian Security Intelligence Organisation**. The Australian government has recognised this with the "be alert not alarmed" and similar campaigns and the national security hotline.

Return to Table of Contents/ Retour à la table des matières

New Zealand/Nouvelle-Zélande

Waihopai documentary digs into the world of spies, eyes and peace video
Stuff News New Zealand, Philip Matthews, 2016 07 23
Wellington - They walked through a vineyard and cut fences in the dead of night, approached the enormous white domes of the **spy base** and said, "In the name of Jesus Christ, we disarm you". Then they plunged sickles into a dome, which deflated like a balloon, and they cried next

to a shrine they set up. The three men were a teacher, a farmer and a Catholic priest. The teacher, **Adrian Leason**, said, "Catholic spirituality was the glue that brought us together." Leason, Father Peter Murnane and farmer Samuel Land were charged for the **2008 attack on the Waihopai spy base near Blenheim** that New Zealand's prime minister at the time, Helen Clark, called "a senseless act of criminal vandalism". But was it senseless? **Leason is the central figure in a new documentary that spreads outwards from that incident at Waihopai to encompass the vast subject of global surveillance and New Zealand's role in the Five Eyes alliance**. Viewers of The **5th** Eye may experience unsettling flashbacks from 2014 as these figures appear before you: **Edward Snowden, Kim Dotcom, Nicky Hager and Glenn Greenwald.**

Return to Table of Contents/ Retour à la table des matières

International

China/Chine

China says sensitive issues could damage ties with US military
Agence France-Presse, Staff reporter, 2016 07 25
Beijing - **Failure to properly handle sensitive issues between the US and China could "very likely disturb and undermine" their military-to- military relations, a top Chinese official told US National Security Advisor Susan Rice** Monday. Rice is the highest-level US official to visit the capital since an international tribunal this month rejected China's vast territorial claims in the South China Sea -- infuriating Beijing and fuelling tensions with Washington. Her trip is intended to prepare for a visit by President Barack Obama to a G20 summit in the city of Hangzhou in September. The Permanent Court of Arbitration in The Hague on July 12 denied the legal basis for Beijing's claim to nearly all of the sea, parts of which are also claimed by neighbouring nations.

Xinhua, China's news agency and 'propaganda tool' (Canada).
The Hindustan Times, Rezaul H Laskar, 2016 07 25
New Delhi - **China's state-run Xinhua news agency is no stranger to controversy, having been accused by governments and journalistic bodies of spreading disinformation at the behest of the ruling Communist party**, biased coverage and even espionage. India last week expelled three Xinhua journalists by refusing to renew their visas to work in the country after they came under the "**adverse attention of security agencies**" for allegedly indulging in activities beyond their journalistic brief. In August 2012, **Canadian journalist Mark Bourrie quit working for Xinhua after accusing it of directing him to spy on the Dalai Lama in Ottawa**. Bourrie alleged his Chinese bureau chief wanted him to use his parliamentary press accreditation to cover the Tibetan spiritual leader's news conference, gather information on the Dalai Lama's meeting with the Canadian prime minister and turn over all notes and materials without writing any reports.

Police hold anti-terrorism drills for 2017 Universiade
The China Post, 2016 07 22
Taipei— The **central government held anti-terrorism exercises in preparation for the 2017 Universiade games Thursday in Taipei**. The exercises were organized by the **Interior**

Ministry's National Police Agency (NPA) and included descent from high-rises, weapons training and non-weapon techniques to display the ability of law enforcement agencies to prevent a potential terrorist attack. According to NPA Director General Chen Kuo-en, the maneuvers were tasked to a special commando unit under the NPA to prepare for possible terrorist incidents.The Universiade is an important event and it is necessary for the police to train its anti-terrorism forces. The government is confident that security preparations against terrorism can be adequately provided, Chen added.

Return to Table of Contents/ Retour à la table des matières

Russia/Russie

Russian FM Lavrov refuses to use 4-letter words in comments about Russian hackers
Pravda, Staff report, 2016 07 26
Moscow - **Russian Foreign Minister Sergei Lavrov said he could not exclude expletives from his comments about the Russian trace in the hacking of the US Democratic Party mail server**. It was reported that Russian hackers could be involved in the recent cyber attack on the USA. Last week, WikiLeaks published documents indicating that the party leadership was favoring Hillary Clinton in the fight for the right to become a candidate for US presidency to the detriment of Bernie Sanders. "I would not like to use four-letter words," Lavrov said when asked to comment on the Russian track in the data leak.

In Hacking, Russia Is Accused of Playing in American Politics
New York Times, David E. Sanger, Nicole Perlroth, 2016 07 25
Washington - An unusual question is capturing the attention of cyberspecialists, Russia experts and Democratic Party leaders in Philadelphia: **Is Vladimir V. Putin trying to meddle in the American presidential election?** Until Friday, that charge, with its eerie suggestion of a Kremlin conspiracy to aid Donald J. Trump, has been only whispered. But the release on Friday of **some 20,000 stolen emails from the Democratic National Committee's computer servers**, many of them embarrassing to Democratic leaders, has intensified discussion of the role of **Russian intelligence agencies** in disrupting the 2016 campaign. The emails, released first by a supposed hacker and later by WikiLeaks, exposed the degree to which the Democratic apparatus favored **Hillary Clinton** over her primary rival, **Senator Bernie Sanders** of Vermont, and triggered the resignation of **Debbie Wasserman Schultz**, the party chairwoman, on the eve of the convention's first day. Proving the source of a cyberattack is notoriously difficult. But researchers have concluded that the national committee was breached by two Russian intelligence agencies, which were the same attackers behind previous Russian cyberoperations at the White House, the State Department and the Joint Chiefs of Staff last year.

Russian intelligence saved Erdogan from coup - media reports
Russian Press Digest - Russicalzvestia, Dmitry Kalinin, 2016 07 22
Moscow - **Reports that Russian intelligence warned the Turkish president about the military coup, allowing him to escape and retain power, appeared in various Russian media outlets in the evening of July 20.** However, it is **unclear to what extent the reports are true:** Erdogan himself said that he learned about the coup from his brother-in-law. Russian media have reported that Turkish **President RecepTayyip Erdogan was warned by Russian intelligence services** about the military coup against him that was thwarted in the early hours of July 16. The Russian media outlets that have spread the version of Moscow's involvement in Erdogan's victory over the plotters cite the major Iranian news agency Fars, which, in turn,

refers to reports by several Arab media outlets (in particular, the Sudanese newspapers Al Sudan Al Youm).

High-flying Russian spies banished to Siberia as punishment for 'indecent' graduation stunt where they paraded through Moscow which revealed their identities
Daily Mail (UK), Multiple reporters, 2016 07 21
London - **Dozens of high-flying trainee Russian spies have been banished to the Siberian wilderness after taking part in 'indecent' graduation that compromised their identities**. The agents staged a brash cavalcade of black Mercedes Gelandewagens through Moscow streets in a mafia- style show of strength to mark their graduation from the **FSB Academy**. They were given the choice of quitting the country's elite security service or being stationed in Chukotka or Kamchatka, and almost all of them picked the second option. Both locations are more than eight hours flying time from Moscow. A **spy source said: 'It was important for the FSB leadership to teach their graduates a lesson for such a provocative behaviour.'**

Moscow security chiefs held over links to mobster
London Times, Tom Parfitt, 2016 07 20
London - **Russia's Federal Security Service has detained officials at the powerful Investigative Committee for alleged links to the mafia godfather Shakro the Young**. The security service said that it had arrested **Major General Denis Nikandrov**, deputy head the Moscow directorate, along with Mikhail Maksimenko, head of the committee's internal security division, and MrMaksimenko's deputy, Alexander Lamonov. Service sources said that General Nikandrov was suspected of promising to free Shakro, whose real name is ZakharyKalashov, for $1 million. Officers were searching the suspects' homes and places of work. A lawyer for MrLamonov said that the detained had men denied doing anything wrong.

One Russian Security Agency Raids Another, in Rare Sign of Dysfunction
New York Times, Andrew E. Kramer, 2016 07 20
Moscow - **Russia's main domestic intelligence service raided the Moscow headquarters of an investigative agency on Tuesday, in a rare sign of dysfunction in the country's domestic security services**. The raid, recalling the rivalries and infighting of the immediate post-Soviet period, played out on a main street in the capital, New Arbat, and ended with arrests of three senior prosecutors. Agents of the **Federal Security Service**, or F.S.B., the main successor to the Soviet K.G.B., searched the offices of the **Investigative Committee**, the powerful branch of the prosecutor's office that deals with politically hued crimes. The raid was all the more baffling because the two agencies are generally viewed as operating in lock step to repress political dissent, crack down on organized crime and pursue other high-profile cases in the capital.

SBU refute Russian security service claims that OSCE SMM translator was their agent
Kyiv Post, Staff report, 2016 07 19
Kyiv - **YuriyTandit, advisor to the chief of the Ukrainian Security Service (SBU), has refuted the statement recently made by the Russian security agencies that a translator employed with the OSCE Special Monitoring Service (SMM) was an SBU informant**. "We do not recruit OSCE employees. Authoritative international organizations confirm our position. We cooperate with the OSCE. It is important for us to implement the Minsk agreements. And the OSCE is here to help us with it," Tandit said in his comment for the online version of Ukrainska Pravda. The **Russian Federal Security Service (FSB)** alleged on July 18 that an SBU agent employed with the SMM as a translator had acted under instructions given by Ukraine's state security agencies to collect intelligence in Donbas.

Return to Table of Contents/ Retour à la table des matières

Europe

DGSE : l'hommage discret aux trois soldats français tués en Libye
Midi Libre, F.B., 2016 07 26
Perpignan - Deux avions pour des autorités militaires très protégées. Une cérémonie très discrète s'est tenue lundi après-midi au coeur de la Citadelle de Perpignan, qui **abrite le Centre d'instruction parachutiste spécialisé (CPIS), le régiment qui est le bras armé de la DGSE**. **Trois militaires français de la Direction générale de la sécurité extérieure sont morts la semaine dernière**, au cours d'une mission de renseignement en Libye. Leur hélicoptère a été vraisemblablement abattu par un missile sol- air tiré par un groupe jihadiste, dans la région de Benghazi.

2 Turkish generals in Afghanistan detained by authorities in Dubai
Daily Sabah, 2016 07 26
Ankara--**Two Turkish generals based in Afghanistan were detained** on Tuesday by authorities in Dubai following the **failed coup attempt** by the Gülenist Terror Organization (FETÖ). The Commander of Afghanistan Turkish Task Force and Hamid Karzai International Airport **Cahit Bakır** and Brigadier General Şener Topuç were detained at Dubai Airport following joint cooperation efforts by the Ministry of Foreign Affairs and the **National Intelligence Organization (MİT)**, diplomatic sources said. They were brought to Turkey early Tuesday. **Bakır previously served as the Head of Intelligence Division of Turkish Air Force Command.**

Bulgarians Practically Equate Politics with Corruption – Poll
Bulgarian News Agency, 2016 07 26
Sofia— **Bulgarians practically equate politics with corruption**. Corruption and political influence in the operation of courts are precisely what is perceived as the main problems in the judicial system, an express survey of Gallup International Balkan agency shows. The poll was conducted through direct telephone interviews of 1,605 people across Bulgaria on July 14-19. The survey is part of the agency's own research programme focused on crime, a topical subject for the judicial system.Bulgarians approve more the institutions that seem depoliticized, instrumental and even repressive. And vice versa, those associated with political power or the judicial system are criticized almost automatically, Gallup says. **Approval of** the National Revenue Agency (60 per cent approval against 32 per cent disapproval), the **State Agency for National Security (51 per cent against 35 per cent),** the Interior Ministry (54 per cent against 42 per cent) is tangibly higher than that for the judiciary, the Justice Ministry or Parliament.

Spain to invest 60m euros to modernize intelligence centre
La Vanguardia (via BBC Monitoring Europe), 2016 07 26
Madrid— A decision in favour of **cyber security and the fight against Jihadist terrorism**. This is how acting **Deputy Prime Minister Soraya Saenz de Santamaria** explained the approval this morning, 22 July, by the cabinet, of an agreement whereby "a commitment to spend" 60 million euros "is undertaken," during future fiscal years, beyond 2016, to **modernize the National Intelligence Centre (CNI).** This "spending commitment" modifies the ceilings laid down by the General Budgetary Act, with the goal of making it possible for the intelligence services to enter into contracts for technological renewal and infrastructure investment.

Ukraine's chief prosecutor to arrest some security service employees for torture
ITAR-TASS World Service, Staff report, 2016 07 26
Moscow - A **group of Ukraine's Security Service brass may be arrested soon for complicity to torture,** Ukraine's Chief Prosecutor Yuri Lutsenko said. "Judging from last week reports, a group of **Ukraine's Security Service employees** is going to be arrested soon because of complicity to torture," Ukraine's Public TV quoted Lutsenko as saying. According to the chief prosecutor, high-ranking security service employees shot at people and inflicted heavy bodily harm in the process of extortion.

Number of Norwegians joining Isis in decline
The Local (Norway), Staff report, 2016 07 25
Oslo - According to Ritzau, **reports from the Danish, Norwegian and Swedish intelligence services indicate that there are fewer Scandinavian citizens travelling to the Middle East to fight for the militant group Isis,** also known as Daesh or Islamic State. Recruitment across the three countries appears to have peaked in 2013 and 2014 when ISIS was aggressively expanding throughout Iraq and Syria. Around 90 Norwegians have gone abroad to join up with Isis and the Norwegian intelligence service **PST** believes that at the end of 2015 there were still roughly 40 Norwegian foreign fighters actively participating in hostilities in Syria and Iraq. Magnus Ranstorp, Research Director Center for Asymmetric Threat Studies (CATS)at the **Swedish National Defence College**, believes that this partially has to do with the fact that Isis has already attracted many of the disaffected citizens in these countries who were receptive to the organisation's extremist ideology.

Turkey's interior minister says plotters' 'brain team' among police intelligence
Hurriyet Daily News, Staff report, 2016 07 25
Istanbul - **Interior Minister Efkan Ala has said there had not been any information from police intelligence ahead of the July 15 coup** attempt and the coup plotters had a "brain team" developed inside the body. "There was no information coming from the police intelligence. There has been a brain team developed among them. Information should have been received from soldiers. Police should have received information as well. **The fact that the MIT [National Intelligence Agency] received information some four to five hours ahead foiled the game for them. We have changed the head of gendarmerie intelligence but could not change within it.** There was no intelligence received from there," said Ala, as he gave an interview to a group of journalists in the aftermath of the July 15 failed coup attempt. Ala added that in five to 10 years another coup attempt could be initiated if the problem, which stemmed "more from system weaknesses, rather than intelligence weaknesses," could not be changed.

Intelligence collection, monitoring of people with mental-health issues seen as keys to improving safety
Wall Street Journal, Julian E. Barnes & Matthew Dalton, 2016 07 23
Berlin - First the massacre by truck in Nice, France, then an ax attack on a German train and now a shooting spree in Munich: Over the past 10 days, Western Europe has seen the calm of everyday life shattered by high-profile acts of violence. **Security officials said the recent string of attacks in both Europe and America show the importance of improving intelligence collection, and improving services and monitoring of people with mental-health issues**. "We are living in fear whether it is from terrorists or [mentally ill] people," said a U.S. official in Europe. "Whether they are self-radicalized or mentally ill they can terrorize and change peoples lives. We have two problems here, we have to focus on both." U.S. officials say the one thing European intelligence and law-enforcement officials could do quickly is find a mechanism with which to **share more intelligence and law enforcement information**, and

share it more widely. American officials have been pushing Europe for more intelligence sharing with the U.S.--not simply providing information on terrorists or potential terrorists who are intent on attacking the U.S. but a far broader swath of information.

Erdogan's 'secret keeper' under fire over Turkey coup lapse
Agence France-Presse, 2016 07 23
Ankara— **Turkey's shadowy spy chief Hakan Fidan has faced an unprecedented public dressing down in the wake of the failed coup but appears set to stay on in his post -- at least for now**. There has been intense speculation over **the future of Fidan, head of the National Intelligence Organisation (MIT) and widely seen as one of Turkey's most powerful men, after President Recep Tayyip Erdogan said intelligence lapses had helped last week's coup.** Erdogan late on Friday held a two-hour meeting with Fidan at the presidential palace but there was no statement afterwards that Turkey's top spy was to go. Indeed, the most significant development -- much to the amusement of social media users -- was that the usually clean-shaven spy chief had grown a moustache in what some saw as an expression of loyalty to the similarly mustachioed president. "No, he did not offer his resignation. We did not discuss this," Erdogan said in an interview with France 24 television. Following reports that MIT caught wind of the coup hours beforehand but did not warn Erdogan, the president admitted there had been an **intelligence failure**. According to the Hurriyet daily, Erdogan had furiously scolded Fidan following the coup, saying: "You got a really bad mark." To which Fidan replied: "Whatever you command, I am ready to do." Erdogan had previously complained of finding out about the coup not from the intelligence service but his brother-in-law -- and then, extraordinarily, of being unable to reach Fidan.

Turkey spy chief survives despite Erdogan criticism... for now
Agence France-Presse, Staff Writer, 2016 07 23
Istanbul - **Turkey's powerful spy chief HakanFidan is to stay on in his job after presiding over an intelligence failure that allowed the botched coup, but his position is under review**, President **RecepTayyip Erdogan** said in an interview broadcast Saturday. There has been intense speculation over the future of Fidan, head of **the National Intelligence Organisation (MIT)** and widely seen as one of the most powerful men in the country, after Erdogan publicly rebuked him for failing to see the putsch coming. Erdogan late on Friday held a two-hour meeting with Fidan at the presidential palace but there was no statement afterwards that Turkey's top spy was to go. "No, he did not offer his resignation. We did not discuss this," Erdogan said in an interview with France 24 television. Following reports that MIT had intelligence of the coup hours beforehand but did not warn Erdogan, the president admitted there had been an intelligence failure.

Ukraine's Security Services and Rebels Are Said to Be Equals in Torture
New York Times, Andrew E. Kramer, 2016 07 22
Moscow - A report by two leading human rights groups released on Thursday **accuses Ukraine's Western-backed security services of practicing abuse and torture in a manner similar to that of the rebel groups they are fighting**. In the report about disappearances and torture in the Ukraine war, titled "You Don't Exist," **Human Rights Watch and Amnesty International** document harrowing abuse by both sides, including waterboarding and the use of electrical shocks. "People in eastern Ukraine who are being seized and hidden away by the warring sides are at the mercy of their captors," Tanya Lokshina, a researcher with Human Rights Watch and one of the authors of the report, said in a statement. "It is never legal or justified to seize people off the streets, cut them off from contact with family and lawyers, and beat and abuse them," she said. **Ukraine's domestic intelligence agency, the Security Service of Ukraine,** denies illegally detaining suspects in the conflict. And yet as recently as

May, it refused to allow a United Nations delegation investigating reports of torture access to sites where suspects were alleged to be held illegally.

Trois militaires de la DGSE morts en Libye
Le Monde, Frédéric Bobin, Cyril Bensimon, et Madjid Zerrouky, 2016 07 22
Tripoli - La **présence militaire française** aux côtés du général Haftar irrite le gouvernement d'union nationale libyen Cinq ans après avoir participé à la chute de Mouammar Kadhafi, la France agit bien militairement en Libye. **Le ministère de la défense a annoncé, mercredi 20 juillet, que trois militaires français y avaient perdu la vie en " service commandé ".** Le gouvernement libyen d'union nationale (GNA) a accusé Paris de " violation " de son territoire, mercredi au soir. Rien ne " justifie une intervention " sans que Tripoli en soit informé, a déclaré le GNA. **Les trois sous- officiers, membres du service action de la Direction générale de la sécurité extérieure (DGSE) selon une source française haut placée**, sont morts dans un " accident d'hélicoptère " en Libye, a précisé, mercredi matin, François Hollande. La France mène " des opérations périlleuses de renseignement (...) . La Libye connaît également une instabilité dangereuse.

Turkish Intelligence Spied on People Involved in Coup Attempt
Sputnik (Russia), Staff report, 2016 07 21
Ankara - **Turkish intelligence service had spied on those arrested and dismissed after the failed coup attempt before it happened**, YasinAktay, deputy chair of Turkey's ruling Justice and Development Party (AKP), told Sputnik on Thursday. "There were lists [of participants before the coup]. The country's intelligence spied on all of them... Of course it knows who is who but everything is in line with the law. We never struggle with people only because they are adherents of a certain organization or have certain political views," Aktay said.

Des militaires français sont morts sur le sol libyen
Le Figaro, Tanguy Berthemet, 2016 07 21
Paris - **L'Élysée a annoncé le décès de trois soldats dans ce pays où des membres des forces spéciales sont engagés contre Daech**. Afrique du Nord Trois sous-officiers français sont morts en Libye lors de la chute d'un hélicoptère, a expliqué mercredi François Hollande. Cette annonce est la confirmation de la présence de militaires français dans ce pays, jusqu'alors jamais officiellement reconnue, même si ce secret était depuis plusieurs mois un secret de polichinelle. « La Libye connaît une instabilité dangereuse. C'est à quelques centaines de kilomètres seulement des côtes européennes. Le **nombre exact de soldats français présents en Libye, membres du service action de la DGSE ou des forces spéciales, est inconnu,** mais ils ne seraient que peu nombreux. La décision d'envoyer des forces sur le terrain aurait été prise fin 2015, alors que l'État islamique gagnait du terrain en Libye.

Turkey to restructure its army after coup attempt: Erdogan
Xinhua News Agency, 2016 07 21
Ankara—Turkish military will be restructured in a short time following a **failed coup attempt**, **President Recep Tayyip Erdogan** said on Thursday. "The army will get fresh blood," Erdogan said in a televised interview in Ankara. The **president underlined significant deficiencies and failure in their intelligence gathering** about the July 15 coup attempt. "No need to hide or deny. I told it to the **undersecretary of national intelligence organization (Hakan Fidan),"** he said. President Erdogan said he was not able to reach the chief of intelligence agency and the general staff at the night of July 15. "I hardly had contact with the prime minister," he said.

Libye : les militaires français tués viendraient du centre de la DGSE de Perpignan
Midi Libre avec l'Agence France-Presse, Romain Duriez, 2016 07 21
Perpignan, France - **Les trois militaires français tués en Lybie seraient du Centre parachutiste d'instruction spécialisée de Perpignan, un centre d'entraînement dédié aux opérations commando et à la guerilla.** Ce mercredi 20 juillet au matin, Paris a annoncé que trois soldats français étaient morts en Libye. **Des espions qui agissent clandestinement** Le ministre de la Défense, Jean-Yves Le Drian, a déploré dans un communiqué la "perte de trois sous-officiers français décédés en service commandé en Libye" sans préciser leur identité ou leur grade. "Ce qui laisse penser qu'il s'agit de trois agents de la **DGSE**" indique RTL précisant qu'ils appartiennent au Centre parachutiste d'instruction spécialisée de Perpignan, anciennement connu sous le nom de 11e régiment parachutiste de choc.

Ukraine, Canada will sign agreement on cooperation in security soon - ambassador
Kyiv Post, Staff report, 2016 07 20
Kyiv - **Ukraine and Canada will soon sign an agreement on cooperation in the field of security, Ukrainian Ambassador to Canada Andriy Shevchenko** has stated. "We hope in the next few months we will sign a security cooperation agreement. This is an agreement on cooperation between the defense ministries of Ukraine and Canada. Work on the text has been actually completed, we are at the finish line, the text is ready to be signed," he said in an exclusive interview with Interfax-Ukraine. According to the ambassador, this is a framework document to be filled with concrete areas of cooperation.

Turkish intel informed top generals hours before coup attempt, says army
Hurriyet Daily News, Staff report, 2016 07 20
Ankara - **Turkey's National Intelligence Organization (MIT) informed the country's top generals hours before the coup attempt was initiated by a group of soldiers within the army on July 15**, while Chief of General Staff Gen. HulusiAkar evaluated the information and issued all necessary warnings and orders against "this despicable and miserable attempt," according to a statement published on the General Staff's official website on July 19.

Turkey intelligence agency suspends 180 personnel
YeniSafak (Turkey), 2016 07 20
Ankara--The **National Intelligence Organization of Turkey (MIT) has suspended 180 personnel following the foiled coup of July 15, which was aiming at toppling the democratically elected government.** MIT personnel were discovered to have been inactive before the discharge. Before MIT, Turkey's Prime Ministry suspended almost 260 personnel , including 257 individuals of 230 clerks, six advisers and two legal advisers. Turkish prime ministry suspends 257 personnel Turkey's Prime Ministry suspended almost 260 personnel on Tuesday amid a nationwide move against those suspected of having links to Friday's military coup attempt which killed hundreds of people. **At least 208 people, including members of the security forces and civilians, were martyred in Istanbul and Ankara** and nearly 1,500 others wounded as they protested against the coup.

Bernard Cazeneuve : « L'état d'urgence ne peut pas être un état permanent »
Le Monde, Journaliste maison, 2016 07 20
Nice - Au lendemain de l'attentat de Nice, le **ministre de l'intérieur se dit « préoccupé de l'exacerbation de certaines tensions dans la société française ».** Mis en cause par la droite et l'extrême droite pour sa gestion de la menace terroriste, Bernard Cazeneuve, le ministre de l'intérieur, répond dans une interview au Monde, et s'en prend à ceux qui, en proposant des « lois d'exception », veulent « s'affranchir de l'Etat de droit ». La droite a immédiatement mis en cause le gouvernement après l'attentat de Nice, survenu le 14 juillet. **Y a-t-il eu une faille dans**

la sécurité ou au niveau des services de renseignement ? A Nice, la polémique a commencé dans les minutes qui ont suivi la commission de l'abject attentat. Des élus ont proféré des accusations et mis en cause les services de l'Etat. Que s'est-il passé ? Un individu, qui n'était pas connu des services de renseignement, qui n'avait jamais été condamné pour des faits en lien avec le terrorisme, est passé à l'acte de manière extrêmement violente.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Iran's Top Security Official Vows Tough Reaction to States Sponsoring Terrorist Acts at Borders
Fars News Agency, 2016 07 26
Tehran - **Secretary of Iran's Supreme National Security Council (SNSC) Ali Shamkhani warned that Tehran will not allow certain countries to support and supply terrorists with arms to foment insecurity at borders** and inside Iran. Shamkhani made the remarks in a meeting with National Security Advisor of Pakistan Nasser Khan Janjua in Tehran on Monday, alluding to Saudi Arabia which has blatantly showed its support for terrorist activities against Iran and other regional countries.

Top National Security Council appointee withdraws candidacy
The Jerusalem Post, Herb Keinon, 2016 07 21
Jerusalem— Avriel Bar-Yosef, **tabbed in February by Prime Minister Benjamin Netanyahu to serve as head of the National Security Council, withdrew his candidacy** Thursday, saying he has decided to work instead in the private sector. Bar-Yosef's appointment was held up for months amid various conflict of interest allegations.He **was to replace Yossi Cohen, who left the job in December to become head of the Mossad**. Since that time, Yaakov Nagel has been serving as acting head of the council. The NSC head is effectively the prime minister's top foreign policy adviser.

Return to Table of Contents/ Retour à la table des matières

Asia/Asie

North orders terror strikes on South Koreans
Korea JoongAng Daily, 2016 07 27
Seoul— **North Korean leader Kim Jong-un ordered terror attacks against South Koreans living overseas, a high-ranking official in Seoul said Tuesday, adding that his intelligence organizations are dispatching agents to China and Southeast Asian** countries. Kim was said to have ordered the terrorist attacks in retaliation for the defection en masse of a group of North Korean restaurant workers to the South earlier this year. He ordered agents who specialize in such acts of terror to Shenyang and Dandong in China's northeastern Liaoning Province, as well as Southeast Asian countries that have maintained diplomatic relations with Pyongyang, such as Laos and Cambodia, which are also key routes for North Koreans to defect through, according to this official. According to a source knowledgeable on Pyongyang affairs,

the **North Korean agencies that were mobilized for potential terrorist attacks on South Koreans include its General Bureau of Reconnaissance's department of overseas intelligence, the State Security Department and the cultural exchange department of the Unification Front Department**.

Pyongyang Radio Revives Coded Broadcasts for Spies
The New York Times, Choe Sang-Hun, 2016 07 22
Seoul— In **an era of sophisticated spycraft, North Korea appears to be returning to the days of shortwave radio**. The North broadcast a series of seemingly random numbers on Pyongyang Radio twice recently, an eerie reminder of the days when the North encrypted messages to its spies in South Korea. In the latest episode last Friday, an announcer read what she described as "a mathematics review assignment for investigative agent No. 27," engaged in a "distance learning" program. "Turn to Page 459, No. 35; Page 913, No. 55; Page 135, No. 86," she said, continuing to cite numbers for 14 minutes. **Kim Dong-sik, a former intelligence officer for North Korea**, said he used to listen for such broadcasts at midnight each night to check whether his spymasters had a message for him. Mr. Kim was caught by the South in 1995 after a gun battle with South Korean agents and police officers. "When I arrived in the South, I had five different call signs assigned to me," said Mr. Kim, who now **works as a senior analyst at the Institute for National Security Strategy, a think tank run by South Korea's National Intelligence Service**. "Each night, I listened for my call signs.'

NIA seeks assistance of six countries in ISIS case probe (Canada).
Press Trust of India, 2016 07 21
New Delhi - **The National Investigation Agency (NIA) has sought assistance from six countries, including the US, UAE and Canada, in its ongoing investigation against various suspected ISIS operatives and their terror activities in the country**. The probe agency disclosed this in its charge sheet filed before District Judge Amar Nath against 16 suspected ISIS operatives, arrested from across the country allegedly on the charges of recruiting and financing people to join the terror group. The agency claimed that these accused were trying to "advance the cause of ISIS and establish Caliphate in India".

Suhardi to boost counterterrorism efforts
The Jakarta Post, 2016 07 21
Jakarta—The **inauguration of Comr. Gen. Suhardi Alius as the new National Counterterrorism Agency (BNPT) head** on Wednesday has not only **raised hopes for better coordination of the nation's counterterrorism efforts**, but is also being seen as a positive sign of unity within the National Police amid rumors of internal power struggle. Suhardi, a reputable officer who has been spearheading reform in the detective division, particularly in addressing the long-running tradition of officers in the division giving money to their superiors, is known to have a close relationship with National Police chief Gen. Tito Karnavian. The appointment of the former chief secretary of the National Resilience Institute (Lemhanas), a position formerly held by Tito, is seen as a move that will greatly assist Tito in leading the police institution.

Malaysia's counter-terrorism efforts draw India's attention
The Star Online, Zulkifli Abdul Rahman, 2016 07 21
Kuala Lumpur - **Indian Prime Minister Narendra Modi has shown serious interest in Malaysia's moderation agenda and its counter-terrorism efforts,** said Deputy Prime Minister Datuk Seri Dr Ahmad Zahid Hamidi. During his 45-minute meeting with Modi on Tuesday, he said Modi asked extensively about Malaysia's de-radicalisation module, anti-terrorism legislation and welfare of Muslims. Modi told him Malaysia had vast experience in combating terrorism and

extremism, and he wanted to know more about terrorism preventive laws such as the Prevention of Terrorism Act (Pota) 2015 and the **Special Measures Against Terrorism in Foreign Countries Act 2015.** "I explained to him that such laws are not punitive legislation, but are more preventive in nature. "He told me that despite being a smaller nation, Malaysia had contributed much to counter-terrorism efforts at the international level.

Return to Table of Contents/ Retour à la table des matières

Africa/Afrique

Menace terroriste sur le Maroc : La DGSN dément
Aujourd'hui Le Maroc, Journaliste maison, 2016 07 25
Casablanca, Maroc - **Pas de menaces terroristes à Casablanca et Marrakech. C'est ce qu'assure la Direction générale de la sûreté nationale suite à la propagation de rumeurs portant sur un éventuel danger terroriste** menaçant ces deux grands pôles urbains du Maroc. La Direction générale de la sûreté nationale a, dans ce sens publié, un communiqué de presse pour démentir de manière catégorique une information attribuée à des «sources sécuritaires», véhiculée sur les réseaux sociaux, selon laquelle les «autorités marocaines auraient élevé le niveau d'alerte en raison d'une menace terroriste imminente durant ce week-end dans les villes de Marrakech ou de Casablanca, en demandant aux citoyens d'éviter de se rendre dans les lieux où pourraient être commis ces actes terroristes». **Dans son communiqué, la DGSN informe l'opinion publique que cette information est «fausse et dépourvue de toute vérité»,** et «dément catégoriquement l'existence d'une quelconque déclaration émanant d'une source sécuritaire officielle faisant état d'un éventuel risque d'acte terroriste imminent».

Kenya security accused of murder and abduction: report
Agence France-Presse, Staff report, 2016 07 20
Nairobi - **Security agencies are killing and abducting men in north-east Kenya who they suspect of links to Islamist extremists, a rights group said Wednesday. Human Rights Watch (HRW)** documented 34 "enforced disappearances" and 11 suspected "extrajudicial killings" over two years in Garissa, Mandera and Wajir counties as part of **counterterrorism operations in Kenya's predominately ethnic Somali north-east**. "People in northeastern Kenya deserve protection from Al-Shabaab attacks, not further abuse from the authorities," said HRW executive director Ken Roth, adding the cases documented were "just the tip of the iceberg." The report details people taken from their homes by masked, armed men who did not identify themselves, or beaten in the streets, before being driven away in government vehicles. Some of the disappeared were last seen in police or military custody. None has been charged with any crime, nor are their families able to trace them.

Return to Table of Contents/ Retour à la table des matières

Americas/Amériques

Dubi expresses confidence in Rio 2016 security plans following alleged plot on Games
Reuters, Liam Morgan, 2016 07 24

(Unidentified Placeline) - **International Olympic Committee (IOC) executive director for the Olympic Games Christophe Dubi has moved to allay fears over security at Rio 2016** by claiming the plans in place are "robust" enough to deal with any threat posed at the event. Concerns over security have been heightened after a group of 10 people were arrested on Thursday (July 21) on suspicion of planning a terrorist plot at next month's Games. An 11th suspect then handed himself into police on Friday (July 22), while authorities have continued to warn of "lone wolf" attacks at the event in the wake of a number of incidents across the world in recent months. Dubi told AgenciaBrasil that he had full confidence in the security plans that are in place for Rio 2016, some of which have had to be revised following attacks in Paris, Orlando and Nice.

A tug-of-war over the right to eavesdrop on Argentines
Buenos Aires Herald, 2016 07 24
Buenos Aires— The brewing debate over which public agency and who precisely has the **legal authority to eavesdrop on the private conversations** was sparked early last month but it is only the latest episode in a tug of war between the **Federal Intelligence Agency** (AFI), the Attorney General's Office and the Supreme Court that dates back to the first months of 2015. According to the La Nación newspaper, AFI officers have said they want to regain control of the agency — currently in the hands of the Buenos Aires City Federal Criminal Appeals Court — to help solve kidnapping cases and aid the fight against drug-trafficking. "Several judges have complained about the way the wiretaps are conducted and it is true that only judges can order to invade someone's privacy, not prosecutors. Prosecutors are one of the parties in investigations," said Justice Minister Germán Garavano when the transfer was announced. Former President Cristina Fernández de Kirchner and Congress had approved a major reform of the **intelligence services** because she thought that **Antonio "Jaime" Stiuso** and other agents had been behind the complaint late AMIA prosecutor Alberto Nisman filed accusing her of seeking to whitewash the alleged Iranian involvement in the 1994 attack on the AMIA Jewish community centre.

Brazilian intelligence community seeks French cooperation
Brazilian daily Folha de Sao Paul (via BBC Monitoring Americas), 2016 07 22
Rio de Janeiro— **Luiz Alberto Santos Sallaberry, Abin (Brazilian Intelligence Agency) counterterrorism director, in Paris held contacts with his French counterparts to seek information on the terrorist attack that killed 84 people in Nice** on 14 July. The intention is to use the information as prevention in possible attacks during the Olympics. Sallaberry, who declined to comment on the arrests that took place on Thursday (21) in Brazil, claiming that this information should be disclosed exclusively by the Justice Ministry, said that Abin every day receives dozens of terrorist warnings, which are assessed and investigated thoroughly. The main level of threat is the one already established, that is, the lone wolves. This is a worldwide trend. It happens not just in our country. Today, these lone wolves represent the major challenges in the areas of intelligence and security," Sallaberry said. The Brazilian team, also including Ronaldo Zonato Esteves, Analysis Coordinator, and Federal Police Agent Camilo Graziani Caetano Paes de Almeida, deputy coordinator of the Counter-terrorism Integrated Center, met with French agents of the DGSI and DGSE (General Directorate of Domestic and Foreign Security), the DRM (General Military Intelligence Directorate) and the UCLAT (Counter-Terrorism Coordination Unit).

Olympic security: Brazil adjusts to new threats with help from global partners
Christian Science Monitor, Taylor Barnes, 2016 07 21
Rio de Janeiro - Even amid questions of whether Brazil will face international threats of terror as host of the first Summer Olympics in the southern hemisphere, nations from around the globe

have stepped up to offer support and training opportunities to prepare it for this extraordinary situation. **Brazilian security officials say the cooperation will not only benefit athletes and fans here for the Olympics this summer, but could leave Brazil's forces with a legacy of new professional skills that can be applied more broadly at home**, ranging from detection of fake documents to improved airport security. Successfully hosting the sporting event will give the country - better known for its deeply troubled domestic security record, and underpaid law enforcement suffering poor working conditions - a positive international bump. "Wherever there has been an important event, we've had Brazilian police collecting information," **Andrei Rodrigues, a federal agent and the head of Brazil's special government agency dedicated to mega- event security,** said in an interview with Brazil's Zero Hora. Rodrigues has been invited to create a database of best practices in partnership with Japan, which will host the 2020 summer games, and has said observers from Russia and Qatar, the sites of the two upcoming World Cups, will come to Brazil for the August Games.

Brazil probes Olympics threats after group backs Islamic State
Reuters, Staff report, 2016 07 20
Brasilia - **Brazil's intelligence agency said on Tuesday it was investigating all threats to next month's Rio Olympics after a presumed Brazilian Islamist group pledged allegiance to Islamic State (IS)** less than three weeks before the Games. The SITE Intelligence Group that monitors the internet reported that a group calling itself "Ansar al-Khilafah Brazil" said on the Telegram messaging app on Sunday that it followed IS leader Abu Bakr al-Baghdadi and had promoted IS propaganda in Arabic, English and Portuguese. Brazilian authorities stepped up security measures following the truck massacre in Nice last week, planning security cordons, further roadblocks and the frisking of visitors in Rio de Janeiro for the Olympics. Police and soldiers took part over the weekend in drills near sports facilities and along transport routes. "All threats related to the Rio 2016 Games are being meticulously investigated, particularly those related to terrorism," the **Brazilian intelligence agency ABIN said in a statement when asked to comment on the previously unknown group's claim of support for Islamic State**. "Many are dismissed and those that deserve attention are investigated exhaustively," ABIN said.

Argentina's spy agency regroups, wins back power under Macri
Reuters, 2016 07 20
Buenos Aires— **A little over a year since Argentina's spy agency was shackled in the wake of the mysterious death of a star prosecutor, President Mauricio Macri is backing its quest for broader powers that critics fear will revive unfettered domestic spying**.
Argentina's spies are pressing Macri to remove restrictions imposed by former president Cristina Fernandez after public investigator Alberto Nisman was found dead in his home in 2015, a source in the judiciary said. Fernandez accused a rogue agent of playing a role in Nisman's murder, which came days after he accused her of covering up Iran's alleged role in the 1994 bombing of a Jewish center in Buenos Aires. Fernandez overhauled the country's spy agency in response, branding it the Federal Intelligence Service, or AFI. But despite the new name, the agency is starting to look more like the *former Intelligence Secretariat, w*ith agents purged by Fernandez moving back into old posts since Macri took power in December, said an intelligence source who spoke on the condition of anonymity.

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

10-08-2016 to/au 16-08-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Attentat terroriste déjoué: Trudeau compte sur le comité parlementaire annoncé
Presse Canadienne, 2016 08 16
Bridgetown, N.É.-- Le premier ministre **Justin Trudeau estime que le comité parlementaire créé pour surveiller les activités des agences de renseignement aura à évaluer l'efficacité du travail de ces agences.** La semaine dernière, la Gendarmerie royale du Canada (GRC) a intercepté un jeune Canadien qui préparait une attaque terroriste. Aaron Driver a été abattu par la police, mercredi soir, dans une petite ville du sud-est de l'Ontario. Le jeune homme était connu des autorités canadiennes. Mais c'est le FBI qui a alerté la GRC alors que l'homme préparait un attentat imminent. Le premier ministre a d'abord félicité les policiers canadiens pour leur travail. Puis, il a rappelé la nécessité d'un équilibre entre la sécurité des Canadiens et le respect de leurs droits, avant d'ajouter qu'un comité parlementaire, annoncé par son gouvernement le printemps dernier, jugera du travail des agences **comme la GRC et le SCRS (Service canadien du renseignement de sécurité).** "La surveillance assurera que nos agences de renseignement et de sécurité sont bel et bien en train de faire tout ce qui est nécessaire pour garder les Canadiens en sécurité", a déclaré M. Trudeau.

RCMP's handling of case questioned
The Globe and Mail, Alex Migdal, Tu Thahn Ha & Kathryn Blaze Baum, 2016 08 13
Ottawa - As police work to clear the scene of a foiled terrorism attack in Strathroy, Ont., residents are **questioning law enforcement's handling of the case and asking why they were not informed that an Islamic State sympathizer was living in their community**. Forensic officers and police dogs continued to comb the property where 24-year-old Aaron Driver had been living under a peace bond until he died Wednesday, in a confrontation with the RCMP that culminated in a bomb blast and gunfire. Canadian officials had acted on a tip from the **FBI**, which had somehow become aware of a video showing a man pledging allegiance to Islamic State leader Abu Bakr al-Baghdadi. Within hours, the RCMP determined that man to be Mr. Driver. A tactical team descended on the home and intercepted the bombcarrying man as he was about to leave in a taxi, bound for a mall in downtown London, Ont....Earlier this spring, **CSIS director Michel Coulombe** said the agency was aware of about 180 Canadians who are engaged with terrorist organizations abroad, while another 60 were back in Canada. RCMP Commissioner Bob Paulson said at the time that Canadian security agencies are keeping tabs on the 60 people who have returned here, even if there is not enough evidence to charge them.

Liberals still plan to repeal parts of counterterrorism powers brought in by Harper government
Ottawa Citizen, Jason Fekete and Marie-Danielle Smith, 2016 08 12
Ottawa - The **Liberal government**, following a thwarted terrorism plot, says it **still plans to repeal parts of sweeping new counterterrorism powers adopted by the Conservatives and insists Canada must focus much more on counter-radicalization**. Prime Minister Justin Trudeau's government came under fire Thursday from the opposition Conservatives over its plans to revoke some of the national security measures contained in the contentious Bill C-51, as well as for the Liberals' overall approach to fighting terror. The **Liberals want to guarantee that all Canadian Security Intelligence Service warrants respect the Charter of Rights and Freedoms;** require that government review all appeals by Canadians on the no-fly list; and

narrow overly broad definitions such as defining "terrorist propaganda" more clearly, among other measures.

Security threat in Ontario shows Canada is not immune to terrorism, says public safety minister
Regina Leader-Post, Will Chabun, 2016 08 12
Ottawa - **Wednesday's deadly terrorist incident in southwest Ontario underlines the importance of the new counter-radicalization centre the federal government plans to set up later this year, federal Public Safety Minister Ralph Goodale said** Thursday." The radicalization of young men raised in Canada has been a constant theme of terrorist attacks and near-attacks within Canada, including Wednesday's incident in Strathroy. Coming legislation for oversight of security agencies will give "extraordinary access" to classified information that will let committee members assess whether these agencies -- **RCMP, CSIS and Communications Security Establishment,** for example -- are effectively protecting Canadians while they also "safeguard the rights and freedom and values of Canadians."

Edmonton Police Admit to Owning Stingray Surveillance Device
Motherboard Blog, Jordan Pearson, 2016 08 12
Edmonton - The **Edmonton Police Service owns a controversial surveillance device called a "Stingray" that indiscriminately surveils any cellphone within its multi-kilometre range,** a police spokesperson confirmed on Thursday to Motherboard. According an emailed statement from police spokesperson **Anna Batchelor**, Edmonton's cops have "used the device in the past during investigations," but would not release any additional details in order to "to protect [Edmonton Police Service] operations." Until now, the only law enforcement in the country known to use the devices was the **Royal Canadian Mounted Police**, the country's analogue to the US **Federal Bureau of Investigation**.

Canada security questioned after FBI tip thwarts attack
Reuters, 2016 08 12
Ottawa - Aaron Driver first came to the attention of Canadian officials in late 2014 after he voiced support for Islamic State on social media. In 2015, the Muslim convert was arrested for communicating with militants involved with attack plots in Texas and Australia. Early this year, he agreed to a court order known as a peace bond that restricted his online and cell phone use. Yet **it took a tip from the U.S. Federal Bureau of Investigation to alert Canadian intelligence officials to what police say was an imminent attack Driver was planning on a major Canadian city**. Driver, 24, died after he detonated an explosive device in the backseat of a taxi as police closed in and opened fire, the Royal Canadian Mounted Police (RCMP) said in Ottawa. The 2016 budget provided C$35-million over five years to combat radicalization, but **little in the way of new funding for the RCMP or the Canadian Security and Intelligence Service (CSIS). Ray Boisvert**, a former assistant director of intelligence at CSIS, said Driver was likely on an increasingly long list of so-called "B- listers" - people known to law enforcement, but considered lower risk than others and not followed regularly.

Honest talk about terrorism
Ottawa Citizen, Phil Gurski, 2016 08 12
Opinion: Wednesday, in the southwestern Ontario town of Strathroy, a young man known to police for having terrorist connections was killed by security forces after he appeared to explode a device, and had another in his possession. The victim, Aaron Driver, had been arrested in June 2015 after expressing support for Islamic State (ISIL) and praising the October 2014 terrorist attack on Parliament Hill. Mr. Driver had been bound by a peace bond and had had several restrictions placed on him, including no online access and no possession of firearms or

explosives...**With what we know so far, it is fairly clear that the peace bond issued on Driver was not sufficient to stop him from preparing a terrorist act**. It is only thanks to the RCMP and its partners that no one was hurt or killed by whatever action Driver was planning. If Canadians decide that the **RCMP and CSIS should not be given certain powers and an act of terrorism takes place that perhaps would have been stopped** had those powers been granted, we are going to face a lot of soulsearching in this country. I am not trying to be dramatic, just a realist. No, we don't have to sacrifice everything in the pursuit of safety - but we do have to make sure we don't hamstring our protectors. (Note: Phil Gurski is president and CEO of Borealis Threat and Risk Consulting. www. borealisthreatandrisk. com)

VPD admit to mass-surveillance tool
Canadian Press, Geordon Omand, 2016 08 11
Vancouver - The **Vancouver Police Department's revelation that it has indeed employed a controversial mass-surveillance device despite initially insisting it had no documentation of its use raises serious legal and public accountability concerns**, a civil liberties group says. The VPD said it received help from the RCMP in using a socalled **StingRay** device during a 2007 investigation in an attempt to track down the cellphone of a person they believed had been abducted. **Micheal Vonn of the B.C. Civil Liberties Association** said it was only after a freedom-of-information request, direct questioning and the prospect of an inquiry by the province's privacy commissioner that the Vancouver police willingly disclosed any information. "This certainly raises a number of further questions," Ms. Vonn said. "How, if they've actually used the RCMP's StingRay, could there be no documents: no memorandum of understanding with the RCMP, no policies and procedures, no communications, nothing. This seems deeply problematic."

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

Donald Trump's Terrorism Plan Mixes Cold War Concepts and Limits on Immigrants
New York Times, David E. Sanger, Maggie Haberman, 2016 08 16
New York - **Donald J. Trump on Monday invoked comparisons to the Cold War era in arguing that the United States must wage an unrelenting ideological fight if it is to defeat the Islamic State.** He said he would temporarily suspend immigration from "the most dangerous and volatile regions of the world" and judge allies solely on their participation in America's mission to root out Islamic terrorism. In a speech at Youngstown State University in Ohio, a critical swing state where polls show him trailing Hillary Clinton, Mr. **Trump combined old vows to seize Middle Eastern oil fields with the announcement of a series of new, if still vague, proposals to change America's battlefield tactics.**

Hackers Say They Hacked NSA-Linked Group, Want 1 Million Bitcoins to Share More
Motherboard (Vice), Lorenzo Franceschi-Bicchierai, 2016 08 15
New York - A **mysterious hacker or hackers going by the name "The Shadow Brokers" claims to have hacked a group linked to the NSA and dumped a bunch of its hacking tools.** In a bizarre twist, the hackers are also asking for 1 million bitcoin (around $568 million) in an auction to release more files. " The hackers referred to their victims as the **Equation Group**, a codename for a government hacking group widely believed to be the NSA. The security firm Kaspersky Lab unmasked Equation Group in 2015, billing it as the most advanced hacking group Kaspersky researchers had ever seen.

Military Officials Distorted Intelligence on ISIS, Report Says
New York Times, Helene Cooper, 2016 08 12
Washington - **Officials from the United States Central Command altered intelligence reports to portray a more optimistic picture of the war against the Islamic State in Iraq and Syria than events on the ground warranted**, a congressional panel said in a report issued Thursday. The interim report, from a task force established by the Republican chairmen of the **House Armed Services Committee, Intelligence Committee and Defense Appropriations Subcommittee**, found "widespread dissatisfaction" among Central Command intelligence analysts, who said superiors were doctoring their assessments of American efforts to defeat the Islamic State. **Central Command, known as Centcom**, is the military headquarters in Tampa, Fla., that oversees American military operations across the Middle East and Central Asia. "Intelligence products approved by senior Centcom leaders typically provided a more positive depiction of U.S. antiterrorism efforts than was warranted by facts on the ground and were consistently more positive than analysis produced by other elements of the intelligence community," a news release about the report said.

Pentagon updates Reagan-era intelligence gathering guidelines
Washington Times, Andrew Blake, 2016 08 12
Washington - The **Pentagon on Wednesday published revised procedures governing the collection, retention and dissemination of intelligence concerning American citizens**. Outlined within the pages of DoD Manual 5240.01, **"Procedures Governing the Conduct of DoD Intelligence Activities,"** the changes pertain to how the U.S. military and assorted government agencies sweep up and store information concerning U.S. persons, including individuals whose details are incidentally collected during the course of investigating foreign targets. The manual updates provisions first laid out in an Executive Order signed by President Reagan in 1982, in turn incorporating new language and instructions for intelligence gathering to apply in a digitally-connected world that would have been impossible to imagine 30 years earlier.

How the U.S. Spies on Medical Nonprofits and Health Defenses Worldwide
The Intercept, Jenna McLaughlin, 2016 08 11
Washington - As part of an ongoing effort to "exploit medical intelligence," the **National Security Agency teamed up with the military- focused Defense Intelligence Agency to extract "medical SIGINT"** from the intercepted communications of nonprofit groups starting in the early 2000s, a top-secret document shows. Medical intelligence can include information about disease outbreaks; the ability of a foreign regime to respond to chemical, biological, and nuclear attacks; the capabilities of overseas drugs companies; advances in medical technology; medical research, and the medical response capabilities of various governments, according to the document and others like it, provided by **NSA whistleblower Edward Snowden**.

Iraqi Insurgents Stymied the NSA and Other Highlights from 263 Internal Agency Reports (Canada)
The Intercept, Margot Williams, Micah Lee, 2016 08 11
Washington - **Early in the fight against al Qaeda in Afghanistan and insurgents in Iraq, the National Security Agency was blindsided by enemy fighters' frequent use of rudimentary wireless communications devices known as "high-powered cordless phones**," according to documents among 263 published today by The Intercept. The documents, drawn from the agency's internal news site, **SIDtoday**, and provided by **NSA whistleblower Edward Snowden**, date mostly to the latter half of 2003, and show the NSA was at the time rapidly expanding its internet monitoring. But even as its digital surveillance grew more sophisticated,

the agency saw its targets increasingly adopting crude forms of communications like shortwave radio, SMS cellphone messaging and, most vexingly, high-powered cordless phones. The "poor man's cell phones," as the cordless devices were called, spread through Afghan borderlands and along Iraqi roadsides. Three months after announcing **InfoWorkSpace**, SIDtoday reported that signals intelligence directors from each Five Eyes agency held their first virtual meeting using the system, but "GCHQ was unable to attend due to a computer failure." In addition to sharing information within the U.S. government, the NSA also provides extensive signals intelligence to its allies. The NSA's closest foreign collaborators are known as "Second Party" partners or the "**Five Eyes**:" spy agencies from the world's English-speaking nations, including the **United Kingdom, Canada, Australia, and New Zealand**.

Classified Briefings and Candidates
New York Times, Michael Hayden, 2016 08 10
Op-ed - The **no-longer-presumptive nominees of the Democratic and Republican parties will soon start receiving periodic classified intelligence briefings**, with the first one coming perhaps this week. Rarely has this routine ritual received so much public attention -- and with good reason. To anyone who has actually had to protect the nation's secrets, Hillary Clinton's email setup as secretary of state was inconceivable and her later explanations of it were incomprehensible. The **judgment by the F.B.I. director, James B. Comey, that her handling of the emails was "extremely careless" was, to the intelligence tribe, a huge understatement**. **Donald J. Trump** has never been exposed to state secrets, so the issue is not that he may have been careless in the past. It's just that he seems to say anything that enters his head at the moment. That's a danger for someone who will now be living partly in a classified world. But with Mr. Trump, the issue goes even deeper. Earlier this week I joined 49 other former national security officials who had served in Republican administrations in declaring that he lacked the "character, values and experience" to be president.

FBI probe of Clinton's emails prompted by espionage fears, secret letters say
Vice News, Jason Leopold, 2016 08 10
New York - **Two secret letters the FBI sent to the State Department have revealed for the first time that the bureau's investigation into Hillary Clinton's private email server, and the classified emails sent through it, stemmed from a so-called "Section 811" referral from the Intelligence Community's Inspector General (ICIG).** The ICIG determined that classified, national security information in Clinton's emails may have been "compromised" and shared with "a foreign power or an agent of a foreign power." Section 811 of the Intelligence Authorization Act of 1995 "is the statutory authority that governs the coordination of counterespionage investigations between Executive Branch departments or agencies and the FBI." A Section 811 referral is a report to the FBI about any unauthorized information that may have been disclosed to a foreign power.

Is It OK for Spies to Elect a President?
The Daily Beast, Shane Harris, 2016 08 10
Washington - **It's a tenet of the intelligence business that spies are supposed to avoid the political fray,** declaring allegiance to no party or candidate, and speaking the unvarnished truth to whomever is in power. **Donald Trump has turned that tradition on its head.** Compelled by a candidate whom they say poses a unique threat to U.S. foreign policy and security, dozens of current and former intelligence professionals have in the past few months lept into the political arena in an unprecedented, coordinated effort to keep a presidential nominee from being elected. **This is new territory for American spies, who, when they do criticize politicians, tend to do it retrospectively in score-settling memoirs or op-eds**, and not in the heat of a presidential campaign. But just as the 2016 election has departed from tradition in so many

ways, intel professionals are now feeling unleashed to try to block Trump and help his opponent get elected.

Man used as test subject in CIA torture program to ask for Guantánamo release
The Guardian (London), Spencer Ackerman, 2016 08 09
New York - A **man the CIA used as a guinea pig for its post-9/11 torture program will plead his case for freedom from Guantanámo Bay later this month**, the Pentagon announced on Tuesday, in perhaps the hardest challenge to date for Barack Obama's intentions to empty the infamous detention center. **Zayn al-Ibidin Muhammed Husayn, better known as Abu Zubaydah**, is one of three men the CIA acknowledged that it waterboarded, a process simulating drowning, at an unacknowledged prison in Thailand. At some point during his 14-year captivity by the US, he lost the use of his left eye. The 23 August hearing, Guantánamo's equivalent of a parole board, will present the first time Zubaydah will have an opportunity to speak about his captivity - an opportunity that contradicts the CIA's preferences. The CIA, per a landmark 2014 Senate investigation, has contended that he ought to be held incommunicado until he dies.

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

British MPs given Mossad self-defence training after Jo Cox murder
Indo-Asian News Service, 2016 08 16
London - **British MPs are being taught unarmed street-fighting techniques used by the Israeli intelligence agency Mossad** in a bid to protect themselves from stalkers, terrorists, and political extremists in the light of **Jo Cox's murder**, it was reported on Monday. According to the Telegraph, the self-defence training known as "Krav Maga" -- Hebrew for "contact combat" -- combines jiu jitsu, judo, boxing, and street fighting. It teaches MPs how to defend themselves against attacks, including swinging punches to the head, a bottle, glass, or ashtray to the head, and a "slash with a knife, most commonly a 3-4 inch lock blade or kitchen utility knife". They will also learn how to disarm a lone-wolf attacker.

No Pokémon for British Spies, as Pokéstops Vanish From MI5 and MI6 Buildings
Motherboard (Vice), Victoria Turk, 2016 08 11
London - **British spies hoping to apply their skills to pokémon training may be out of luck**: Players report that pokéstops and pokémon gyms have vanished from London's **MI5 and MI6 headquarters**. A redditor by the name of Mesoplodon remarked this week that a gym located at the MI6 Building in Vauxhall (the one blown up in the James Bond film Skyfall) had been removed. Previously, several players had reported on Twitter and Reddit that there was a gym located at the MI6 Building, though some said it was not reachable from outside.

Nuclear espionage charge for China firm with one-third stake in UK's Hinkley Point
The Guardian (London), Maria L. La Ganga, 2016 08 11
San Francisco - The **Chinese company with a major stake in the proposed Hinkley Point C nuclear power station has been charged by the US government over nuclear espionage**, according to the US justice department. In a 17-page indictment, the US government said nuclear engineer **Allen Ho**, employed by the **China General Nuclear Power Company**, and

the company itself had unlawfully conspired to develop nuclear material in China without US approval and "with the **intent to secure an advantage to the People's Republic of China".** CGNPC has a 33% stake in the £18bn Hinkley Point project in Somerset, which Theresa May has delayed partly because of concerns over China's involvement.

Return to Table of Contents/ Retour à la table des matières

Australia / Australie

Cyber spies target high schools
Canberra Times, Adam Gartrell, 2016 08 14
Canberra - **Australia's top cyber security agency is targeting high school students as young as 14** as part of a recruitment plan to build an army of "white hat" hackers to shield the country from internet attacks like those that crippled the census. The **Australian Signals Directorate,** the shadowy spy agency that works out of the Department of Defence, **has embarked on a major new recruiting drive** - and teenaged bedroom hackers and computer whizkids are in its sights. The directorate - which is tasked with intercepting and analysing foreign communications under the motto "Reveal their secrets, protect our own" - has been distributing a recruitment brochure in public and private secondary schools and has even begun opening its doors for work experience placements for students from years 9 to 12.

A-G claims terror fears for diary secrecy
The Australian, Sean Parnell, 2016 08 12
Canberra - **Lawyers for the federal Attorney-General George Brandis have invoked a counter-terrorism argument in their bid to restrict access to official diaries under Freedom of Information laws,** potentially allowing elected officials greater secrecy over their affairs. Government lawyers will ask the Federal Court today to overturn an Administrative Appeals Tribunal ruling that Senator Brandis's office was wrong to refuse to process a Labor FOI request for diary entries on the basis that it would be too time- and resource-intensive. While the AAT found in favour of Labor, requiring the Attorney-General's office to process the FOI request for eight months of diary entries during 2013-2014, Senator Brandis's lawyers have advanced their initial argument that a "practical refusal reason" exists.

ASIO monitoring of right-wing extremists uncovered alleged plan to attack radical left
Sydney Morning Herald, Nick McKenzie & Michael Bachelard, 2016 08 12
Canberra - **ASIO's monitoring of the aggressive right-wing extremist movement uncovered alleged plans to attack an "extreme left" target, and led to the arrest last week of Braybrook man Phillip Galea.** Fairfax Media understands that Mr Galea's arrest was prompted by concerns that he and possibly two other members of right-wing groups were canvassing an attack aimed at their perceived political enemies in radical left-wing groups. His arrest marks a new and potentially dangerous development in the recent growth of extreme right-wing opinion in Australia. "Politically- motivated extremism is increasing, and it is a concern to the AFP and its law enforcement and national security partners," **Federal Police Assistant Commissioner Jennifer Hurst** told Fairfax Media. The Australian Security Intelligence Organisation warned in October that "violent rhetoric continued from extreme right-wing and left-wing individuals in Australia", and that the "terrorism environment is likely to remain fluid and will be affected by nationalist and ethnic tensions, acts of violence overseas and an increased propensity and ability for violence-prone individuals to move to action".

Australia blocks electricity network sale to Chinese bidders on security concerns
Reuters, Jonathan Barrett and Byron Kaye, 2016 08 11
Sydney - **Australia blocked the A$10 billion ($7.7 billion) sale of its biggest energy grid to State Grid Corp of China and Hong Kong's Cheung Kong Infrastructure Holdings** citing security concerns, a blow to the country's privatisation plan. Nine months after clearing the sale of TransGrid to an investor group 40 percent controlled by Kuwaiti and Abu Dhabi interests, **Australian Treasurer Scott Morrison** said on Thursday he was rejecting the sale of Ausgrid to the rival Asian bidders because of risks to the national interest. "**During the review process national security issues were identified in critical power and communications services that Ausgrid provides to businesses and governments,**" Morrison said in a statement. State Grid, China's dominant power distributor, did not immediately respond to requests seeking comment. Cheung Kong Infrastructure (CKI), controlled by Hong Kong billionaire tycoon Li Ka-Shing, said the decision was not related to CKI. Australia's decision to reject the bids deprives the New South Wales state government of what would have been a record haul for a single privatisation sale, and also underscores the country's changed political climate since a handful of protectionist senators took power in general elections last month.

Australian Bureau of Statistics says website attacked by overseas hackers
ABC (Australia), Staff reporter, 2016 08 10
Canberra - The **Australian Bureau of Statistics says it believes a series of hacking attacks which led to the census website being shut down last night were part of a deliberate attempt to sabotage the national survey**. The Australian Bureau of Statistics (ABS) says it believes a series of hacking attacks which led to the census website being shut down last night were part of a deliberate attempt to sabotage the national survey. Thousands of Australians were prevented from taking part in the census on Tuesday night as the ABS website crashed. This morning the ABS's **David Kalisch** said the census website had been attacked by hackers four times and was shut down as a precaution after the fourth attack. "It was an attack, and we believe from overseas," When asked if the hacks were a deliberate attempt to sabotage the census, Mr Kalisch replied: "We believe so". "The **Australian Signals Directorate** are investigating, but they did note that it was very difficult to source the attack."

Lone terrorists proving difficult to track
Australian Associated Press, Lauren Farrow, 2016 08 10
Jakarta - If **Australia is going to be able to successfully track the "virtually indistinct" financial transactions of lone wolf terrorists, the region must work together**, Justice Minister Michael Keenan says. More than 100 people are being monitored by Australia's financial intelligence agency - **AUSTRAC** - as authorities continue to grapple with a problem that will be around for decades. In an address to a summit in Bali on counter- terrorism, Mr Keenan is expected to tell the meet that while operationally there have been some successes in combating Islamic State, there has also been an increase in frequency and severity of terrorist attacks.

Return to Table of Contents/ Retour à la table des matières

New Zealand / Nouvelle-Zélande

GCSB wins power to spy on Kiwis
Dominion Post, Vernon Small, 2016 08 16
Wellington--The **Government is set to break a long-standing ban on the Government Communications Security Bureau (GCSB) spying on New Zealanders** with a sweeping

revamp that brings our spy agencies under a single law. Prime Minister **John Key** yesterday said Cabinet had accepted the bulk of changes, **including extra powers for the GCSB**, as recommended by the Cullen-Reddy review in March. He said the changes were the most significant reform to the agencies' legislation in the country's history. New Zealanders had a high degree of confidence the Government was "not out there snooping on their private thoughts, their private emails or aspects of their life that have no relevance to other New Zealanders", he added. **They expected the GCSB and the Security Intelligence Services (SIS)** to look for genuine or real threats that one or two of a very small group of people potentially posed.

The Raid
The Intercept, Ryan Gallagher, Nicky Hagger, 2016 08 15
Washington - Tony Fullman is a middle-aged former tax man and a pro-democracy activist. But four years ago, a botched operation launched by New Zealand spies meant he suddenly found himself deemed a potential terrorist -- his passport was revoked, his home was raided, and he **was placed on a top-secret National Security Agency surveillance list**. The extraordinary covert operation, revealed Sunday by Television New Zealand in collaboration with The Intercept, was launched in 2012 after New Zealand authorities believed they had identified a group planning to violently overthrow Fiji's military regime. As part of the spy mission, the NSA used its powerful global surveillance apparatus to intercept the emails and Facebook chats of people associated with a Fijian "thumbs up for democracy" campaign. The agency then passed the messages to its New Zealand counterpart, **Government Communications Security Bureau**, or GCSB. One of the main targets was Fullman, a New Zealand citizen, whose communications were monitored by the NSA after New Zealand authorities, citing secret evidence, accused him of planning an "an act of terrorism" overseas.

New GCSB bill allows spying on Kiwis
Stuff News New Zealand, 2016 08 14
Wellington - A **new bill which gives New Zealand's security and intelligence agencies more power to spy on Kiwis is likely to be introduced this week. Prime Minister John Key** said the expansion of powers of the **Government Communications Security Bureau (**GCSB) was for good reason. "If you wanted to allow GCSB to spy against a New Zealander, at the moment they can't do that," Key said on Breakfast. "Under the new law they would be able to, under very narrow conditions, but they'd need what's called a triple- lock warrant, so they need a warrant not only from the Commissioner and from the Minister but with review from the Inspector-General." A review undertaken by Sir Michael Cullen and Dame Patsy Reddy called for reform in a report released in March. The report into the country's intelligence and security laws recommended a single piece of legislation be established to cover both the GCSB and the **Security Intelligence Service (SIS)** - and its authors would have recommended a merger of the two agencies if they had been allowed.

Return to Table of Contents/ Retour à la table des matières

International

China / Chine

Espionage arrest of nuclear engineer fuels US suspicions of Chinese tactics
The Guardian, Rob Davies, 2016 08 11
London— A **string of cases have fuelled suspicions in the US and beyond that some Chinese firms will resort to any measures to obtain valuable intellectual property** that could give them a technological leg-up. In 2010, **former Boeing engineer Dongfan "Greg" Chung was jailed for 15 years and nine months for economic espionage** after he was convicted of passing trade secrets to Beijing to assist the Chinese aviation industry. In letters to a Chinese state official, Chung said that he wanted to "make some contributions to the modernisations [sic] of the Motherland". **FBI** agents began looking into Chung while investigating a separate case against Chinese-born naturalised US citizen Chi Mak. Mak was found guilty in 2007 of conspiring to export sensitive defence technology to China while working for defence contractor Paragon Power… Repeated allegations of spying by state-sponsored hackers have also added to tensions between the west and China. Repeated allegations of spying by state-sponsored hackers have also added to tensions between the west and China. Google's travails in China, where the search engine is banned, are well documented. In 2010, the US internet firm said a **cyber-attack originating in China** had targeted its intellectual property. Google said the attackers' main aim was to infiltrate the email accounts of Chinese dissidents and human rights activists, but it also flagged up efforts to steal information from companies in industries including chemicals, technology and finance. In 2014, a Chinese hacker group called Putter Panda, thought to be based in the offices of the **People's Liberation Army**, was said by security experts to have hacked satellite technology companies in the US and UK.

China steals FBI surveillance secrets through veteran who worked inside as spy
Asia Times, Bill Gertz, 2016 08 10
Unidentified Placeline— A **Chinese penetration agent operated secretly within the U.S. Federal Bureau of Investigation and passed valuable intelligence to Beijing** for at least 10 years without being detected. The case of Kun Shan Chun was disclosed by the Justice Department Aug. 1 as part of a plea agreement involving Chun admitting he acted illegally as a Chinese government agent. Chun, a Chinese-born naturalized U.S. citizen, was arrested in March although authorities kept the case secret until the plea bargain was announced last week. No details of the information supplied by Chun to China were provided by court papers made public in the case. However, as an electronic technician, Chun likely supplied **Chinese intelligence** with valuable **counter-surveillance information** that would assist the large numbers of Chinese agents operating in the United States in avoiding detection. Most of China's human and technical spying activities in the United States are carried out by the two main services, the civilian Ministry of State Security and militarily what has been called until recently the Second **Department of the General Staff Department**, known as 2PLA. China's espionage against the United States has produced several legendary coups. They included the theft during the 1990s of secrets related to all deployed nuclear warheads through recruiting American scientists at nuclear weapons labs.

Return to Table of Contents/ Retour à la table des matières

Russia / Russie

Putin Dismisses a Longtime Ally as Chief of Staff in Favor of a 'Servant'
New York Times, Neil MacFarquar, 2016 08 13

Moscow - **President Vladimir V. Putin unexpectedly fired his longtime chief of staff on Friday**, the latest in a series of high-profile Kremlin changes that have ushered out an older layer of Putin peers and replaced them with a younger generation of unquestioning loyalists. "Putin is gravitating toward those who serve him, and distancing himself from those who, by virtue of their resources, attempt to rule alongside Putin," wrote Tatyana Stanovaya, a political scientist, in a recent commentary for the Carnegie Moscow Center. "He does not need advice, he needs people who will carry out his orders with as little fuss as possible." As if on cue, after the announcement, pictures of **Anton E. Vaino, 44**, the relatively unknown aide promoted to chief of staff to replace **Sergei B. Ivanov**, suddenly popped up online. They showed Mr. Vaino shadowing Mr. Putin and even carrying an umbrella to protect the president from the rain. The changes come amid a spike in foreign and domestic tensions that might arrive as a welcome -- or manufactured, as some have suggested -- diversion for a nation depressed by a long stretch of economic hardships brought on by the collapse of oil prices and Western economic sanctions for Mr. Putin's adventures in Crimea and eastern Ukraine.

Crimea subversion group included professional secret service officers
ITAR-TASS World Service, Staff report, 2016 08 11
Moscow - **Yevgeny Panov, the supposed leader of the Ukrainian subversive group seized in Crimea, has made a confession stating that secret service career officers had been members of the group in charge of preparing sabotage attacks**. The video recording with his confessions was aired by Rossiya'24 news channel. "The group included the professional intelligence officers Alexander Kirillov (codename Kirill), someone Dmitry by name, and Oleg Litvinenko (codename Dog Fox). Also, the group includes Sambul Alexei (codename Sigh), and a guy whose first name or surname I don't know but who has the codename Deshikh," Panov said. The **Russian Federal Security Service** said on Wednesday, August 10, that it had detained a group of Ukrainian saboteurs near the city of Armyansk (Crimea) and that it had prevented terrorist attacks in Crimea prepared by the Ukrainian Defense Ministry's main intelligence directorate. The **FSB** said their planned targets were critically important infrastructure and life support facilities. (Full report).

Russia's FSB thwarts activity of online cells raising funds for IS
ITAR-TASS World Service, Staff report, 2016 08 11
Moscow - The **Russian Federal Security Service (FSB) has prevented the activity of the international Internet community cells promoting the ideas and raising funds for the Islamic State terrorist group (outlawed in Russia).** "The **Federal Security Service** in cooperation with the Russian Interior Ministry has identified and thwarted the activity of cells of the international online community "Rohnamo ba sui davlati Islomi" (translated as A Guide to Islamic State from Tajik) in the Sverdlovsk, Tyumen and Chelyabinsk regions set up to promote terrorist ideology and recruiting gunmen to the Islamic State of Iraq and the Levant," the FSB Public Relations Center has told TASS.

Russia Allows Rare Protest of New Antiterrorism Laws
New York Times, Lincoln Pigman, 2016 08 10
Moscow - **In a mass public protest with a rare permit, hundreds of critics of the Russian government gathered in Moscow on Tuesday evening to demonstrate against a new set of so-called antiterrorism laws.** Signed into law by President **Vladimir V. Putin** in July, the legislation introduced what critics have called intrusive measures, including requirements to store all communications data for six months, and phone and texting records for one to three years. **Protesters decried the legislation as an assault on privacy and internet freedom**.

Return to Table of Contents/ Retour à la table des matières

Europe

Un service de renseignement mieux armé mais mieux surveillé
Agence Télégraphique Suisse, 2016 08 15
Berne— Le **Service de renseignement de la Confédération (SRC)** disposera d'un nouvel arsenal de mesures pour lutter contre le terrorisme. Mais il sera davantage surveillé. Aperçu du projet soumis en votation et qui ne devrait pas entrer en vigueur avant la mi-2017. **Avec la nouvelle loi sur le renseignement, les agents du SRC pourront surveiller des communications (courrier, téléphone, courriel),** observer des faits dans des lieux privés, si nécessaire en installant des micros, ou perquisitionner secrètement des systèmes informatiques et y installer des "chevaux de Troie". Le Conseil fédéral estime à une dizaine par an le nombre de cas pouvant faire l'objet de ces "recherches spéciales", un cas complexe pouvant nécessiter plusieurs mesures..

One month after coup bid, Turkey transformed
Agence France Presse, Stuart Williams, 2016 08 14
Analysis : **With a thorough shake-up of its armed forces, a reassessment of foreign policy and the biggest purge in its modern history, Turkey has undergone a transformation in the month since the July 15 coup bid**. On the surface, street life has returned to its normal bustle in Istanbul and Ankara, where terrified residents witnessed bombings by fighter jets and tanks driving amok in the streets on the night of the attempted putsch. But the huge red Turkish flags hanging from public buildings, billboards hailing the coup's defeat and pictures in metro stations of the "martyrs" killed are all reminders that life is not the same as it was before the events which began at around 1900 GMT on July 15. **So far untouched by the shake-up is the powerful National Intelligence Agency (MIT)**, which has faced vehement criticism for failing to warn Erdogan about the coup. But the government has vowed it will also undergo restructuring.

Germany Proposes Measures to Combat Terrorism
New York Times, Alison Smale, 2016 08 12
Berlin - The **German government proposed a broad range of measures on Thursday to bolster security and combat terrorism**, its strongest official response so far to two recent attacks by terrorists pledging loyalty to the Islamic State and a deadly shooting rampage in Munich. Many of the measures, which include closer monitoring of refugees and enhanced surveillance, seem likely to win legislative approval but prompted concerns in a country that is deeply protective of privacy and civil liberties. The **proposals announced by the interior minister, Thomas de Maizière, call for hiring more federal police officers; making it a crime to express sympathy for terrorism; greater sharing of intelligence data across Europe**; closer watching of the "dark web," the part of the internet that is invisible to ordinary users; stripping dual citizens of their German citizenship if they fight for extremist groups; and making it easier to deport foreigners deemed to be dangerous.

Lutte antiterroriste : « le défi d'une génération » , selon Valls
Le Figaro, Philippe Goulliaud, 2016 08 12
Paris - En plein coeur de l'été, **l'exécutif tient à montrer que la sécurité reste une priorité absolue et qu'il reste à la barre,** après les polémiques qui ont suivi les attentats de Nice et de Saint-Étienne-du- Rouvray. **François Hollande a présidé jeudi matin un nouveau conseil de défense à l'Élysée, en présence de Manuel Valls, des ministres de l'Intérieur Bernard**

Cazeneuve, de la Défense Jean-Yves Le Drian, de la Justice Jean-Jacques Urvoas et des Affaires étrangères Jean-Marc Ayrault, ainsi que de hauts responsables civils et militaires. L'objectif était de faire le point sur les opérations antiterroristes en cours, tant qu'en France que sur les terrains extérieurs.

New far-right group comes under gaze of state spies
The Local (Germany), 2016 08 12
Berlin—The far-right Identitarian Movement is growing in popularity in Germany to the extent that the main federal intelligence agency has started watching them. Up until this point, the movement, which originated in France and has been present in Germany since 2012, had been observed by spy agencies at the state level. "We are seeing in the Identitarian Movement indications of efforts to undercut the democratic order," said **Hans-Georg Maaßen, head of the Federal Office for the Protection of the Constitution - Germany's domestic security agency**. He added that the group seems to have become more radicalized in its anti-asylum efforts in the time since Germany started accepting hundreds of thousands of refugees last summer.

Estonian PM, US intelligence coordinator speak about security
Baltic News Service, 2016 08 11
Tallinn--**Estonian Prime Minister Taavi Roivas and Director of U.S. National Intelligence James Clapper in their meeting on Thursday spoke about the security situation** in the region and cooperation between the two countries. **"Good intelligence analysis and substantive exchange of information help to make the right decisions. I'm glad that the intelligence institutions of Estonia and the United States are working closely together," Roivas said** at the meeting held in Tallinn. A retired lieutenant general in the United States Air Force, Clapper served as director of the **Defense Intelligence Agency (DIA**) from 1992 until 1995. He was the first director of defense intelligence within the Office of **the Director of National Intelligence** and simultaneously the under secretary of defense for intelligence. Clapper has held several key positions within the U.S. intelligence community. He served as the director of the National Geospatial-Intelligence Agency (NGA) from September 2001 until June 2006.

Terrorisme: nouveau conseil de défense à l'Elysée
Agence France-Presse, Journaliste maison, 2016 08 11
Paris - Le **président François Hollande a réuni jeudi à l'Elysée un nouveau conseil restreint de défense en présence du chef de gouvernement et de plusieurs ministres pour faire le point sur les opérations anti- terroristes en cours**, à l'intérieur et à l'extérieur de la France. Dans la foulée de la réunion, le chef de l'Etat doit se rendre en Corrèze pour visiter l'Ecole de gendarmerie de Tulle et Manuel Valls à Montluçon, dans l'Allier, également pour visiter une Ecole de gendarmerie accueillant des réservistes en formation. Le Conseil a commencé juste après 9H00 par un point d'information sur les graves incendies dans les Bouches-du-Rhône effectué par le ministre de l'Intérieur **Bernard Cazeneuve**. A côté des deux têtes de l'exécutif, étaient également présents le ministre de la Défense Jean-Yves Le Drian, de la Justice Jean-Jacques Urvoas et des Affaires étrangères Jean-Marc Ayrault. Avec eux se trouvaient le chef d'état-major des armées, le général Pierre de Villiers, **le directeur de la DGSE Bernard Bajolet et Louis Gauthier, secrétaire général de la Défense et de la Sécurité nationale**.

L'Allemagne veut durcir sa législation antiterroriste après les attentats
Agence France-Presse, Journaliste maison, 2016 08 10

Berlin - **Le ministre allemand de l'Intérieur prépare une batterie de mesures pour renforcer ses outils de lutte contre le terrorisme après les deux attaques du mois de juillet** revendiquées par le groupe Etat islamique, a indiqué la presse allemande mercredi. Le ministre Thomas de Maizière, qui a prévu une conférence de presse jeudi, veut en particulier introduire une procédure accélérée d'expulsion de réfugiés et demandeurs d'asile "représentant un danger pour la sécurité publique", selon le quotidien populaire Bild citant des sources sécuritaires. Cette mesure fait suite aux deux attentats commis dans le sud du pays fin juillet dans le pays qui a accueilli plus d'un million de migrants en 2015.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Iran detain a dual national linked to British intelligence

Reuters, 2016 08 16

Tehran - **Iran said on Tuesday it had arrested a dual national last week in Tehran linked to Britain's intelligence service**, the latest in a string of arrests of dual nationals over the past year. "The accused was working in an economic sector related to Iran," Tehran prosecutor general, **Abbas Jafari Dolatabadi**, was quoted as saying by the state news agency IRNA. Dolatabadi **did not identify the accused person nor the second nationality**. The prosecutor said the arrest was part of a crackdown against what officials have portrayed as "Western infiltration". Iran's potential opening up to the West after last year's nuclear deal has alarmed Iranian hardliners.

Israel arrests Palestinians 'recruited by Hezbollah' via Facebook

Agence France Presse, 2016 08 16

Jerusalem— **Israel's Shin Bet security service announced Tuesday it has arrested a network of Palestinians allegedly recruited via Facebook** by Lebanon's militant Hezbollah movement to attack Israelis. "Along with the orders to carry out shooting attacks and suicide bombings against Israeli targets, the agents were ordered to help recruit more (Palestinians) for the organisation's activities," a **Shin Bet** statement read. In one case, a Hezbollah agent had used Facebook to recruit a resident of Qalqilya who in turn recruited four others from his city in the north of the occupied West Bank, it said. The five allegedly began gathering intelligence on Israeli army activities in the area and to conduct weapons training, before being arrested in June. Shin Bet also said a Gazan recruited by Hezbollah through Facebook recruited three Palestinians from the West Bank who had started to train and plan attacks.

'The James Bond of Israel': Daniel Silva's spy series takes us deep into Israeli intelligence

National Post Online, Robert Fulford, 2016 08 15

Review : A building blows up in the Marais district of Paris. Vengeful Palestinians are knifing Israeli civilians at random. ISIL, the Islamic State, is charging across the landscape. This is the torn-from-the-headlines background where **Daniel Silva locates his most recent thriller featuring an Israeli spy, Gabriel Allon**. Once a year since 2000, Silva has written a new novel about the exploits of Allon as a soldier on "the secret battlefields of Europe and the Middle East." The 16th in the series, The Black Widow (HarperCollins), will not surprise his followers. Like the earlier books it takes us deep into Israeli intelligence as Silva imagines it and into the life of the remarkable Allon, a spy so good that all other spies measure their careers against his. e's the James Bond of Israel, but more talented and deeper. Like Bond, he chases villains into

every remote corner where they hide. Like Bond, he often gets into life threatening predicaments at the hands of his enemies. In fact, a recent attempt on his life was so credible that Israel decided to announce his death just to confuse the would-be killers and give him time off-the-grid to recover from his injuries. Unlike most fictional spies, Allon can double as an administrator. He's slated to become head of what Israel calls the **Mossad**, which Silva's characters never call anything except the Office.

A spy tale so real that Israel censored it
The Washington Post, Richard Lipez, 2016 08 15

Book Review: **"The English Teacher" is the story of a Mossad operative written by a former Israeli intelligence officer**. It's not an autobiography but rather a thriller, based loosely on facts, or as its author, **Yiftach Reicher Atir**, writes in his introductory note, "a true story, of real life operatives that are wholly made up, and actual missions that never happened." **Atir provides an astonishing look at Middle Eastern spycraft.** He alerts readers that "numerous changes and omissions were imposed" by his government's censors. Because a lot of what got into the novel seems plenty revealing and is often hair-raising, one is left wondering what shockers were left out. Also, how much of what Atir (who participated in the 1976 hostage-rescue operation in Entebbe, Uganda) put into the book is actually disinformation meant to throw other Middle Eastern intelligence agencies off track about how the Mossad spy agency actually operates?

Iranian Supreme Leader Meets Intelligence Minister, Officers
Fars News Agency, 2016 08 10
Tehran - **Supreme Leader of the Islamic Revolution Ayatollah Seyed Ali Khamenei held a meeting with the intelligence ministry officials and officers, advising them to keep a close eye on the country's redlines, specially with regard to the US**. "Drawing a line of separation with the head of the (world) arrogance stream, that is the US, is amongst the most crucial, and definite principles pursued by the late Imam (Khomeini) and this issue can no way be compromised and ignored," Ayatollah Khamenei said during the meeting in Tehran on Tuesday.

Return to Table of Contents/ Retour à la table des matières

Asia / Asie

More info needed to analyze change over N.K. intelligence agency: Seoul
Yonhap News Agency, 2016 08 16
Seoul--**South Korea said Tuesday that more information is needed to analyze whether control of North Korea's intelligence agency** has changed following the latest overhaul of its cabinet organization. The **Ministry of State Security**, **Pyongyang's intelligence** agency, was previously placed under the control of the powerful National Defense Commission (NDC) before the country's parliament replaced the NDC with a newly created state apparatus named the State Affairs Commission (SAC) in late June. The NDC previously had three ministries--the Ministry of People's Armed Forces, the North's defense ministry, and the Ministry of People's Security, the North's police agency--under its wing.

Bali summit agrees to stronger collaboration to combat terrorism financing
Jakarta Post, Ni Komang Erviani, 2016 08 12
Jakarta - **Country representatives participating in the second Counter-Terrorism Financing Summit agreed on Thursday to a Nusa Dua Statement for stronger**

collaboration on countering terrorism financing. The statement is a follow-up to the Sydney Communiqué agreed to in the first summit in Sydney, Australia, last year. All delegates from 26 countries proclaim in the Nusa Dua Statement that "the Islamic State (IS) in Iraq and the Levant constitutes a global threat to international peace and security". In the statement, they also emphasize that governments cannot work alone to protect financial systems and regional security from terrorism and its financiers.

Govt. to strengthen anti-terror laws, apparatus
Press Trust of India, 2016 08 12
New Delhi - With terrorists widely using social media for their propaganda and new threats emerging, **Union Home Minister Rajnath Singh on Friday said the NDA government is working on strengthening the anti-terror laws and providing legal protection for under cover operations**. Addressing the 'national conference on investigating agencies', the Home Minister said the government is committed to punishing terrorists and is working to strengthen the **Unlawful Activities (Prevention) Act and the National Investigation Agency (NIA) Act.** "We are considering legal protection for undercover operation, use of intelligence collected as evidence and entire gamut of issues relevant to combating terrorism," he said. Mr. Singh said due to widespread use of social media by terrorists, new threats have been emerging in the country.

Security forces seek warrantless wiretaps
Bangkok Post, Wassayos Ngamkham and Ariane Kupferman-Sutthavong, 2016 08 11
Bangkok - **Police are seeking the cabinet's go-ahead to wiretap criminal suspects without having to wait for the court's permission to speed up their investigations**. The request is believed to have support and backing from other security forces and the **National Security Council (NSC)**. A source at the Royal Thai Police (RTP) said Pol Col Kreangsak Chutiwut, chief of the Office of Legal Affairs and Litigation's legal affairs unit, had made the request to the cabinet.

Kunduz intelligence chief wounded in Taliban ambush
Pajhwok Afghan News, Ajmal Kakar, 2016 08 10
Kunduz City - The **intelligence chief for northern Kunduz province was wounded in a Taliban ambush** on Wednesday, a security official said. The **National Directorate of Security (NDS) director, Gen. Mohammad Jassim Anwari**, came under attack on his way to the airport in the provincial capital. Senior police officer Brig. Gen. Aziz Kamawal told Pajhwok Afghan News the NDS director had been wounded in the legs. However, he is said to be in stable condition. Meanwhile, another police officer, who did not want to be named, said Gen. Anwari had been evacuated to a hospital of German forces in Mazar-i-Sharif for medical care. With the Taliban yet to comment on the ambush, security officials said no one else was harmed in the incident.

PM should sack officers of intelligence agencies if they fail to trace Quetta attack perpetrators
Pakistan Dawn, Raza Khan, 2016 08 10
Islamabad - **Pakhtunkhwa Milli Awami Party (PkMAP) chief Mahmood Khan Achakzai on Tuesday demanded from the prime minister to sack officers from the security and intelligence agencies** if they fail to trace out the elements involved in the **deadly Quetta attack**. “Nawaz Sharif should sack the concerned officers of the intelligence and security agencies if they are unable to trace-out the executors and masterminds of the attack in Quetta within a specified time,” said Achakzai while taking part in the National Assembly debate on Monday’s blast. The PkMAP chief termed the Quetta attack an intelligence failure and

demanded to fix the responsibility of the blast. He asked the premier to "act as the real chief executive and take bold decisions". “Nawaz Sharif is chief executive of the country. He must order the security and intelligence agencies to hold an inquiry into the Quetta attack,” said Achakzai.

Return to Table of Contents/ Retour à la table des matières

Africa / Afrique

Le clan présidentiel continue de voir partout l'ombre de l'ex- chef du DRS
Liberté (Algérie), Mehdi Mehenni, 2016 08 14
Alger - Le **clan présidentiel continue de voir partout l'ombre de l'ex-chef du DRS Toufik ou la paranoïa du pouvoir** Il ne se passe plus un événement dans le pays sans que le clan au pouvoir soupçonne l'ombre du toujours mystérieux ex-patron du **Département du renseignement et de la sécurité (DRS).** Après la main de l'étranger, c'est désormais la main de Mohamed Mediène, dit Toufik, que le pouvoir agite pour... sévir ! Son ombre plane toujours et l'"exagération" dont use actuellement le clan au pouvoir, par rapport à de supposées manoeuvres en sourdine du général Toufik, prêtent parfois à rire.

Africa Intelligence Chiefs Unite to Protect International Law
The New Times (Rwanda), 2016 08 10
Kigali—**African intelligence and security services chiefs have called for temporary suspension of all pending arrest warrants and prosecutions filed against African leaders** and high ranking officials until discussions are held among stakeholders to resolve the stalemate. This was part of the declaration following a week-long **Conference of the Committee of Intelligence (CISSA) in Kigali** that attracted Chiefs of Intelligence Services from 51 African countries. Among other items on agenda, the meeting deliberated on how African countries have fallen victim to abuse of international law. The Conference was held under the theme, "Countering the Growing threat of Abuse of Universal Jurisdiction against Africa."

Return to Table of Contents/ Retour à la table des matières

Americas / Amériques

Brazil uses collaborative approach to track terror threats during Olympics
USA Today, Taylor Barnes, 2016 08 12
Rio de Janiero—Above the food trucks and cruise ships stationed along Rio's festive Olympic Boulevard, a quiet room is lined with desks that have a flag above each computer: Iran, Russia, China, United States, Oman. The police here watch a news memo board, a map with roving red squares that represent federal agents monitoring sports venues, and a live stream of Olympic judo. **Brazilian organizers say this control room is one of several such centers that represent a unique approach to collaboration to provide security for the 500,000 foreign guests during the August and September sports competitions here in Rio de Janeiro**. The Games have so far gone off without any major hitch in security for visitors other than conventional crime and robberies, just like Brazil's 2014 World Cup and 2013 Confederations Cup. Brazilian hosts say they have taken every measure necessary to prepare themselves for threats unknown. Brazilian authorities gave few details on the arrests, only saying that the goal was "to guarantee the security of the Olympic Games and citizens' well-being." In a similar series of arrests in July, a prosecutor confirmed that their tip came from the **Federal Bureau of Investigation**. What's unique about **Rio's International Police Cooperation Center (IPCC),** according to Urquiza, is actively sharing information rather than the host nation's police

informing visiting agents once a day in briefings of occurrences in the area, as he said was the case in the 2010 World Cup in South Africa and the 2008 Beijing Olympics. Brazilian police opened this special control room for international law enforcement to work on its premises around the clock. In addition to Rio's IPCC, which hosts representatives from 31 countries, a corollary center in Brasilia pools intelligence data to monitor foreigners arriving in Brazil. Another in the capital city focuses on counter-terrorism, drawing on nine countries which Urquiza said have the best know-how in the field

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

24-08-2016 to/au 30-08-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Port du hijab dans la GRC --Une pratique déjà permise dans d'autres agences représentant la loi
La Presse+, Joël-Denis Bellavance, 2016 08 29
Ottawa--En permettant à ses agentes de confession musulmane de porter **le hijab avec leur uniforme** en janvier, la **Gendarmerie royale du Canada** (GRC) **a simplement emboîté le pas à plusieurs autres organisations fédérales chargées de faire respecter la loi et l'ordre**. La Presse a appris que **l'Agence des services frontaliers du Canada (ASFC), le Service canadien du renseignement de sécurité (SCRS), l'Administration canadienne de la sûreté du transport aérien (ACSTA) et Services correctionnels Canada (SCC) offrent déjà à leurs employées respectives depuis un certain temps le droit de porter le hijab**...Le SCRS, dont les employés travaillent dans l'ombre et à l'abri des regards, n'offre pas d'uniforme à ses employés de sorte que ces derniers peuvent porter ce qu'ils veulent. « Le SCRS est un organisme civil. Par conséquent, les employés ne portent pas d'uniforme. Il n'y a donc pas de politique en oeuvre à ce sujet. Au SCRS, non seulement la diversité fait- elle partie de sa culture, mais elle y constitue une stratégie fondamentale. La diversité de son effectif aide le SCRS à atteindre ses objectifs. Elle lui permet de mieux comprendre les données démographiques des communautés canadiennes qu'il protège et ainsi d'être mieux outillé pour recueillir des renseignements pertinents et exacts. Ensemble, les employés du service parlent environ 106 langues et son effectif est représentatif de cela », a précisé **Tahera Mufti**, porte-parole du SCRS.

Exclusive: Mountie outlines roadblocks in terror fight
CTV.CA, Josh Dehaas, 2016 08 26
Ottawa - **On the same day a new report confirmed hundreds of Canadians have travelled abroad in support of terror groups like ISIS, one of the country's top cops outlined for CTV News what he sees as flaws in the fight against extremism**. In an exclusive interview with Mercedes Stephenson, RCMP **Deputy Commissioner Mike Cabana** said the Mounties receive significant amounts of **information from CSIS and the FBI** but are barred from bringing charges. "Sometimes we have information that clearly indicates the individuals may be moving toward violent tendencies but unfortunately we cannot proceed with criminal charges because that information would be inadmissible," Cabana said. Another problem for the RCMP is tracking terror suspects. Police estimate that only about half of terror suspects in Canada are ordered by judges to wear GPS tracking bracelets.

Liberals end Harper Tories' anti-terror project
Globe and Mail, Colin Freeze, 2016 08 26
Ottawa - **As the Liberals prepare to launch their signature anti- terrorism initiative, they have closed the door on a previous one by the Conservative government**. On Thursday, Liberal **Public Safety Minister Ralph Goodale released a report on the terrorist threat to Canada that said the Islamic State is the main concern**. The report also said that a fiveyear initiative by the Tories that had delivered $10-million, mostly to academics researching terrorism in hopes of finding ways to understand and fight it, had ceased operations in March.

RCMP allow wearing of hijab to attract Muslim women to force
Globe and Mail, Laura Stone, 2016 08 25
Toronto - **Female members of the RCMP are now allowed to wear a hijab head scarf as part of their uniform, as the Mounties look to encourage more Muslim women to join their ranks**. The newly discovered uniform option was adopted by the force in January. But according to law, members must still seek approval from RCMP Commissioner Bob Paulson for any faith-based accommodation, and there has yet to be a formal request to wear the hijab while on duty. "The move to offer the hijab as part of the RCMP uniform is intended to better reflect the changing diversity in the community and encourage more Muslim women to consider policing as a career option," **according to an RCMP briefing note sent to Public Safety Minister Ralph Goodale.** "The objective will be to demonstrate that the RCMP is a progressive and inclusive police service that values and respects persons of all cultural and religious backgrounds," it said.

What Aaron Driver taught us - As Ralph Goodale's ministry of public safety takes the lead on counter-radicalization, where is the RCMP?
Maclean's Magazine, John Geddes, 2016 08 25
In showing that chilling video of Aaron Driver, clad in a black balaclava, on a big screen at the force's Ottawa headquarters, above the heads of two grim-faced senior Mounties, the RCMP's message was clear: This is what homegrown terrorism looks and sounds like, and Canadians should be thankful that fast, smart police work stopped him from carrying out his murderous plan. But another point could also be taken from the story of Driver's death on Aug. 10 in Strathroy, Ont., killed by a police bullet after the 24-year-old self-proclaimed ISIS supporter set off a homemade explosive device in the back of a taxi. In fact, Public Safety Minister Ralph Goodale wasted no time making it: "The government of Canada has to get far more proactive on the whole issue of outreach, community engagement, counter-radicalization, determining how and in what means the right positive constructive influences can be brought to bear to change what otherwise would be dangerous behaviour." Within days he was visiting a Montreal centre that tries to help parents who fear their sons are being drawn to violent ideas, like Driver's embrace of radical Islam. Goodale announced that he will soon appoint an adviser on the issue, and later set up a counter- radicalization office. **What Goodale didn't spell out was that by assuming the lead on this long-overdue push, his department appears to be taking over where the RCMP has failed to make visible progress. The federal police force has been touting its work on countering violent extremism for a few years. In late 2014, Mounties said a landmark program would be rolled out in early 2015.** The basic concept was to support "hubs" where RCMP officers would work with groups of social agencies, religious leaders and community groups to intervene when radicalized individuals looked to be heading toward violence. But no big national launch ever happened.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

FBI says foreign hackers penetrated state election systems
Yahoo News, Michael Isikoff, 2016 08 30
Washington - **The FBI has uncovered evidence that foreign hackers penetrated two state election databases in recent weeks, prompting the bureau to warn election officials across the country to take new steps to enhance the security of their computer systems,**

according to federal and state law enforcement officials. The FBI warning, contained in a "flash" alert from the FBI's Cyber Division, a copy of which was obtained by Yahoo News, comes amid heightened concerns among U.S. intelligence officials about the possibility of cyberintrusions, potentially by Russian state-sponsored hackers, aimed at disrupting the November elections. Those concerns prompted **Homeland Security Secretary Jeh Johnson to convene a conference call with state election officials on Aug. 15**, in which he offered his department's help to make state voting systems more secure, including providing federal cybersecurity experts to scan for vulnerabilities, according to a "readout" of the call released by the department. Johnson emphasized in the call that Homeland Security was not aware of "specific or credible cybersecurity threats" to the election, officials said.

Russian Bid to Affect U.S. Voting Is Suggested
New York Times, David E. Sanger, 2016 08 30
Washington - The **Senate minority leader, Harry Reid of Nevada, asked the F.B.I. on Monday to investigate evidence suggesting that Russia may try to manipulate voting results in November**. In a letter to the F.B.I. director, James B. Comey Jr., Mr. Reid wrote that the threat of Russian interference "is more extensive than is widely known and may include the intent to falsify official election results." Recent classified briefings from senior intelligence officials, Mr. Reid said in an interview, have left him fearful that President Vladimir V. Putin's "goal is tampering with this election." **News reports on Monday said the F.B.I. warned state election officials several weeks ago that foreign hackers had exported voter registration data from computer systems in at least one state**, and had pierced the systems of a second one. The bureau did not name the states, but Yahoo News, which first reported the confidential F.B.I. warning, said they were Arizona and Illinois. Matt Roberts, a spokesman for Arizona's secretary of state, said the F.B.I. had told state officials that Russians were behind the Arizona attack. After the F.B.I. warning, Arizona took its voter registration database offline from June 28 to July 8 to allow for a forensic exam of its systems, Mr. Roberts said.

If Spies Can Hack Our iPhones, What's Stopping Them From Framing Us for Crimes?
Haaretz, Jack Watling, 2016 08 30
Jerusalem - "**There is something intimate and insidious about a telephone," observed former CIA officer William Johnson, in his 1987 monograph on the spy trade.** "No matter how careful I am when using the telephone, I cannot help giving away information of value to somebody investigating me." If you want to put this to the test, try setting up a meeting with someone without using any words that could allow a third party to work out where or when it will take place, or the subject to be discussed. **Today's spies are just as quick to acknowledge that phones — and especially smartphones — are not secure**. These devices leak revealing personal information to anyone who takes an interest, and yet outside the intelligence community the news of the latest vulnerability is met with an amnesic surprise.

FBI vs. State Department Over Hillary Clinton's Secrets
The Daily Beast, Shane Harris, 2016 08 29
Washington - **The FBI and the State Department are at odds over whether Hillary Clinton's personal lawyers had the proper government-issued security clearances that they needed to keep copies of her emails in a Washington**, DC, law office last year. Some of those emails contained classified information, which the lawyers and State Department officials knew at the time. The issue has become a flashpoint in the broader controversy over Clinton's private email server. Republican lawmakers are pressing the FBI on whether it investigated the State Department's decision to give security clearances to Clinton's attorneys and let them store copies of the emails on a thumb drive.

U.S. Revamps Line of Attack in Social-Media Fight Against Islamic State
Wall Street Journal, Nicole Hong, 2016 08 29
New York - Recent initiatives by technology companies to push back against Islamic State's social-media messaging highlight a sobering fact: The U.S. government's battle on that front has mostly sputtered. In a number of terrorist attacks over the past year, the attackers were found to have been inspired by Islamic State propaganda and videos, which are often described as Hollywood-level productions. Despite numerous military victories against Islamic State, U.S. officials acknowledge they have struggled to counteract the terrorist group's online campaign. **"We were able to disrupt networks, arrest terrorist cells, kill terror operatives," said Ali Soufan, a former Federal Bureau of Investigation counterterrorism agent who now runs a security consulting firm, the Soufan Group**. But "we haven't been doing a great job in countering the ideology." The government's countermessaging efforts so far have been scattershot and, some close to the government think, largely ineffective. **Officials say the government's new strategy is to empower third parties to create their own messages**, a contrast from earlier efforts that were criticized for having too much direct government involvement.

Lessons in how not to operate the FBI
Los Angeles Times, Del Quentin Wilber, 2016 08 26
Washington - Dressed in plainclothes to blend in with tourists at the National Mall, **a few dozen FBI agents in training fanned out across the Martin Luther King Jr. memorial on an unusual mission.** Their months-long training at the FBI Academy in Quantico, Va., covers target practice, boxing, surveillance and self-defense. But these trainees were dispatched on a more personal quest at the Washington memorial: Pick the most inspirational King quote among those etched into stone slabs and then share their insights during a brief, touchy-feely rap session in the shadow of the slain civil rights leader's statue. The field trip capped one of the **newest exercises** added to the training for aspiring agents and analysts. It's a **daylong dive into the FBI's investigation into King, including a surprisingly frank review into improper wiretapping**, harassment, abuse of power and racially motivated double standards. The training is the brainchild of **FBI Director James B. Comey**, who in 2014 began mandating this institutional introspection into what he called the "shameful" targeting of King by former FBI Director J. Edgar Hoover, which included delving into King's sex life and trying to destroy his reputation.

U.S. rules out swap of jailed Cuban spy Ana Belen Montes
Miami Herald, Nora Games Torres, 2016 08 26
Miami— The O**bama administration "has no intention" of releasing or swapping jailed Cuban spy Ana Belen Montes,** according to a letter sent by the U.S. Department of State to the House Permanent Select Committee on Intelligence. The Aug. 19 letter, obtained by el Nuevo Herald, followed a number of news reports pointing to the **possibility of freeing Montes -- a top Defense Intelligence Agency (DIA) analyst on Cuban affairs who is serving a 25-year prison sentence --** in exchange for Cuba handing over American fugitive Assata Shakur, formerly known as Joanne Chesimard. The letter, addressed to committee chairman Devin Nunes, R-Ca., says the State Department "want(s) to assure you that the United States government has no intention of releasing or exchanging Montes."

US intelligence still sorting out NSA hack
Associated Press, Staff report, 2016 08 25
Yorba Linda, California - The U**.S. is still probing the extent of a recent cyber leak of what purports to be hacking tools used by the National Security Agency**, the nation's top intelligence official said Wednesday. "We are still sorting this out," **James Clapper**, director of

national intelligence, said at an event at the Nixon Presidential Library and Museum in Yorba Linda, California. "It's still under investigation," Clapper said. "We don't know exactly the full extent -- or the understanding -- of exactly what happened." The tool kit consists of malicious software intended to tamper with firewalls, the electronic defenses protecting computer networks.

CIA releases thousands of previously classified briefings to Presidents Nixon and Ford
Los Angeles Times, David S. Cloud, 2016 08 24
Washington - The **CIA pulled the veil back Wednesday on long- classified foreign intelligence briefings it gave President Nixon in the 1970s during both the height of his power and his fall from grace,** a period of intense turmoil at home and abroad. The release of 2,500 President's Daily Briefs -- about 28,000 pages in all -- shed light on such historic events as Nixon's opening to China, the invasion of Cambodia, the U.S.- backed overthrow of an elected leader in Chile, the 1973 Arab-Israeli war, and ultimately the first resignation of a sitting U.S. president. The release also covers briefings given to President Ford, who took over when Nixon resigned on Aug. 9, 1974, until he left office in January 1977. That period included the fall of Saigon and the end of America's bitter war in Vietnam. **CIA Director John Brennan and Director of National Intelligence James Clapper released the briefs and other documents at a symposium at the Richard Nixon Presidential Library in Yorba Linda**.

Chinese cyber spies may be watching you, experts warn
CNN.com, Thom Patterson, 2016 08 24
Washington - About a year ago, **China and the United States formally agreed not to conduct or knowingly support the cyber theft of each other's intellectual property**. So, how is that agreement working out? **Not great, said Adm. Mike Rogers, head of US Cyber Command. "Cyber operations from China are still targeting and exploiting US government, defense industry, academic and private computer networks**," Rogers said last April during testimony before a US Senate committee. Cyber theft of US trade secrets can easily ruin American businesses and result in higher prices for consumers. Even more worrisome, stolen American military secrets could put US servicemen and women at risk during combat.

Police Broke Surveillance Rules After 9/11, Inquiry Finds
New York Times, Rick Rojas, Al Baker, 2016 08 24
New York - The **New York police repeatedly broke rules governing intelligence-gathering while targeting Muslims for surveillance after the terrorist attacks of Sept. 11, 2001**, according to a report issued on Tuesday. The report -- by the Office of the Inspector General for the New York Police Department, an oversight agency created in 2013 -- said that the department's Intelligence Bureau regularly let deadlines pass before asking to extend investigations into political activity, and often failed to explain the roles of undercover officers and confidential informers, as required. "The fact that deadlines were missed and rules were violated is troubling and must be rectified," the report said.

The Real Russian Mole Inside NSA (Canada)
New York Observer, John R. Schindler, 2016 08 24
Column - **Moles--that is, long-term penetration agents--are every intelligence service's worst nightmare. T**hough rarer in reality than in spy movies and novels, moles exist and can do enormous damage to a country's secrets and espionage capabilities. They're what keep counterintelligence experts awake at night. The recent appearance on the Internet of top secret hacking tools from the **National Security Agency** has shined yet another unwanted spotlight on that hard-luck agency, which has been reeling for three years from Edward Snowden's defection

to Moscow after stealing more than a million classified documents from **NSA**. As I explained, this latest debacle was not a "hack"--rather, it's a clear sign that the agency has a mole. Of course, I've been saying that for years. It's not exactly a secret that NSA has one or more Russian moles in its ranks--not counting Snowden. Now the mainstream media has taken notice and we have the "another Snowden" meme upon us. Viewing NSA as the head of the Western intelligence alliance, the core of which are the Anglosphere **"Five Eyes" countries (America, Britain, Canada, Australia, and New Zealand), and which dates to Allied victory in World War II, there was no point during the Cold War where the Five Eyes system wasn't penetrated somewhere by Soviet intelligence**. There are other indications of Russian penetration of NSA that had nothing to do with Snowden. An espionage case that got too little attention was that of **Jeffrey Delisle**, a Canadian navy junior officer who was arrested in 2012 for passing secrets to Moscow. He admitted his guilt, specifically that for almost five years beginning in 2007, he regularly sold secrets to **GRU**, that is Russian military intelligence. Upset over his wife's infidelity and short of cash, the sad-sack Delisle, who was assigned to a Canadian intelligence center in Halifax, simply downloaded secrets on a thumb-drive, which he passed to GRU every month or so. Most of what Delisle gave Moscow wasn't Canadian information but belonged to Five Eyes, much of which came from NSA. Yet the most interesting part of the Delisle case is what GRU did not want from him. Note: John Schindler is a security expert and former National Security Agency analyst and counterintelligence officer. A specialist in espionage and terrorism, he's also been a Navy officer and a War College professor.

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

UK threat to cut security ties as Calais crisis grows
London Times, Michael Savage, Charles Bremner, 2016 08 30
London - **Britain is threatening to review security co-operation with France should it try to shift the Calais border back across the Channel**. Senior government sources issued the warning after leading French politicians called for the unravelling of a 2003 deal under which British border checks take place in Calais. The agreement stops thousands of potential migrants from crossing into Britain. Amber Rudd, the home secretary, will fly to Paris today for talks with Bernard Cazeneuve, her French counterpart. Nicolas Sarkozy, one of the leading contenders to be the next French president, has said that Britain should be forced to handle on its soil the asylum claims of about 9,000 people who have gathered at the Calais camp known as the Jungle.

The secret life of 'C'
The Sunday Times, Max Hastings, 2016 08 28
Book review: **SPYMASTER The Life of Britain's Most Decorated Cold War Spy and Head of MI6,** Sir Maurice Oldfield by MARTIN PEARCE Bantam Press £20 pp400. When Alec Guinness was debating whether to accept the role of the spymaster George Smiley in the BBC adaptation of John le Carré's Tinker Tailor Soldier Spy, the author arranged for him to lunch with Maurice Oldfield, newly retired as the head of MI6. Guinness later said: "I was told he would be extremely reticent, very, very shy." In reality, he reported, he had "rarely met a more garrulous, informative, un-shy person". Many intelligence chiefs lack colour, but this could never be said of Oldfield, the dancer, church organist, global networker, yet pillar of Derbyshire farming society.A Manchester University contemporary gave a description of this renowned "C" that would not

change much until his death: "Maurice was short and fat, pale and pasty, with full lips and a mop of unruly dark auburn hair. He wore an ill-fitting dark pinstriped suit, whose collar seemed to be there for the sole purpose of catching dandruff. Visually, he put me very much in mind of the actor Charles Laughton." Martin Pearce, Oldfield's great-nephew, always regarded him with an affection that, he said, moved him to write this book because he felt no previous writer has got Oldfield quite right. That is unsurprising: in the nature of secret services, none of us, including the author, knows much about Oldfield's professional achievements. All that is for sure is that he commanded much respect among his peers in MI6 (who overcame their institutionalised snobbery to acknowledge his talents) and the politicians whom he served.

The police chief battling cybercriminals from Russia and Ukraine
The Guardian (London), Patrick Collinson, 2016 08 27
London - **Half of online fraud comes from abroad, says Ian Dyson, commissioner of the City of London police,** who has enlisted the help of Google and Microsoft to fight it. Last Christmas Ian Dyson got a call from his bank. Was he really in a Travelodge, ordering takeaway pizzas? No, was his answer, he was at home with his family. Like millions of others, Dyson had fallen victim to card fraudsters stealing from his account. But Dyson is not like everyone else - he is the commissioner of the City of London police, with the job of protecting not just London but the whole country from fraud. And the depressing reality is, like so many other frauds, the criminals got away with it. **The City of London police have a specialist officer permanently stationed in Wall Street, and worked with the Spanish police to swoop on 110 conmen operating a "boiler room" fraud targeting elderly investors. But Russia? Do the London police receive any help from their counterparts in Moscow? "No, not at all. Ukraine is limited too**. You'll be aware of the limitations of some foreign jurisdictions." Another limitation is budgets. "Policing has taken a 20% hit in its budget so I've got to do what I can with what I've got," he says, while noting that virtually everyone else in the public sector has faced similar cuts.

Return to Table of Contents/ Retour à la table des matières

Australia/ Australie

Australia unveils "how-to" guide to fight militant propaganda
Reuters, Matt Siegel, 2016 08 30
Canberra - **Australia on Tuesday released what the government says is the world's first ever how-to-guide for combating radical Islamist propaganda in Southeast Asia**, which it hopes will help disrupt local recruitment efforts by groups such as Islamic State. Australia, a staunch U.S. ally, has been on heightened alert for attacks by home-grown Islamist radicals since 2014 and authorities say they have thwarted a number of plots. The 43-page document, entitled "**Undermining Violent Extremist Narratives in South East Asia**", will be accessible online and aims to provide tools to disrupt the winding path to radicalisation, said Justice Minister Michael Keenan. "The process of radicalisation to violence is an incredibly complex issue. Terrorist propaganda affects each individual's state of mind, their thoughts and emotions differently. There is no single pathway to radicalisation," Keenan told a conference in Canberra, according to an advanced copy of his remarks shared with Reuters.

Secret security review: special forces to get call if terrorists strike at home
The Australian, Paul Maley, 2016 08 29

Canberra - **Army special forces could be called out to resolve deadly Lindt cafe-style sieges as part of a wideranging secret review aimed at streamlining the so-called "call-out" powers that allow the military to operate on domestic soil**. Almost two years after Lindt cafe gunman Man Haron Monis brought Sydney's CBD to a standstill, resulting in the deaths of two hostages and raising serious questions about the ability of local police to handle major terrorist attacks, The Australian can reveal moves are afoot to fast-track the procedures via which the army can be used to fight terrorists. The Australian understands the Defence Department has initiated a nationwide review of the call-out powers, widely considered archaic and ill-suited to the fast-moving pace of modern terrorism. The review is part of a more - aggressive approach to counter- terrorism strategy, spurred by the Lindt cafe siege as well as last year's shooting attacks in Paris and Brussels, which were carried out by Islamic State terrorists intent on killing as many people as quickly as possible. Taken together, the attacks have rendered much of the thinking around responding to terrorism redundant, in particular the so-called "contain and negotiate" strategy favoured by police. Instead, specialist police are being retrained to engage terrorists quickly and with deadly force.

Government computer networks breached in cyber attacks as experts warn of espionage threat
ABC (Australia), Linton Besser & Jake Sturmer, 2016 08 29
Canberra- **Sensitive Australian Government and corporate computer networks -- including those holding highly confidential plans for a privately financed geostationary communications satellite -- have been penetrated by sophisticated cyber attacks**, a Four Corners investigation has established. **Austrade and the Defence Department's elite research division, now named the Defence Science Technology Group, both suffered significant cyber infiltrations in the past five years by hackers based in China**. Intelligence sources say they suspect the attackers in these cases were sponsored by Beijing. Four Corners has also confirmed Newsat Ltd, an Australian satellite company whose assets were sold off last year after the company went into administration, was so comprehensively infiltrated three years ago that its entire network had to be rebuilt in secret. But these incidents, revealed for the first time, are only a fraction of the cyber attacks being waged against Australian governments and companies. The **Prime Minister's cyber security adviser, Alastair MacGibbon, told the program the Australian Government was "attacked on a daily basis".** "We don't talk about all the breaches that occur," he said. Government and industry sources said the true targets for the cyber attack may have been defence assets linked to the BoM and its vast data-collection capabilities. **One was the Australian Geospatial-Intelligence Organisation, an intelligence agency within the Department of Defence** which provides highly detailed mapping information for military and espionage purposes.

ASIO push to 'streamline' judicial safeguards criticised by legal groups
Australian Broadcasting Corporation, Francis Keany, 2016 08 27
Canberra - A **push by domestic intelligence agency ASIO to reduce the level of judicial safeguards in terrorism investigations has been criticised by a peak legal group.** Special warrants currently allow ASIO to question and detain people for up to a week without charge. Under the proposal only the Attorney-General, and not a judge, would be needed to issue those warrants. **Director General of ASIO Duncan Lewis** told an inquiry into the Government's detention powers his agency would support amendments that made the current process "more efficient and effective". "ASIO has made a number of recommendations in our submissions to this review on how the current authorisation process could be streamlined for our questioning powers," he said. "This would make them more efficient in responding to the current fast paced threat environment." **Law Council of Australia director Arthur Moses said the move could set a dangerous precedent and politicise investigations**. "Ministers can and do get things

horribly wrong in the heat of the moment as they straddle a number of competing issues including how their decisions may be received by the press or how it may be politically detrimental to the government," Mr Moses said.

ASIO seeks detention without a judge's warrant
Sydney Morning Herald, David Wroe, 2016 08 27
Canberra- **ASIO has proposed scrapping the need for judge-approved warrants to detain and question Australians for up to a week without charge in terrorism investigations**, a watering down of safeguards that has alarmed lawyers and rights advocates. The power to grant the security agency a controversial "questioning and detention warrant" would rest instead with the Attorney-General, a situation the **Law Council of Australia** has branded "unprecedented". The changes requested by ASIO would also remove a separate requirement that an independent legal authority such as a retired judge be present when a person was being questioned. Rather, oversight of questioning would rest with the intelligence watchdog, the Inspector-General of Intelligence and Security. Under laws passed after the September 11 and Bali bombing attacks, ASIO has the power to hold someone for up to seven days and question them during a terrorism investigation. **ASIO head Duncan Lewis** told a review inquiry last week into the laws that the process could be "more efficient and effective". Mr Lewis told the hearing these powers were "fundamental to ASIO's work in responding to the terrorism threat that we face". Police and intelligence agencies say terrorism plots in the Islamic State era are increasingly rudimentary and fast-moving, which means processes such as obtaining warrants need to be streamlined as much as possible.

Return to Table of Contents/ Retour à la table des matières

New Zealand/Nouvelle-Zélande

Megaupload's Dotcom argues extradition appeal should be livestreamed
Reuters, 2016 08 30
Wellington— An **appeal by flamboyant German tech entrepreneur Kim Dotcom over a decision to extradite him to the United States began in New Zealand on Monday**, with the Megaupload founder's legal team arguing the hearing should be livestreamed on YouTube. The High Court hearing opened in Auckland nine months after a lower court ruled Dotcom could be sent to the United States to face copyright infringement and money-laundering charges over the operation of file-sharing website Megaupload. U.S. authorities say Dotcom and three co-accused Megaupload executives cost film studios and record companies more than $500 million and generated more than $175 million by encouraging paying users to store and share copyrighted material, such as movies and TV shows. Years of legal wrangling followed Dotcom's arrest in New Zealand police raid in 2012, and it **emerged that the Government Communications Security Bureau had illegally spied on him before the raid.**

Return to Table of Contents/ Retour à la table des matières

International

China/Chine

First counter-terror fines issued to hotels ahead of G20 summit
Global News, Staff reporter, 2016 08 30
Beijing - A **hotel in Nanjing, East China's Jiangsu Province - which neighbors the G20 host city - was fined by police for failing to register its guests' personal information accurately, becoming the first business in Nanjing to face such punishment since China's Counter-terrorism Law took effect in January**. During an inspection of the hotel on August 10, police found that personal information of guests in one room was not registered properly and instructed the hotel to rectify the problem, the Yangtze Evening Post reported Monday. However, the hotel had not registered travelers' information for another four rooms when police returned on Wednesday.

China's Covert Weapons Procurement Revealed in Florida Case
Washington Free Beacon, Bill Gertz, 2016 08 24
Washington - **China's government covertly tried to obtain advanced U.S. fighter jet engines and a Reaper drone** in a high-technology spying operation uncovered by federal authorities in Florida. A Chinese-born woman, **Wenxia Man**, was sentenced to 50 months in prison on Friday following her conviction for conspiracy to export restricted American defense articles, namely engines for F-35, F-22, and F-16 jets, and the Reaper, a front-line unmanned aerial vehicle used by the military and intelligence agencies. Court papers in the case stated that Man, a naturalized U.S. citizen residing in California who is also known as Wency Man, worked with a Chinese government procurement agent, Xinsheng Zhang, in trying to purchase the military items. The **Chinese planned to reverse-engineer the U.S. military goods to avoid the costs and time required for indigenous development**.

Anti-graft body: no relief for fugitives overseas (Canada)
China Daily, Zhang Yi, 2016 08 24
Beijing - **One-third of the people listed by Interpol as China's 100 most-wanted corrupt officials and businesspeople have returned to the country to face justice and atone for their crimes.** Zhang Yi reports. "I feel ashamed of what I did, stealing public funds and fleeing to Singapore to avoid jail time in China. I don't deserve to be a Chinese citizen. I realize there is no point living a miserable life in a foreign country, because the rest of my days would be a mere existence on earth." Those words, from a confessional letter written by **Li Huabo, No 2 on a list of arrest warrants for China's 100 most-wanted economic fugitives published by Interpol** last year, were made public for the first time at the weekend. Li returned to China in May last year, after serving 15 months in a Singaporean jail for depositing stolen money in bank accounts in the island state. The 55-year-old former official at the finance bureau in Poyang county, Jiangxi province, is suspected of embezzling 94 million yuan ($14 million) in government funds. In the confession, he said he felt relieved when he agreed to return to China and turn himself in. He is just one of 33 people on the Interpol list who have returned to China to face the music. Thanks to a global dragnet, the country's most-wanted economic fugitives are discovering that they can run, but in the end, they will be brought to justice. Last year, the CCDI started "Skynet", a program to coordinate efforts to bring errant fugitives to justice. "Suspected government officials and crooked businesspeople in the private sector are on the Interpol list. Those **who worked for State-run departments or enterprises have chosen to hide in**

economically advanced countries, such as the US, Canada and New Zealand, because they can access a favorable living environment and a well-rounded legal system which they believe will favor their interests," said Huang Feng, a professor of international criminal law at Beijing Normal University.

Return to Table of Contents/ Retour à la table des matières

Russia/Russie

Des « privés » russes engagés sur le front syrien
Le Figaro, Pierre Avril, 2016 08 29
Moscou-Le nom du musicien romantique allemand qui lui est accolé ne doit pas faire illusion. Le **« groupe Wagner »** est devenu le centre d'attention de la communauté militaire russe depuis la publication, le 25 août, par le journal RBK d'une longue enquête consacrée aux compagnies militaires privées opérant en Syrie**. Sous ce pseudonyme artistique se cacherait Dmitri Outkin, un ancien officier des renseignements militaires russes (GRU) qui aurait donné son nom à ce qu'il convient d'appeler une compagnie de mercenaires, à l'image des Blackwater et KBR**, ces fameux « chiens de guerre » américains ayant combattu en Irak. Selon une source interrogée par RBK , près de 1 600 employés du groupe Wagner auraient déjà simultanément servi en Syrie en 2016, leur nombre variant au gré des combats, pour un salaire plafonnant à environ 300 000 roubles mensuels (4 100 euros). Plusieurs d'entre eux se seraient distingués lors de la libération de Palmyre, alors contrôlée par l'État islamique. Depuis 2015, ils disposeraient d'une base militaire destinée à leur préparation, située à Molkino dans la région de Krasnodar (Sud) et placée sous le contrôle du GRU. Dmitri Outkin lui-même aurait déjà servi au Proche-Orient sous les ordres d'une compagnie russe baptisée

Russia Says Chinese Hackers Are Getting More Aggressive
Bloomberg News, Stepan Kravchenko, 2016 08 26
Moscow - **While the West sees Russia as a cyber predator, hackers in the East increasingly view it as prey, according to online security company Kaspersky** Lab, which says there's been a sharp spike in attacks from China. Cases of Chinese hacking of Russian industries including defense, nuclear, and aviation rose almost threefold to 194 in the first seven months of this year from 72 in the whole of 2015, according to Alexander Gostev, the Moscow-based company's chief security expert. **Proofpoint**, a California- based cyber security company, also reported an increase in Chinese attacks on Russia. The hacking is going on "despite the officially promoted friendship between **Russia and China and accords on cyber security, cooperation and non-aggression" between the two governments**, Gostev said in an interview. "I don't see them working."

Why are Russian hackers going after US news organizations?
Christian Science Monitor, Ben Rosen, 2016 08 24
Boston - **Hackers linked to Russian government agencies targeted The New York Times this month in an apparent effort to extract intelligence about US political system**, CNN first reported Tuesday. The FBI has started an investigation into the attempted breach of the Times and other US news organizations. But, Eileen Murphy, a spokeswoman for the newspaper, said Tuesday the hackers were not successful. "This is what cyber conflict actually looks like," James Lewis, a senior fellow at the **Center for Strategic and International Studies**

(CSIS), a Washington think tank, told The Christian Science Monitor earlier this month. "The problem in the US is we're very militarized, so we tend to think about attacking infrastructure. The Russian approach is much more political and about trying to manipulate public opinion." The spotlight the leak has thrown on Russia - warranted or not - underscores how different countries have different targets with their spying. Russia comes under suspicion partly because the DNC case reflects the Kremlin's global campaign to influence political outcomes - as opposed to say, **China's focus on hacking as an economic tool."China is all about its global rise based on its economy, and we can see that fixation in the cases we've seen"** of hacking into corporations and focusing efforts on accessing corporations' intellectual property, says Fiona Hill, director of the Brookings Institution's Center on the US and Europe.Russia's cyber focus has evolved."The Russians at one point a number of years ago were also focused on their economic aspirations," she adds, "but now they're back to the old political space and are very much working from the playbill of the **KGB** in the cold war days."

FBI investigating Russian hack of New York Times reporters, others
CNN.com, Evan Perez, Shimon Prokupecz, 2016 08 24
Washington - **Hackers thought to be working for Russian intelligence have carried out a series of cyber breaches targeting reporters at The New York Times and other US news organizations,** according to US officials briefed on the matter. The intrusions, detected in recent months, are under investigation by the FBI and other US security agencies. Investigators so far believe that Russian intelligence is likely behind the attacks and that Russian hackers are targeting news organizations as part of a broader series of hacks that also have focused on Democratic Party organizations, the officials said. The Times said email services for employees are outsourced to Google. CNN requested comment from Google but didn't receive comment. The FBI declined to comment. Times spokeswoman Eileen Murphy said the company had seen "no evidence" that any breaches had occurred of the Times's internal systems. CNN's report didn't say that the Times internal systems were breached, but that reporters were targeted.

New York Times's Moscow Bureau Was Targeted by Hackers
New York Times, Nicole Perlroth, David E. Sanger, 2016 08 24
New York - The N**ew York Times's Moscow bureau was the target of an attempted cyberattack this month.** But so far, **there is no evidence that the hackers, believed to be Russian, were successful.** "We are constantly monitoring our systems with the latest available intelligence and tools," said Eileen Murphy, a spokeswoman for The Times. "We have seen no evidence that any of our internal systems, including our systems in the Moscow bureau, have been breached or compromised." On Tuesday, citing United States officials briefed on the matter, CNN reported that The Times, along with other news organizations it did not identify, had been the victims of computer breaches by hackers thought to be working for Russian intelligence. The **Federal Bureau of Investigation** is looking into the attempted attack on The Times, a government official briefed on the inquiry said, but has no investigations underway of such episodes at other news organizations.

Return to Table of Contents/ Retour à la table des matières

Europe

Italy expels Russian accused of inept bid to buy Nato secrets
London Times, Tom Kington and Deborah Haynes, 2016 08 30

London— **Italy has handed a suspected Russian spy back to Moscow two months after he was allegedly caught buying Nato secrets from a Portuguese agent.** European security sources said that the detention of **Sergei Pozdnyakov** would have embarrassed and enraged Moscow at a time of tension between Russia and the West. *"This was a counter-intelligence coup for the Italians and the Portuguese,"* one source said.Court documents suggest that the Russian had already got his hands on Nato secrets from the same alleged agent. Mr Pozdnyakov, suspected of **being a senior member of Russia's Foreign Intelligence Service**, had allegedly travelled to Italy without obtaining diplomatic immunity — a basic error of tradecraft. Paying an official for secret information is illegal, although unspoken diplomatic rules usually mean that a foreign intelligence officer caught running agents is expelled within 48 hours. On this occasion the Russian was freed only last month, without fanfare, after eight weeks behind bars. His alleged occupation was never proved and the Russian embassy described him as a diplomat.

Germany's Spy Agency Offers Rare Glimpse Inside Its New Gates
Wall Street Journal, Zeke Turner, 2016 08 29
Berlin - **Germany's top-secret spy service, the Federal Intelligence Agency, invited the public this weekend for the first--and only--time to visit inside the gates of its new billion-euro campus in the center of Berlin**. The **Bundesnachrichtendienst--or the BND for short, Germany's answer to the Central Intelligence Agency--is marking its 60th anniversary**, and next year will leave its reclusive headquarters in a Munich suburb for its new Berlin office. It is the biggest, and one of the most expensive, buildings the postwar German government has ever built. An advanced group of 170 workers are already on site, BND officials said. Many of them are setting up computer networks and phones for the rest of the agency's 4,000 workers, who will move to Berlin next year. At that point, it will be impossible to visit inside the agency's gates. The move into prominent, centrally located new headquarters comes as Germany is putting evermore emphasis on its spy operations. Last week, **Chancellor Angela Merkel said that gathering and sharing intelligence was among the most important things European Union countries could do to justify the bloc's existence.** Faced with fears of another imminent terror attack on German soil,

« La loi sur le renseignement est liberticide »
Le Temps, Bernard Wuthrich, 2016 08 29
Berne-- **Conseiller national durant 24 ans, cofondateur du GSsA, le socialiste Andreas Gross a tourné la page de la politique**. Mais il **s'engage résolument contre la nouvelle loi sur les services secrets, qu'il considère comme « trop vague » et inefficace.** Avant de quitter le Conseil national, où il a siégé de 1991 à 2015, Andreas Gross (PS/ZH) a encore eu le temps de **voter contre la loi sur le renseignement (LRens).** Cet ancien fiché y voit un danger pour les citoyens. Que reprochez-vous à la LRens? Cette loi exprime une mentalité de soupçon envers les citoyens. Elle met la protection de l'Etat au centre, pas celle de la liberté individuelle. La preuve? Dans son message, le Conseil fédéral dit que les droits des citoyens sont « pris en compte », ce qui signifie qu'ils ne sont pas la préoccupation première de la LRens. La loi permet de s'introduire dans la sphère privée des gens: lire le courrier postal, écouter les discussions téléphoniques, s'infiltrer dans les ordinateurs.

«Ne rien faire, c'est indirectement se rendre complice d'un attentat»
Le Matin Dimanche (Suisse), Philippe Castella et Fabian Muhieddine, 2016 08 28
Berne--**Guy Parmelin défend son premier objet devant le peuple dans un mois, un renforcement de la loi sur le renseignement, dans un contexte marqué par la multiplication des attentats terroristes.** Interview. **Avez-vous peur d'un attentat terroriste en Suisse? Peur, ce n'est peut-être pas le mot, mais nous devons nous préparer à toutes**

les éventualités. Avant même les attentats de cet été, toutes les analyses parlaient déjà de menace élevée. Nous continuons à mener ces évaluations. Le risque d'attentat a même augmenté. Vous êtes-vous déjà retrouvé au milieu d'une fête populaire avec des images d'attentat vous venant à l'esprit? Pas à titre personnel, mais j'ai rencontré des gens qui m'ont clairement dit qu'ils avaient renoncé à tel ou tel événement, où ils se rendaient régulièrement avec leurs enfants....Les menaces se sont diversifiées, c'est juste. Elles n'émanent plus seulement de groupes structurés avec une stratégie et un but bien déterminés. Il faut s'y adapter avec de nouveaux instruments et des collaborations internationales pour anticiper les situations. Mais, avec nos moyens, nous resterons dépendants des services secrets étrangers. C'est presque toujours eux qui nous avertissent, comme dans l'affaire d'espionnage de RUAG. C'est un échange**. Nos services de renseignement donnent aussi des informations aux autres pays.** En Suisse, nous cherchons à adapter nos instruments à l'évolution en matière de terrorisme et de cyberattaques. Mais nous voulons le faire de manière proportionnée, avec un rapport coût- efficacité adéquat.

Ecoutons les agents de terrain dans la lutte contre le terrorisme!
Le Monde, Isaac Getz avec Erwin Van Waeleghem, 2016 08 26
Non identifié - **Nos agents de liaison, en contact direct avec la menace terroriste, sont très efficaces pour collecter des données, mener des enquêtes préventives et partager les informations**. Las, **ils sont trop rarement entendus par leur hiérarchie** Il est trop tôt pour tirer les leçons des déficiences des services de sécurité concernant les attaques terroristes de 2015-2016 en Europe. Il en va autrement des attentats de 2001 aux Etats- Unis. Examiner ces manquements, autant que les meilleures pratiques organisationnelles de centaines de structures, nous fournit des leçons uniques sur la façon d'améliorer nos services pour mieux combattre le terrorisme. Devinez où a été écrite cette note de service d'une salariée destinée à son directeur : " Les agents sur le terrain et leur manageur de proximité seraient mieux à même de mettre en place des solutions rapides et efficaces (...) pour prévenir des (...) risques. Bien que le personnel du siège ait (...) été d'une aide incommensurable (...) , j'ai beaucoup de mal à penser à des cas résolus par eux et je peux en nommer plusieurs qu'ils ont " foirés " ! La prise de décision est intrinsèquement plus efficace et plus rapide quand elle est décentralisée plutôt que concentrée. " Les **dysfonctionnements du FBI Vous pourriez penser que c'est une salariée d'une grande entreprise qui en est l'auteure, mais il s'agit en fait de Coleen M. Rowley, agent du FBI à Minneapolis.** Elle a exposé des -dysfonctionnements du FBI, lesquels, s'ils avaient été traités plus tôt, auraient pu prévenir les attentats du 11 septembre 2001. Voici un exemple de sa propre expérience : " Les agents à Minneapolis - étant - (...) dans la meilleure position afin d'évaluer la situation sur place, - ils - ont pleinement pris conscience du risque terroriste posé par Moussaoui et ses possibles co-conspirateurs, même avant le 11-Septembre. (...) Cependant, l'agent spécial de surveillance au siège du FBI (...) semble avoir constamment, presque délibérément, contrecarré les efforts des agents du FBI de Minneapolis. " Rowley cite aussi l'expérience de Kenneth Williams, un agent du FBI pour l'antiterrorisme à Phoenix qui a envoyé une note de service au siège le 10 juillet 2001. Elle s'ouvrait par la mise en garde contre les plans de Ben Laden d'envoyer des étudiants aux Etats-Unis pour apprendre à piloter. Williams n'a jamais reçu de réponse réelle. Des dysfonctionnements similaires existent en Europe. En **Belgique, par exemple, le chef d'une police locale n'a pas partagé avec les services antiterroristes à Bruxelles l'information de son agent de terrain sur le locataire de l'éventuelle planque du terroriste belge Abdeslam**. Après quatre mois, grâce à un témoignage spontané, Abdeslam sera arrêté précisément dans ce lieu. Quant à l'agent en question, il a fini en burn-out ...

Turkey accused of 'systematic spying' in Austria
The Local (Austria), Staff report, 2016 08 25

Vienna - An **Austrian politician has accused Turkish authorities of spying on people living in Austria who are opposed to the Turkish leader President Tayyip Erdogan**. It follows similar accusations made in recent days in Germany and the Netherlands regarding possible networks of thousands of Turkish spies in Europe. The security spokesperson for Austria's Green party, Peter Pilz, announced on Wednesday that "systematic spying" is being carried out of people living in Austria who are against the Turkish government. Pilz claims information about opposition supporters is being gathered by organisations affiliated with the AKP, the ruling party in Turkey formerly led by Erdogan before he became president.

Youth novel explores real causes of terror in Germany
Deutsche Welle, 2016 08 25
Berlin-- A **German-Turkish teen joins the 'IS' and plans a terror attack in Germany. While that's the basis for a new work of youth fiction, it's disturbingly close to the reality in Germany**, writes DW's Rolf Rische. "Allahu akbar!" shouts the 16-year-old in front of the St. Paul soccer stadium in Hamburg. He's about to blast himself and hundreds of innocent people to bits. The young man is a native German, a soccer fan and, as of recently, a religiously motivated terrorist. The scene is both frightening and absurd at the same time. But tragically, it's also all too reminiscent of things that have really happened in Germany this past year. The novel "Kadir, der Krieg und die Katze des Propheten" (Kadir, the War and the Prophet's Cat), **by Peter Mathews und Benno Köpfer,** opens with this scene. The book traces the path of German-Turkish youth Kadir from an inconspicuously, relatively well adjusted teenager to a jihadist. What Kadir experiences and how he is treated corresponds to reality, according to the book's authors. **Benno Köpfer has worked for many years as an analyst for the Federal Office for the Protection of the Constitution**. His mission is to fight Islamist terrorism. Köpfer studied Muslim Studies in Freiburg, Cairo and Sana'a. As an archaeologist, he participated in excavations in Yemen and Syria and has traveled the Islamic world from Mauretius to Pakistan. Köpfer **aims to help his colleagues at the Federal Office for the Protection of the Constitution understand what leads young men in Germany to become terrorists**. "Islam as a religion is only part of what draws young people into the jihad for the 'IS,'" he says.

Le cryptage des messageries, casse-tête de Cazeneuve
Le Figaro, Lucie Ronfaut, 2016 08 24
Bruxeles - Le **chiffrement des communications n'a pas fini d'embarrasser les autorités. Bernard Cazeneuve, ministre de l'Intérieur, et son homologue allemand Thomas de Maizière souhaitent proposer à la Commission européenne une loi soumettant les services de messagerie en ligne aux mêmes obligations que les opérateurs télécoms**, afin de les forcer à collaborer dans le cadre d'enquêtes antiterroristes. L'idée n'est pas neuve. La semaine passée, l'agence Reuters affirmait que la Commission européenne voulait étendre aux applications de messagerie les règles de sécurité et de confidentialité appliquées aux opérateurs télécoms. En **France, ces derniers doivent permettre l'interception des données de leurs utilisateurs dans le cadre d'enquêtes judiciaires ou sur demande des services de renseignement.** Dans cette lignée, Cazeneuve a affirmé mardi vouloir obliger les services en ligne « non coopératifs » à « retirer des contenus illicites ou déchiffrer des messages dans le cadre d'enquêtes judiciaires, que leur siège soit en Europe ou non » .

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

CIA declassified intel files reveal briefings on Israel
Jerusalem Post, Staff Report, 2016 08 26
Jerusalem - The **day before the Yom Kippur War broke** out on October 6, 1973, **US intelligence assessments reported large-scale military exercises in Egypt,** but that "they do not appear to be preparations for an offensive against Israel." The **assessment was found in one of about 2,500 documents released by the CIA on Wednesday, containing the US government's intelligence analysis on key national security issues** during the presidencies of Richard Nixon and Gerald Ford, from January 1969 to January 1977. The release took place at an event at the Nixon Presidential Library & Museum in Yorba Linda, California. Another document from the day the war began said that neither side seemed inclined to start hostilities.

Minister says overseas intelligence agencies try to make Iran insecure
Iranian Young Journalists' Club website, via BBC Monitoring Middle East, 2016 08 25
Tehran— **Iran's Intelligence Minister Mahmoud Alavi has US, UK, Israeli and Saudi intelligence services are funding groups who aim to make the country** insecure. According to the **semi-official Young Journalists' Club** (YJC), which is run and funded by the country's state broadcaster, Alavi said: "Behind all of this we see evidence proving coordination between intelligence services of hostile countries, with **US, UK and Saudi intelligence and the Mossad at the helm.** "We find their traces in the southeast and beyond our borders. They form teams of 10 to 12 people and spend 500,000 dollars on every operation to challenge the safety and security of our country."

Iran's Revolutionary Guard targets 450 social media users
Associated Press, 2016 08 24
Tehran - The **cyber-arm of Iran's powerful Revolutionary Guard says it has summoned, detained and warned some 450 administrators of social media groups in recent weeks**. The announcement Tuesday, carried on a website affiliated with the Guard's cyber arm, says those detained used social media like the messaging app Telegram, which is popular in Iran. The announcement says those detained or summoned made posts that were considered immoral, were related to modeling, or which insulted religious beliefs. It says the Guard only took action after "judicial procedures" were completed, without elaborating. In May, authorities announced an operation targeting those involved in modeling on Instagram.

Return to Table of Contents/ Retour à la table des matières

Asia/Asie

S. Korean Embassy in China warns against possible N. Korea terror attacks, abduction
Yonhap News Agency, Staff reporter, 2016 08 29
Seoul - The **South Korean Embassy in Beijing has warned South Koreans in China about possible terrorist attacks or abduction attempts by North Korea in the wake of the recent defection of a senior diplomat**, sources said Monday. The embassy urged South Korean residents and travelers in China to refrain from visiting the North Korea-China border areas or coming in contact with North Koreans in a message recently conveyed to South Korean expatriate groups and other associated organizations in China, according to the sources. "Given

the recent defection of a high-level North Korean official and North Korea's threats of provocations, there seem to be high possibilities of terrorist attacks and abductions of our citizens," the embassy message said. "South Koreans are advised to pay special attention to their personal safety," it said. South Koreans in China are also advised to abstain from trips to the border areas and meeting with any suspected North Koreans, the message also said, urging them to constantly check safety information updates from the embassy.

Japan gov't to submit revised conspiracy bill citing terrorist threat
Kyodo News, Staff reporter, 2016 08 26
Tokyo - **The Japanese government plans to submit a revised bill criminalizing conspiracy to the Diet in September to strengthen counterterrorism measures before Tokyo hosts the 2020 Summer Olympics**, sources close to the matter said Friday. Earlier versions of the bill have been submitted three times but all were scrapped due to concerns over intrusive state surveillance and the granting of arbitrary powers to investigators as the act of conspiracy would be a punishable offence even when a crime is not committed. **Senior lawmakers of the ruling Liberal Democratic Party led by Prime Minister Shinzo Abe have stepped up calls for the introduction of a conspiracy charge in the wake of the deadly terror attacks in Paris** last November. "It is an important responsibility of the government to secure the public's safety," Chief Cabinet Secretary Yoshihide Suga told a press conference, commenting on the need for the legislation. In the new bill targeting organized crime, the government plans to specify that to face the charge, individuals must have been involved not only in conspiring to commit a crime but also in preparatory acts such as fundraising, they said.

N.K. resumes encrypted numbers broadcast after 2-week hiatus
Yonhap News Agency, Staff reporter, 2016 08 26
Seoul - **North Korea's state radio station on Friday resumed the broadcast of mysterious numbers after a two-week hiatus, which some experts say are coded messages to its agents in South Korea**. A female announcer at Radio Pyongyang read numbers for more than four minutes starting at 12:45 a.m., calling out numbers, such as "No. 68 on Page 509." The announcer said she is "giving review works in basic information technology lessons of the remote education university for No. 27 expedition agents." Since June, North Korea has now carried out encrypted numbers broadcasts five times. Broadcasts of mysterious numbers were used by North Korea to give missions to spies operating in South Korea during the Cold War era. **Spies could decode numbers to get orders by using a reference book.**

North Korea Unveils Netflix-Like Service With Propaganda on Demand
New York Times, Patrick Boehler, Choe Sang-Hun, 2016 08 26
Hong Kong - Days before North Korea's leader, **Kim Jong-un**, successfully tested a ballistic missile that he said could hit parts of the continental United States, his reclusive regime unveiled another technical triumph: a **Netflix-like streaming service. Called Manbang, the service delivers on-demand videos to televisions through a set-top box**, Korean Central Television said in a report last week. In the report, a narrator says that Manbang is further proof of North Korea's "socialist cultural power," which will allow its people to watch their country "make a leap forward every day, every hour." Very few of the country's roughly 25 million citizens are permitted access to the actual internet. Content that can be streamed is largely restricted to state-run television and propaganda-filled movies.

No 'technical traces' about varsity attack found, Kabul told
Dawn (Pakistan), 2016 08 26
Islamabad— Pakistan informed the Afghan government on Thursday that **no "technical traces" of telephonic contacts between the Kabul university attackers** and people on its

side of the border could be found, and sought more evidence. This was conveyed during a telephonic conversation between Afghan President Ashraf Ghani and Army Chief Gen Raheel Sharif, according to a security source. **Pakistani intelligence agencies are, however, continuing with the evaluation of the intelligence shared by Afghanistan after the attack. Absence of an operational intelligence-sharing mechanism between the two countries makes such cooperation between the two countries complicated**. There have been several attempts to establish intelligence sharing arrangement, but all efforts have been unsuccessful because of Afghan intelligence agency NDS' opposition to it. Pakistani intelligence agency ISI and NDS last year signed a cooperation agreement, but it was scuttled by the Afghan side.

Japan, Australia agree to beef up security ties amid China's rise
Kyodo News, Staff reporter, 2016 08 25
Tokyo - The **Japanese and Australian defense ministers agreed Thursday to strengthen security cooperation** amid China's growing maritime assertiveness and North Korea's repeated ballistic missile launches, including one fired the previous day. "I have been clearly instructed by Prime Minister Shinzo Abe to promote defense cooperation between Japan and Australia. I would like to deepen the relationship," Defense Minister Tomomi Inada said at the outset of the talks with her Australian counterpart Marise Payne in Tokyo. Payne also noted the importance of the two countries' cooperation for regional peace and safety amid growing security challenges.

Terror intelligence unit to double number of staff
Japan News, Hirotaka Fukaya, 2016 08 25
Tokyo - The **government plans to double the number of officials assigned to the Counterterrorism Unit-Japan (CTU-J) to improve its ability to collect and analyze information**, sources said. The staff increase, which could occur this year, would increase the unit's personnel to about 40 people. Also, the number of officials stationed overseas, who are not part of the unit, will be increased from about 20 to about 40. In total, about 80 officials at home and abroad will be in charge of information-gathering. **One objective is to bolster the nation's ability to prevent terrorist attacks during the 2020 Tokyo Olympics and Paralympics**. The unit was created in December after incidents including the simultaneous attacks in Paris the month before. Organizationally, it is part of the Foreign Ministry. Its original staff of about 20 officials were from the Defense Ministry, the National Police Agency, and other related ministries and agencies. All the unit's members are concurrently posted to the Cabinet Secretariat, which essentially puts it directly under the prime minister and chief cabinet secretary.

N. Korea dispatches defector kidnapping agents to China
Dong-A Ilbo Daily, Staff reporter, 2016 08 24
Beijing - **Following defection to South Korea of 13 employees at a North Korean state-run restaurant in China and Thae Yong Ho, a top North Korean diplomat at the embassy in London, North Korea has pledged revenge and has massively dispatched members of national security department and North Korea's Reconnaissance General Bureau to China** to strengthen supervision of North Korea-China borders. These North Korean officials are staying in major Chinese airports to monitor any movements of defections. "North Korean officials monitor at the exit at Shenyang Airport in Liaoning when a plane arrives from South Korea," a North Korea source said Tuesday. "They are special agents dispatched from North Korea to kidnap defectors visiting China after the defection of 13 waitresses.

Another Japanese indicted over spying allegations in China
Kyodo News, Staff reporter, 2016 08 24

Beijing - **One of four Japanese who were arrested by Chinese authorities from last year to early this year over alleged involvement in spying activities has been indicted, sources privy to Sino-Japan relations** said Tuesday. The man from Kanagawa Prefecture was detained in May last year in Liaoning Province, close to China's border with North Korea. He is the third of the four known to have been indicted. It is not clear what the charges against him were or at which court he will stand trial. A former defector from North Korea, the man could have been indicted for dealing with sensitive North Korea-related information. Chinese authorities took the four into custody separately from May to June last year over the alleged involvement in spying. China said last month that another Japanese man is under investigation on suspicion of "endangering China's national security."

Return to Table of Contents/ Retour à la table des matières

Africa/Afrique

Somali intelligence said proactive following appointment of new chief
Somali Shabelle Media Network, via BBC Monitoring Africa, 2016 08 30
Mogadishu— **Appointment of General Abdullahi Gafow Mahmud as the Director of the Somali National Intelligence Agency has made a difference to security in Mogadishu** which has been stepped up. The appointment of the new director of the Somali National Intelligence has helped address issues of insecurity in Mogadishu with security forces foiling a number of suicide attacks which al-Shabab has been planning to carry out in the capital. **The new leadership at the national intelligence agency** has put in place measures to detect vehicles being used in attacks and safely removed explosives before they were used to cause harm.

Mandelas want answers about CIA's involvement
New Age (South Africa), 2016 08 29
Midrand, South Africa— **The Mandela family has upped the ante in demanding answers from the American government regarding the involvement of the country's intelligence agency in the arrest of Nelson Mandela in 1962**. Inkosi Mandla Mandela, Nelson Mandela's grandson who is also the chief of Mvezo, yesterday urged the Americans to shed more light regarding their involvement. This comes after a retired CIA officer, Donald Rickard, who was based in Durban at that time, publicly said they helped the apartheid government to arrest Madiba because they viewed him as "the world's most dangerous communist". This is according to a report published by the Washington Post earlier this year.

Return to Table of Contents/ Retour à la table des matières

Americas/Amériques

Venezuela accuses US, opposition of planning coup
Buenos Aires Herald, 2016 08 30
Caracas— Venezuela once again accused the United States and the country's political opposition of planning a coup, alleging that this Thursday — the day that government opponents have called for a march to demand a recall vote against President Nicolás Maduro — has been

pencilled in. The Foreign Ministry's North America agency issued a statement yesterday protesting US State Department spokesman John Kirby's call for the release of the jailed former mayor of San Cristóbal, **Daniel Ceballos, who was taken from his home early Saturday by state intelligence agents** and moved back to prison in central Guárico state. He had been under house arrest.

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

31-08-2016 to/au 06-09-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

New DND facility falls short on security
Globe and Mail, Robert Fife, 2016 09 02
Ottawa - The **new $1-billion headquarters of the Department of National Defence is not secure enough to house top-secret intelligence work and sensitive military operations** because the facility at the old Nortel campus does not meet the exacting security standards of Canada's international intelligence allies. After years of delay, the first wave of 3,400 military and civilian employees will begin the move into the 10- building complex in an Ottawa suburb in November. DND will eventually transfer 8,500 employees to the 148-hectare site by 2020. Despite extensive work on the complex, including clearing it of listening devices planted by corporate spies in its Nortel days, the new headquarters falls short of the rigorous security requirements of Canada's Five Eyes intelligence partners: the United States, Britain, Australia and New Zealand. "The **bottom line is that we made a decision that we are not going to spend the money** to replicate the physical infrastructure and the information systems and all the other technologies that are required to support intelligence and operations," **ViceAdmiral Mark Norman, the vicechief of the defence staff in charge of overseeing the relocation**, told The Globe and Mail. Canada's cyberspy agency, the **Communications Security Establishment**, met those standards when it recently moved into a new $1.2-billion headquarters in Ottawa.

La GRC veut contrer une éventuelle attaque par drone contre Trudeau
Radio-Canada Nouvelles, Bahador Zabihiyan, 2016 09 01
Montréal--La **GRC craint que des individus mal intentionnés se servent d'un drone pour s'en prendre aux personnalités publiques, à commencer par Justin Trudeau**. Les policiers fédéraux se penchent ainsi sur des solutions pour contrer de telles attaques, a appris Radio-Canada. Les drones, ces appareils volants qui peuvent être télécommandés, sont de plus en plus populaires dans de nombreux secteurs. Faciles à manipuler, certains de ces appareils peuvent représenter une menace pour la sécurité des personnalités au Canada, à commencer par le premier ministre Justin Trudeau.

Ex-spy boss urges Ottawa to prepare for 'cyber war'
Toronto Star, Alex Boutilier, 2016 09 01
Ottawa - The **former chief of Canada's electronic spies is calling on Ottawa to develop an arsenal of cyber weapons - and give defence and intelligence agencies the green light to attack.** "Cyber war" is still in its infancy, **John Adams** argued in a July paper, but computer viruses could soon cause as much damage to a country as conventional bombs and bullets. Canada has traditionally - at least officially - focused cyber efforts on defending against espionage and attacks from both hostile states and hackers. But Adams, the **chief of the Communications Security Establishment between 2005 and 2012, is calling on the federal Liberals to rethink that approach and allow Canada to go on the offensive.** "Some people think that cyber war will sooner or later replace kinetic war. More frequently, cyber war is presented as a new kind of war that is cheaper, cleaner and less risky for an attacker than other forms of armed conflict," Adams wrote in a paper published by the Canadian Global Affairs Institute. "In either case, the Canadian Armed Forces have a responsibility not only to protect their own systems but they also need to have the authority to direct offensive action . . . if that is what it takes to blunt an ongoing catastrophic attack on critical infrastructure." Adams argued that if a hostile state were attacking Canada's networks, Canada should be able to respond in

kind to stop that attack. But in an interview with the Star on Tuesday, Adams was clear that he's envisioning a much wider range of actions for Canada's defence agencies.

Canada's Border Agency Saying Little About Its 15 Employees Accused of Sex Assault
Vice News, Hilary Beaumont, 2016 08 31
Toronto—**Fifteen Canada Border Services Agency (CBSA) employees have been accused of sexual assault in the last decade through the agency's internal investigation mechanism**, VICE News has learned. And at least five of those accused employees still work for the CBSA, according to documents obtained through an access to information request. In the cases included in the access to information request, women and men reported allegations of sexual assault through the agency's internal investigation mechanism, the Security and Professional Standards Analysis section, which looks into the allegations and determines if they are founded, unfounded or inconclusive. The CBSA says it fully investigated and found the case inconclusive, but police in Quebec found enough evidence to lay charges.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

Air Force, Short of Drone Pilots, Uses Contractors to Fight Terror
New York Times, Michael S. Schmidt, 2016 09 06
Washington - The **American military's extensive use of drones against the Islamic State and other terrorist groups has resulted in a shortage of Air Force pilots and other personnel to operate the aircraft, leading the Pentagon to rely more on private contractors for reconnaissance missions in Afghanistan and Iraq.** Since the Sept. 11, 2001, attacks, the Pentagon has used contractors to perform many duties traditionally carried out by uniformed personnel, like protecting military bases and feeding service members. The contractors who are now serving as drone pilots are based in the regions where the drones are flown, and they are legally prohibited from being "trigger pullers" and firing weapons, Air Force officials said. But there is no limit on the type of reconnaissance they can perform, and they are providing live video feeds of battles and special operations.

Inside Menwith Hill
The Intercept, Ryan Gallagher, 2016 09 06
Washington - The narrow roads are quiet and winding, surrounded by rolling green fields and few visible signs of life beyond the occasional herd of sheep. But on the horizon, massive white golf ball-like domes protrude from the earth, protected behind a perimeter fence that is topped with piercing razor wire. **Here, in the heart of the tranquil English countryside, is the National Security Agency's largest overseas spying base. Once known only by the code name Field Station 8613, the secret base -- now called Menwith Hill Station -- is located about nine miles west of the small town of Harrogate in North Yorkshire. Originally used to monitor Soviet communications through the Cold War, its focus has since dramatically shifted, and today it is a vital part of the NSA's sprawling global surveillance network.** For years, journalists and researchers have speculated about what really goes on inside Menwith Hill, while human rights groups and some politicians have campaigned for more transparency about its activities. Yet the British government has steadfastly refused to comment, citing a longstanding policy not to discuss matters related to national security. Now, however, top-secret documents obtained by The Intercept offer an unprecedented glimpse behind Menwith Hill's razor wire fence. The files reveal for the first time how the NSA has used

the British base to aid "a significant number of capture-kill operations" across the Middle East and North Africa, fueled by powerful eavesdropping technology that can harvest data from more than 300 million emails and phone calls a day. Over the past decade, the documents show, the NSA has pioneered groundbreaking new spying programs at Menwith Hill to pinpoint the locations of suspected terrorists accessing the internet in remote parts of the world. The programs -- with names such as **GHOSTHUNTER and GHOSTWOLF** -- have provided support for conventional British and American military operations in Iraq and Afghanistan. But they have also aided covert missions in countries where the U.S. has not declared war. NSA employees at Menwith Hill have collaborated on a project to help "eliminate" terrorism targets in Yemen, for example, where the U.S. has waged a controversial drone bombing campaign that has resulted in dozens of civilian deaths.

Intelligence community investigating covert Russian influence operations in the United States
Washington Post, Multiple reporters, 2016 09 05
Washington - **U.S. intelligence and law enforcement agencies are probing what they see as a broad covert Russian operation in the United States to sow public distrust in the upcoming presidential election and in U.S. political institutions**, intelligence and congressional officials said. The aim is to understand the scope and intent of the Russian campaign, which incorporates cyber-tools to hack systems used in the political process, enhancing Russia's ability to spread disinformation. The effort to better understand Russia's covert influence operations is being spearheaded by James R. Clapper Jr., the director of national intelligence. "This is something of concern for the DNI," said Charles Allen, a former longtime CIA officer who has been briefed on some of these issues. "It is being addressed." A Russian influence operation in the United States "is something we're looking very closely at," said one senior intelligence official who, as others interviewed, spoke on the condition of anonymity to discuss a sensitive matter. Officials are also examining potential disruptions to the election process, and the FBI has alerted state and local officials to potential cyberthreats. **The official cautioned that the intelligence community is not saying it has "definitive proof" of such tampering, or any Russian plans to do so.** "But even the hint of something impacting the security of our election system would be of significant concern," the official said. "It's the key to our democracy, that people have confidence in the election system."

Obama Met With Putin, Said Hackers Shouldn't Create a Cyber 'Wild Wild West'
ABC News, Jordyn Phelps, 2016 09 05
New York - President Obama addressed his tense, 90-minute-long meeting with Russian President Vladimir Putin on the sidelines of the G20 in a press conference on Monday. The two leaders apparently held fast to their positions on hot button issues like cyber-security and brokering a cease- fire in Syria. Russian hackers having been implicated in some current cyber threats and security issues was a key topic. Though Obama didn't identify specific instances, **he said "we have had problems with cyber intrusions from Russia in the past" and that the goal is to not to duplicate a "cycle of escalation" that has occurred in arms races of the past.**

U.S. Spy Agency Tweets, Deletes, Then Apologizes
The Wall Street Journal, Damian Paletta, 2016 09 04
Washington— Whoever had the Labor Day weekend shift on **the Defense Intelligence Agency's Twitter account** may have been feeling a little punchy. On Saturday afternoon the "verified" account, which has 83,400 followers, likely including foreign spies, sent a pointed and sarcastic message aimed at the Chinese government. "**Classy as always China," the tweet read, linking to a New York Times article about a heated verbal kerfuffle that almost**

escalated into something serious between U.S. and Chinese officials after President Barack Obama landed in China aboard Air Force One. The **Twitter message was quickly deleted, but not before its pointed snark was noticed by a number of people.** "The guy or gal who runs @DefenseIntel's Twitter feed over the weekend needs a medal & raise right now," tweeted **Aki Peritz**, a former Central Intelligence Agency official. It is unclear what prompted the DIA to delete the tweet. The Defense Intelligence Agency is one of the government's most-secretive arms, a spy agency within the Pentagon that is involved in some of the country's most-sensitive missions. Its Twitter feed tends to be one of the tamest in Washington, highlighting public speaking engagements and similar events.

F.B.I. Email Inquiry Reveals Some of Secretary's Habits
New York Times, Michael S. Schmidt, 2016 09 03
Washington - **Documents released by the F.B.I. on Friday revealed new details about the Justice Department's yearlong investigation into Hillary Clinton's use of a private email server and whether she and her aides mishandled classified information**. Among the documents was an 11-page summary of an interview F.B.I. agents conducted with Mrs. Clinton on July 2. Two days later, the F.B.I. director, James B. Comey, said the bureau had recommended to the Justice Department that neither Mrs. Clinton nor her aides should be charged with a crime. Here are six highlights from those documents: According to the F.B.I., in December 2014 a top aide to Mrs. Clinton told the company that housed her server to delete an archive of emails from her account. The company, Platte River Networks, apparently never followed those instructions.

F.B.I. Files on Email Inquiry Show Grilling on Clinton's Judgment
New York Times, Eric Lichtblau, 2016 09 03
Washington - **F.B.I. officials questioned Hillary Clinton extensively about her judgment in using her private email system to discuss classified drone strikes and in allowing aides to destroy large numbers of emails, before ultimately deciding she should not face criminal charges, according to investigative documents released Friday**. The documents provided a number of new details about Mrs. Clinton's private server, including what appeared to be a frantic effort by a computer specialist to delete an archive of her emails even after a congressional committee had requested they be preserved. In a 3½-hour interview with the Justice Department's top counterintelligence officials on July 2, Mrs. Clinton defended her handling of the private email system by repeatedly saying she had deferred to the judgment of her aides, an F.B.I. summary of the interview showed. Mrs. Clinton's use of the private server has shadowed her presidential campaign for a year and a half.

Leaked Catalogue Reveals a Vast Array of Military Spy Gear Offered to U.S. Police
The Intercept, Sam Biddle, 2016 09 02
Washington - A **confidential, 120-page catalogue of spy equipment, originating from British defense firm Cobham and circulated to U.S. law enforcement, touts gear that can intercept wireless calls and text messages, locate people via their mobile phones, and jam cellular communications in a particular area**. The catalogue was obtained by The Intercept as part of a large trove of documents originating within the **Florida Department of Law Enforcement,** where spokesperson **Molly Best** confirmed Cobham wares have been purchased but did not provide further information. The document provides a rare look at the wide range of electronic surveillance tactics used by police and militaries in the U.S. and abroad, offering equipment ranging from black boxes that can monitor an entire town's cellular signals to microphones hidden in lighters and cameras hidden in trashcans. Markings date it to 2014.

Security Debate Draws Attention to U.S. Border With Canada
Wall Street Journal, Chster Dawson, 2016 09 01
Westby, Montana - The **U.S. border with Canada is attracting greater scrutiny as debate rages in the U.S. presidential campaign about security on its southern border with Mexico, and concern grows over global terrorism and vulnerability to illegal crossings**. The U.S. government has been steadily beefing up surveillance of the northern border with new technology designed to help monitor areas too remote for round-the-clock patrols by field agents. Much of the change comes from the gradual rollout of new technologies that were promised in the aftermath of a security reassessment following the 2001 terrorist attacks. Sen. Heidi Heitkamp (D., N.D.) this year called on the Department of Homeland Security to pay closer attention to the northern border and not view it as an "afterthought." Last year, she co-sponsored a bill with Sen. Kelly Ayotte (R., N.H.) to step up funding for recruiting more border agents to specifically target more remote areas along the border with Canada. Some lawmakers in northern border states cite Canada's greater willingness to accept refugees. "A threat to one country is a threat to the other," said **Christine Constantin**, a spokeswoman for the Canadian Embassy in Washington, adding that Canada has a "zero tolerance" policy for refugees with security concerns. **"No terrorists have been successful in attacking the homeland coming through America's northern border,"** she said.

Former Anti-Terror FBI Employee Now Finds Himself a Target
The Intercept, Trevor Aaronson, 2016 09 01
Washington - As **an FBI surveillance employee, Ray Tahir spent the last decade tailing Muslims in counterterrorism cases**. Among the investigations whose surveillance Tahir led were those of the charity Holy Land Foundation for Relief and Development in Texas and North Carolina's Daniel Patrick Boyd, who with others was convicted of conspiracy to provide material support to terrorists and conspiracy to commit murder, maiming, and kidnapping overseas. Both FBI cases had their critics. The American Civil Liberties Union described the prosecution of Holy Land Foundation as "discriminatory enforcement of counterterrorism laws." In the Boyd case, as in other informant-led FBI stings, there are questions about whether the men convicted would have done anything at all were it not for the FBI's involvement. As the FBI targeted Muslims in the United States following the 9/11 attacks, Tahir was among the front-line employees who made some of these cases possible. Now, he alleges, he has **become a target himself**. Tahir, who had been called for a hearing at the **FBI's Office of Professional Responsibility**, was accused of making personal charges on his covert credit card, unauthorized gasoline purchases, and lack of candor.

Democrats' Email and a Murky Trail
New York Times, Eric Schmitt, 2016 09 01
Washington - **American intelligence agencies believe that the Russian government was behind the theft of emails and documents from the Democratic National Committee**, but many questions remain about how the documents made their way to WikiLeaks, which released them. Before the WikiLeaks release, a large sampling was published by several news organizations and a hacker called **Guccifer 2.0**, who investigators now believe was an agent of the G.R.U., Russia's military intelligence service. American intelligence agencies say the earlier leaks from Guccifer and the WikiLeaks material have the same bits of code and telltale metadata traced to previous intrusions attributed to the **G.R.U. or the F.S.B.**, another Russian spy agency. However, **Julian Assange**, the editor of WikiLeaks, makes a distinction between the Democratic National Committee material he released and the earlier releases by Guccifer and others, saying there is no proof that the Russians gave him the documents. In recent weeks, Mr. Assange has threatened to take his revelations to a new level. In August, some of the National Security Agency's source code for breaking into foreign computer systems -- the

holy grail of the **N.S.A.'s Tailored Access Operations** unit -- was revealed on a website, with the announcement of an auction for the remainder of it.

Democrats ask the FBI to investigate Trump advisers' Russia ties
Washington Post, Josh Rogin, 2016 08 31
Column - **Several leading Democratic lawmakers are asking the Federal Bureau of Investigation to investigate senior Trump campaign advisers for collusion in the suspected Russian hacking of American political organizations and election systems**. It's the most serious set of allegations to date about deep connections between the Trump team and the Kremlin, though the case is largely circumstantial. On Monday, The New York Times broke the story of **Senate Minority Leader Harry Reid's August 27 letter to FBI Director James Comey asking the bureau to investigate alleged Russian interference in the U.S. presidential election**, which followed new reports that foreign hackers penetrated two state election databases. In the same letter, without naming them directly, Reid pointed Comey to two specific Trump advisers, each of whom is allegedly connected to Russia, according to Reid and the Clinton campaign. Reid's letter implicitly asks Comey to look into the dealings of Roger Stone, the longtime Trump friend who has claimed to be in touch with Wikileaks founder Julian Assange, and Carter Page, a Trump foreign policy advisor who traveled to Moscow in July.

FBI Director: Americans Never Had 'Absolute Privacy'
Nextgov.com (US), Frank Konkel, 2016 08 31
Washington - **FBI Director James Comey said his agency is preparing for a renewed conversation on encryption by collecting information regarding how "widespread default encryption"** has affected law enforcement at the federal level. Comey said default encryption--especially on mobile devices-- in the post-Edward Snowden era has fundamentally impacted law enforcement agencies at the local, state and federal levels, providing a near "absolute privacy" he argued had never occurred before in history. Comey said the FBI has been unable to collect evidence from 650 of 5,000 devices, including mobile phones and tablets, received from state and local governments this year. The **FBI is tallying that data and other statistics, Comey said, for a public conversation on encryption**--specifically the balance between security and privacy--sometime after the Nov. 8 election.

FBI Director Has High Expectations for New Cyber Security Agents
NBC News, Marianna Sotomayor, 2016 08 31
New York - **Federal Bureau of Investigations Director James Comey has high expectations when it comes to recruiting agents for their cyber security team.** He says the perfect applicant would be intelligent, have integrity and the perfect dose of physicality to work competitively at the FBI. But he knows that finding the trifecta of talent in one person can be rare, especially when strict rules can keep top recruits from applying. "We may find people of great technical talent who want to smoke weed on the way to the interview," Comey said at the Symantec Government Symposium in Washington, D.C. on Tuesday. Though the joke was welcomed by laughs in the audience, **Comey made a point to say that even though a candidate for the job may not be perfect, the FBI is trying to find people they could "grow" and mold in other areas where they lack skills.**

FBI head: We're taking suspected political hacks 'very seriously'
The Hill, Julian Hattem, 2016 08 30
Washington - The **FBI is "very seriously" examining alleged hacks at two state election offices, director James Comey said Tuesday**. "We take very seriously any effort by any actor -- including nation states but especially nation states -- that moves beyond the collection of information about our country, and then offers the prospect of an effort to influence the conduct

of affairs on our country, whether that's election or something else," Comey said at a conference in Washington hosted by Symantec, a digital security company. "Don't want to comment on the particular, but those kinds of things are something that we take very, very seriously and work very, very hard to understand so that we can equip the rest of our government with options for how to deal with it."

The CIA's Venture-Capital Firm, Like Its Sponsor, Operates in the Shadows
Wall Street Journal, Damian Paletta, 2016 08 31
Washington - **Forterra Systems Inc., a California startup focused on virtual reality**, was in need of money and its products didn't have much commercial appeal. Then **funds came in from a source based far from Silicon Valley: In-Q-Tel Inc., a venture-capital firm in Virginia funded by the Central Intelligence Agency**. One catalyst for the 2007 infusion, according to a former Forterra executive and others familiar with it, was a recommendation by a man who sat on the board of the venture-capital firm-- and also on the board of Forterra. In-Q-Tel pumped in cash, Forterra developed some tools useful to the military, and government contracts started coming in. Like the agency that founded it, **the CIA-funded venture- capital firm operates largely in the shadows.** In-Q-Tel officials regard the firm as independent, yet it has extremely close ties to the CIA and runs almost all investment decisions by the spy agency. The firm discloses little about how it picks companies to invest in, never says how much, and sometimes doesn't reveal the investments at all. Even less well-known are potential conflicts of interest the arrangement entails, as seen in this Forterra example and others continuing to the present.

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

Parliament's back for Snoopers' Charter. Former head of GCHQ talks to El Reg
The Register (UK), Alexander J. Martin, 2016 09 05
London - **Parliament has returned from recess (only for a fortnight before conference season begins) and the House of Lord's committee stage examination of the Investigatory Powers Bill will resume this afternoon**. The upper chamber had been waiting for the publication of a review of the bill's bulk powers, which had been led by the independent reviewer of terrorism legislation, David Anderson QC. Bulk hacking missions were addressed last week at a panel convened by the Chartered Institute of IT. **Academics, National Crime Agency representatives, and Sir David Omand -- the former director of GCHQ and visiting professor at KCL -- discussed the difficulties that traditional law enforcement techniques encountered when attempting to tackle cybercrime.** Corresponding with The Register, Sir David explained how in his experience such bulk hacking powers were necessary for law enforcement purposes on the internet, rather than just being necessary for national security reasons. Omand wrote: "The recent serious rise in global cybercrime by organised criminal groups...has only reinforced the importance of having the specialist techniques and international liaisons of the secret agencies available to support the investigations of law enforcement."

Page 3 girl flirts with joining punk mum in jihadist brides brigade
Sunday Times, 2016 09 04

London— **Anti-terrorist police fear that a former glamour model from West Yorkshire who has secretly embraced Islam is being groomed online by Isis to become a jihadist bride.Kimberley Miners,** who has posed topless for The Sun, has been using Facebook to communicate with a British fighter in Syria who is urging women to leave the UK and join the Isis "caliphate". The Sunday Times has discovered that Miners, 27, from Bradford, appears on social media under the alias Aisha Lauren al-Britaniya and has posted images of Muslim women brandishing rifles and other weapons. Pictures show her fully veiled or with only her blue eyes on display, but in public she wears skinny jeans and leaves her long blonde hair uncovered. She says she was abused when she went out in Islamic dress. Miners revealed on Friday that she had travelled to Turkey — the most common springboard for Syria — on two previous occasions and planned to visit the country again this autumn, although she denied wanting to marry a jihadist. It is understood that her activities, which include "liking" and sharing Isis videos, have triggered an **investigation by anti-terrorist police and MI5**. They have spoken to her up to four times and referred her to an anti-radicalisation programme. She has been warned that she faces arrest if she continues to engage in extremism.

State spying helps to create extremists. My father was one of them
The Guardian (London), Francis Beckett, 2016 08 31
Op-ed - When you lock people up without trial, "whether it is in Belmarsh or Guantánamo Bay, you recruit more terrorists than you contain", warned Shami Chakrabarti earlier this year. She has said that senior intelligence officials made a successful bid for enormous power post-9/11, particularly in government surveillance. And appalling attacks in France and Belgium have made us more likely to give the security services the power to curtail our liberties. But should we? I claim some special insight. **For at least the first 10 years of my life, from 1945 to 1955, my childhood home was under constant MI5 surveillance. My parents knew it, though I did not; and I have spent a lot of the past two years with recently released MI5 records at the National Archives, reading verbatim my parents' telephone conversations from 60 years ago and the spies' reports on their movements.** I recognise a few of the people described as the adults who peopled my childhood, and I can picture in my mind where the watcher's car was parked when he reported on my family's movements. My father, John Beckett, was a leading fascist. He was in prison for nearly four years during the second world war, then under a sort of house arrest, not allowed to live within 20 miles of London or to travel more than five miles from his home. When these restrictions were lifted, the surveillance continued, masterminded by Graham Mitchell, who became deputy director of MI5 in 1956. It is mostly Mitchell's memoranda I have been reading. They betray a deeply unhealthy pleasure in the secret power his position gave him over the life of another man.

Return to Table of Contents/ Retour à la table des matières

Australia / Australie

PM's stance on China worries experts
The Australian Financial Review, Aaron Patrick, 2016 09 03
Canberra - **The government's top intelligence experts are concerned Prime Minster Malcolm Turnbull isn't taking their warnings about the security threat posed by China seriously enough and the former banker is relying on advice from outside experts.**
Despite vetoing a Chinese bid for Sydney's electricity network this month, Mr Turnbull and some other cabinet ministers are reluctant to act on or receive warnings that China is engaging in

spying on an "industrial scale" and that business secrets are among its top targets, three sources with senior contacts in the security services said. "It is far more ambitious and better resourced than ever before," said Paul Monk, an intelligence and foreign affairs expert who headed China analysis for the Defence Intelligence Agency. "It's notorious with politicians that they find intelligence to be a new thing when they go into politics. It's things they would prefer not to know or suggest actions that can be embarrassing." Security experts say China has a well-resourced effort that uses cyber-espionage and human agents to steal Australian commercial secrets and obtain sensitive government information.

Domestic spy chief sounded alarm about donor links with China last year
ABC (Australia), Chris Uhlmann, 2016 09 01
Canberra - **Australia's domestic spy chief warned the nation's major political parties last year that some of their donors had strong links to the Chinese Government**. The revelation comes as pressure grows for a ban on foreign donations to Australian politics. Australia's domestic spy chief warned the nation's major political parties last year that some of their donors had strong links to the Chinese Government. The **ABC has confirmed that the director-general of the Australian Security Intelligence Organisation (ASIO), Duncan Lewis, personally briefed former Liberal federal director Brian Loughnane, outgoing Labor secretary George Wright and the Nationals' federal director Scott Mitchell on the national security risks posed by foreign-linked donations.** The verbal briefing included naming donors his agency believed were acting on behalf of the Chinese Government. None of the party leaders would comment on the meetings. It comes as pressure grows for a ban on foreign donations to Australian political parties. Labor frontbencher Stephen Conroy has called on the Prime Minister to commit to electoral donation reform. "Ban foreign companies from actually being able to donate at all," Senator Conroy said. "We're one of a very small number of countries who actually don't ban this practice." The security warning to party chiefs is another indicator of the growing concern in intelligence agencies about the use of "soft power" in Australia.

Canadian only foreigners likely to show in Ausgrid contest
The Australian, Staff reporter, 2016 08 31
Sydney - A **raft of Canadian funds are expected to be the only foreign groups lining up for a potential acquisition of NSW electricity distributor Ausgrid**, ahead of a revised sale process run by Deutsche and UBS. The Canadian Pension Plan Investment Board and Caisse de depot et placement du Quebec are believed to be the two foreign parties interested in buying a 99-year lease of a 50.4 per cent interest in Ausgrid. CDPQ is being advised by the Royal Bank of Canada, while the likely advisers for CPPIB would be Morgan Stanley or Goldman Sachs. While bidders are yet to receive any assurance on the terms in which foreigners can participate in the sales process, it is understood China's State Grid has abandoned any hope of an acquisition, while Hong Kong's Cheung Kong Infrastructure is unlikely to participate. It comes after both bidders were blocked from buying the asset in the last process after Treasurer Scott Morrison flagged concerns about an acquisition by the parties on the grounds of national security. The **thinking now is that the government may argue an investment by the Canadians can be justified because it is among the countries that form the so-called Five Eyes intelligence alliance that already share sensitive information.**

Return to Table of Contents/ Retour à la table des matières

New Zealand / Nouvelle-Zélande

People urged not to give in to demands of cyber criminals
Radio New Zealand News, Staff reporter, 2016 08 31
Wellington - **People who fall victim to ransomware attacks are being urged not to give in to the demands of cyber criminals**. The executive director of Netsafe, Martin Cocker, says his organisation deals with a handful of people each week who are wondering what to do after finding their computer files locked up. Mr Cocker says those people are discouraged from paying a ransom. He says cyber criminals use whatever money they get to fund further crime and even if a ransom is paid, there is no guarantee someone will get their files back. **The electronic spy agency, the GCSB, has raised concerns that these sorts of cyber attacks are becoming more common.**

Return to Table of Contents/ Retour à la table des matières

International

China / Chine

American student kidnapped by Kim Jong Un 'was arrested in China for helping North Korean refugees escape oppressive country'
Mail Online, Kelly Mclaughlin and James Wilkinson, 2016 09 02
London— A US **student who thought to have been kidnapped by Kim Jong Un's secret agents was actually arrested in China for helping defectors escape the North Korean dictator's oppressive regime, it** has been claimed. **David Sneddon** of Brigham Young University was just 24 when he disappeared in Yunnan Province. Chinese police have said that Sneddon likely disappeared in a hiking accident. South Korea's Abductees' Family Union claimed he was abducted by North Korea to teach English to Kim Jong Un.The union's chief Sung-Yong Choi said Sneddon is now living in the North Korean capital of Pyongyang, where he has a wife and two children. But new evidence has emerged which suggests he was arrested in China on charges of helping illegal residents travel through the country. A document revealed to DailyMail.com by Sneddon's family claims **the Ministry of State Security of the People's Republic of China (MSS)** then handed over to North Korea officials in 2004. According to the report from the National Association for the Rescue of Japanese Kidnapped by North Korea (NARKN) from May 2012, Sneddon was arrested in August of that year.

Hong Kong authorities 'attacked by Chinese hackers'
Agence France-Presse, Staff reporter, 2016 09 02
Beijing - **Mainland Chinese hackers have attacked two Hong Kong government departments**, a US-based security firm said Friday, as the city prepares for a crucial election. The attack occurred in August, in the run- up to parliamentary elections Sunday, as fear of Beijing's tightening grip on semi-autonomous Hong Kong creates unprecedented social and political divides. **California-based security firm FireEye** said Friday a China-based group they have been tracking since 2011 attacked at least two Hong Kong government agencies early last month. The firm's Asia Pacific chief technology officer Bryce Boland believes the group carrying out the attacks, known as APT3, "is sponsored by the People's Republic of China". "Typically when we see government attacks on other governments, it's about intelligence gathering and trying to gain access to information they can't get via other means," Boland told AFP.

American Is Facing Spy Trial in China, and Husband Seeks Obama's Help
New York Times, Chris Buckley, 2016 08 31

Beijing - An **American businesswoman faces trial in China on spying charges dating back 20 years,** including that she tried to recruit Chinese in the United States to spy against their homeland, her husband said on Tuesday. He urged President Obama to raise the case with President Xi Jinping of China at a Group of 20 summit meeting in eastern China beginning over the weekend. The businesswoman, **Phan Phan-Gillis, widely known as Sandy, was indicted last month on the espionage charges after having been detained while visiting China last year.** But her husband, Jeff Gillis, said he had held off revealing the indictment while new lawyers for his wife tried to come to grips with the case. "The time really is critical for Sandy, with the imminent meeting between President Obama and Xi Jinping," Mr. Gillis said by telephone from the couple's home in Houston.

Return to Table of Contents/ Retour à la table des matières

Russia / Russie

Putin Says DNC Hack Was a Public Service, Russia Didn't Do It

Bloomberg News, 2016 09 02

Vladibostok-- **Vladimir Putin said the hacking of thousands of Democratic National Committee emails and documents was a service to the public, but denied U.S. accusations that Russia's government had anything to do with it.** "Listen, does it even matter who hacked this data?" Putin said in an interview at the Pacific port city of Vladivostok on Thursday. "The important thing is the content that was given to the public." U.S. officials blame hackers guided by the Russian government for the attacks on DNC servers earlier this year that resulted in WikiLeaks publishing about 20,000 private emails just before Hillary Clinton's nominating convention in July. The documents showed attempts by party officials to undermine her chief Democratic rival, Bernie Sanders, and led to the resignation of the head of the DNC, Representative Debbie Wasserman Schultz of Florida. "There's no need to distract the public's attention from the essence of the problem by raising some minor issues connected with the search for who did it," Putin said of the DNC breach. "But I want to tell you again, I don't know anything about it, and on a state level Russia has never done this."

How Russia Often Benefits as Assange Reveals Secrets

New York Times, Multiple reporters, 2016 09 01

New York - **Julian Assange** was in classic didactic form, holding forth on the topic that consumes him -- the perfidy of big government and especially of the United States. Mr. Assange, the editor of WikiLeaks, rose to global fame in 2010 for releasing huge caches of highly classified American government communications that exposed the underbelly of its wars in Afghanistan and Iraq and its sometimes cynical diplomatic maneuvering around the world. But in a televised interview last September, it was clear that he still had plenty to say about "The World According to US Empire," the subtitle of his latest book, "The WikiLeaks Files." From the cramped confines of the Ecuadorean Embassy in London, where he was granted asylum four years ago amid a legal imbroglio, Mr. Assange proffered a vision of America as superbully: a nation that has achieved imperial power by proclaiming allegiance to principles of human rights while deploying its military-intelligence apparatus in "pincer" formation to **"push" countries into doing its bidding, and punishing people like him who dare to speak the truth. Notably absent from Mr. Assange's analysis, however, was criticism of another world power, Russia, or its president, Vladimir V. Putin, who has hardly lived up to WikiLeaks' ideal of transparency.** A **New York Times examination of WikiLeaks' activities during Mr. Assange's years in exile found a different pattern: Whether by conviction, convenience**

or coincidence, WikiLeaks' document releases, along with many of Mr. Assange's statements, have often benefited Russia, at the expense of the West. Among United States officials, the emerging consensus is that Mr. Assange and WikiLeaks probably have no direct ties to Russian intelligence services. But they say that, at least in the case of the Democrats' emails, Moscow knew it had a sympathetic outlet in WikiLeaks, where intermediaries could drop pilfered documents in the group's anonymized digital inbox.

Return to Table of Contents/ Retour à la table des matières

Europe

Suspected spy sentenced to three years after plea agreement
Hina-Croatian News Agency, 2016 09 06
Zagreb— The **High Court in Belgrade has upheld a plea agreement with Cedo Colovic, charged with spying for Croatian intelligence services, sentencing him to three years in prison**, the court said Tuesday. Colovic, who has dual Serbian and Croatian citizenship, was arrested outside Belgrade on September 2 and the plea agreement was reached with the Public Prosecutor's Office on September 4. He had lived and worked in Croatia until 1990 when he moved to Serbia. According to Belgrade media, Colovic served as an officer in the army of the self-proclaimed Republic of Serb Krajina and came to Serbia as a refugee in August 1995 at the time of Operation Storm. He was suspected of providing confidential military and intelligence information to a Croatian intelligence service.

Allemagne : le gendarme de la vie privée étrille les services de renseignement
Le Monde, Journaiste maison, 2016 09 06
Berlin - Une **inspection menée sur une installation des services de renseignement allemands a débouché sur 12 plaintes formelles**. En Allemagne, les révélations d'Edward Snowden sur les activités de surveillance des Etats-Unis n'en finissent pas de faire des vagues. **La très grande proximité et la collaboration entre la National Security Agency américaine (NSA) et le Service fédéral de renseignement (BND) a notamment déclenché une enquête du commissaire fédéral pour la protection des données (BfDI).** Il a pu se rendre dans l'une des installations conjointes de la NSA et du BND, à Bad Aibling, dans le sud du pays. Il en a tiré une analyse juridique, classifiée, que s'est procurée le site allemand spécialisé Netzpolitik . Une analyse au lance-flammes Cette analyse est extrêmement sévère pour le BND: le commissaire a dénombré 18 violations sévères de la loi, et a adressé 12 plaintes formelles liées à ces manquements. Netzpolitik note qu'il s'agit du nombre de plaintes adressé par le commissaire sur une année entière pour tout l'appareil fédéral allemand. Selon le BfDI, le BND a créé et utilisé au moins sept bases de données sans aucun fondement légal. Ces bases, écrit-il, doivent être détruites immédiatement.

Loi sur le renseignement: les cantons latins unis
Tribune de Genève, Lafargue, 2016 09 06
Genève - **Les chefs des Départements de justice et police des six cantons romands et du Tessin étaient hier à Genève Les membres de la Conférence latine des chefs des départements de justice et police (CLDJP) ont fait part de leur soutien unanime à la nouvelle loi sur le renseignement,** hier à Genève. Ils espèrent qu'elle recueillera « l'assentiment franc et massif de la population » lors des votations du 25 septembre. « Cette conférence de presse est exceptionnelle, la CLDJP ne prend pas position habituellement » , a déclaré Pierre Maudet, conseiller d'Etat PLR genevois et président de la CLDJP. Provenant de

partis différents, les sept membres de la conférence soutiennent la nouvelle loi, a-t-il précisé. Selon eux, elle placera la Suisse au même niveau que les pays européens et donnera les moyens d'agir au **Service de renseignement de la Confédération (SRC).**

DGSE L'espion qui parlait trop
Le Monde, Journaliste maison, 2016 09 05
Paris - **Lors d'une anodine réunion d'anciens élèves d'une grande école d'ingénieurs, Bernard Barbier, personnage central de la DGSE durant dix ans, a livré en public, dans une intervention filmée, quelques secrets d'Etat, notamment sur la guerre cybernétique**. Comment les Etats-Unis ont espionné l'Elysée, par le biais des logiciels malveillants glissés sur Facebook par la NSA. Comment la France a monté ses équipes de " hacking " et créé son propre logiciel malveillant, baptisé " Babar ". Comment Bernard Barbier a proposé une fusion entre la DGSE et son homologue allemand, qui a été rejetée pour des raisons politiques. Comment les révélations d'Edward Snowden ont aidé la France à se protéger de l'espionnage " ami " des Américains.

Les confessions d'un maître de l'espionnage (Canada)
Le Monde, Jacques Follorou, 2016 09 05
Paris - **Bernard Barbier, personnage-clé de la DGSE pendant dix ans, a levé le voile sur plusieurs secrets d'Etat**. C'est une intrusion inespérée dans un monde interdit aux regards extérieurs, celui du renseignement et des guerres secrètes. Espionnage et cybersécurité, Bernard Barbier reçu par Symposium Centrale Supélec: **M.Barbier, qui fut de 2006 à 2014 l'homologue du directeur de l'Agence nationale de sécurité (NSA) américaine, en tant que chef de la direction technique de la Direction générale de la sécurité extérieure (DGSE),** a commencé sa carrière au Commissariat à l'énergie atomique (CEA). Au sein de la DGSE, il obtient, en2008, une enveloppe de 500millions d'euros et 800 nouveaux postes pour l'une des plus formidables révolutions du renseignement français: créer un système de collecte massive de données replaçant la France dans la course à l'espionnage moderne. Au cours de cette causerie, il a ainsi fait oeuvre de transparence sur certaines des principales affaires d'espionnage récentes ayant touché la France. Il **a brisé des tabous, notamment en relatant l'attaque chinoise sur Areva et en confirmant la responsabilité de la France derrière une attaque informatique mondiale détectée par les services canadiens.**

Head of Turkey's intelligence expected to resign
Trend News Agency, 2016 09 02
Istanbul— **After the recent resignation of Turkey's Interior Minister Efkan Ala, head of the country's National Intelligence Organization Hakan Fidan is also expected to step down from his position,** the Milligazete reported Sept.2. Fidan's resignation is being discussed in Ankara's political circles, according to the newspaper. Hakan Fidan was appointed head of the National Intelligence Organization in May 2010. It was earlier reported that a number of reforms will be held in this structure. It was planned that the National Intelligence Organization will have two divisions: foreign and domestic intelligence.

German spies 'systematically violating constitution'
The Local (Germany), Staff report, 2016 09 02
Berlin - The **BND**, Germany's version of the CIA, **has been accused of massive breaches of the constitution in a leaked report by the government's representative for data protection**. "The BND [Bundesnachrichtendienst] systematically lifted and used personal data without a legal basis to do so," wrote Federal Data Protection Commissioner Andrea Voßhoff in a report seen by public broadcasters NDR and WDR. Voßhoff is responsible for ensuring that government agencies do not infringe on German citizens' legal rights when using their personal

data. In this capacity she carried out a study of how the BND monitor telecommunications data. In the 60-page report, Voßhoff listed how the BND "systematically and regularly" violates the constitution and used the word "unlawful" 30 times, according to the broadcasters.

German spy agency systematically broke the law: report
Deutsche Welle, Staff report, 2016 09 02
Berlin - **Germany's data protection commissioner, Andrea Vosshoff, has issued a scathing review of the country's Federal Intelligence Service (BND), accusing the agency of egregiously abusing its mandate and breaking the law**. The revelations emerged from a secret 60-page report that was initially published in March of this year. The document was leaked to the German broadcaster NDR, which revealed its findings on Thursday. "Without any legal basis, the BND collected personal data and continued to systematically use them," Vosshoff wrote, using the German acronym for intelligence agency. As Germany's highest-ranking protector of data security, Vosshoff had been tasked with evaluating the intelligence agency's surveillance of telecommunications data.

Ukraine's SBU Answers Illegal Detention, Torture Accusations With Meme
Radio Free Europe, Anna Shamanska, 2016 09 02
Prague - The **Ukrainian Security Service (SBU) has posted images from a Hollywood blockbuster film on Twitter in an apparent effort to mock serious allegations led by two respected international rights watchdogs of secret detentions and torture**. Three stills from the 2016 movie Suicide Squad -- in which jailed villains are coerced by a secret government agency into becoming covert antiheroes to save the world -- appeared in the September 1 tweet by the Security Service (@ServiceSsu) with a caption that read "Prisoners of SBU secret jail." The post was subsequently deleted. The message appeared to be aimed at bolstering the Ukrainian Security Service's denial of accusations by Amnesty International and Human Rights Watch (HRW) in a report in July titled "You Don't Exist" Arbitrary Detentions, Enforced Disappearances, And Torture In Eastern Ukraine.

Le retour en grâce des services secrets
Le Temps, Sylvain Besson, 2016 09 01
Berne--**Longtemps ridiculisés et ignorés par ceux qui comptaient à Berne, les espions helvétiques sont à nouveau pris au sérieux**. Ils devraient triompher le 25 septembre, lors de la votation sur le renseignement. Histoire d'une résurrection C'est un renouveau après des années de déboires. Lors de la votation du 25 septembre, les services secrets suisses devraient opérer un retour en grâce remarqué dans l'opinion publique. Les sondages anticipent un soutien massif à la nouvelle loi sur le renseignement, qui doit leur donner des pouvoirs étendus de surveillance et d'enquête. Après un long purgatoire, marqué par des scandales retentissants et des réformes difficiles, le **Service de renseignement de la Confédération (SRC) semble enfin inspirer confiance.** Y compris dans l'administration fédérale, où l'on apprécie à nouveau son travail après une période d'indifférence glaciale. «Le service est infiniment meilleur qu'il a quinze ans, atteste un fonctionnaire qui lit fréquemment les rapports du SRC. Dans la coopération avec le reste de l'administration, il y a eu des efforts énormes. Dans la coopération avec l'étranger aussi. Pour tous ceux qui reçoivent ses informations [diplomates, procureurs, policiers fédéraux], la qualité de son travail est bien meilleure. Il y a vingt ans, c'était abyssal. Aujourd'hui, ça correspond à ce que doit faire le service d'un pays de notre taille, avec les moyens qui sont les siens.» **Une partie du crédit en revient à son directeur, Markus Seiler.** Un pur bureaucrate, très politique, choisi à ce poste parce qu'il n'était ni du SAP, ni du SRS. Et qu'il était trop libéral- radical pour Ueli Maurer, qui n'en voulait plus comme secrétaire général du Département de la défense.

Czech spy agency warns of a threat of attack by militants
Associated Press, 2016 09 01
Prague— **Islamic radicals could carry out an attack on Czech territory, The Czech Republic's counter-intelligence agency said on Thursday**. The **agency, known as BIS, said in its annual report** that such a threat comes from militants linked to the Islamic State group and also from the Nusra Front. The announcement comes after a wave of attacks in Western Europe. BIS said that according to its information, seven Muslims who were in the Czech Republic for an unspecified period of time left in 2015 with the aim of joining extremist groups in Syria, especially the Islamic State movement and Nusra — which has renamed itself Jabhat Fatah al-Sham since announcing its split from al-Qaida.

Russian intelligence wages information war, says Czech security service
Reuters, 2016 09 01
Prague— **Russian intelligence services are conducting 'an information war' in the Czech Republic, building a network of puppet groups and propaganda agents** that could be used to destabilize the country, the **BIS counterintelligence service** warned on Thursday. Czech security services have long focused attention on a Russian presence that remains significant a quarter century after the country of 10.6 million broke from Moscow's orbit and became a member of NATO and the European Union. In its annual report, the BIS said Russian and Chinese intelligence remained the most active operating in the Czech Republic, and Russia particularly sought to influence Czech media over its role in the Ukrainian and Syrian conflicts.

Sweden: Anti-terror strategy has existed for one year
Esmerk Swedish News, 2016 08 31
Stockholm— The **Swedish government's strategy against terrorism has now existed for one year.** Many of the measures have already been taken, such as the criminalization of terrorism trips. Sweden's Minister of the Interior, Anders Ygeman (S), says that the strategy will not be changed following the terror attacks this summer as it is incredibly difficult to protect oneself against a lone perpetrator who is prepared to die.
On 31 August, a proposal was submitted for consideration, and according to this proposal, the **Swedish Security Service (Säpo),** the military intelligence service Must and the National Defence Radio Establishment (FRA) are to be able to exchange information digitally when making terror threat estimates.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Counterterrorism Taskforce Established in Aden
Asharq Al-Awsat, Bassam al-Qadi, 2016 09 06
Aden - As governorates are freed from militia-hold in **Yemen**, they self repair- a major number of security and judicial institutions in southern Yemen have been reinstated and are operational. Brigadier General Saleh Mohammed Al Qamli, head of the Aden criminal investigations unit told Asharq Al-Awsat newspaper that local police **have launched a special investigations counterterrorism unit, a first for the country**. The task force's chief mission is to pursue suspects believed to be affiliated with the hardline terror groups such as al-Qaeda or ISIS. Qamli explained that the counterterrorism force will also be involved with case files of criminal fugitives and will account to 80 percent of crime prevention.

Foreign Ministry reasons away spy in nuclear team claims
Tehran Times, 2016 09 02
Tehran - The **Iranian Foreign Ministry has snubbed allegations by critics of the nuclear deal who keep saying there has been a spy in the country's nuclear negotiations team.** Deputy Foreign Minister Hamid Baidinejad tried to reason away the allegations as "hasty" and "misinformed" in a message he published on Telegram on Wednesday. The allegations are made to imply that the Joint Comprehensive Plan of Action (JCPOA) is faulty in structure, the diplomat noted, adding, "This approach seems a bit naïve since the process of the nuclear talks was more complicated than to allow a fault to the JCPOA even if such claims were true." Numerous accounts emerged in Iran in the past few weeks over the arrest of one of the country's nuclear negotiators, one contradicting the other.

Iran, Russia Widening Cooperation against Terrorism
Fars News Agency, 2016 09 01
Tehran - **Tehran and Moscow are intensifying efforts to destroy terrorism in the region based on their increasingly strategic relations and cooperation**, a prominent Russian analyst said as Russia's special envoy and deputy foreign minister arrived in Iran on Wednesday. "There is no doubt that the relations between Iran and Russia are strategic. This type of ties is naturally long-term and even permanent and pursue multi-dimensional and complicated goals," Alexnader Paranjiov, a professor at Plekhanov Russian University of Economics, told FNA on Wednesday. Noting that Iran and Russia's second target is settlement of the regional differences and helping the establishment of peace and stability in the region, Paranjiov said that another important goal pursued by both countries is maintaining their national security.

Former Mossad Chief: Israel's Greatest Threat Is Internal Division, Not Hezbollah
Haaretz, Noa Shpigel and Jonathan Lis, 2016 08 31
Jerusalem - **Former Mossad chief Tamir Pardo said on Tuesday that the greatest danger Israel faces isn't external, but rather the divisions within Israeli society**. Speaking at a press conference ahead of an event commemorating fallen Druze soldiers, Pardo said that "If a divided society crosses a certain threshold, you can reach phenomena such as civil war, in extreme cases," adding that the distance between the present-day situation in Israel and a civil war is growing smaller. "I'm afraid we're in that direction," he added. Pardo made his comments in response to a question regarding the threats facing Israel. "Threats to countries today are internal and not external. What you have in Syria, in Iraq, in Libya and in Yemen and in a lot of countries - you see the daily statistics of attacks."

Return to Table of Contents/ Retour à la table des matières

Asia / Asie

BIN Chief Candidate to Undergo Fit and Proper Test on Wednesday
Tempo.co, 2016 09 05
Jakarta— The **Indonesian National Police deputy chief General Budi Gunawan is scheduled to undergo a fit and proper test to take up the State Intelligence Agency (BIN) chief position** replacing Sutiyoso on Wednesday, September 7, 2016. “If all goes well, Budi Gunawan will undergo a fit and proper test at the House's Commission I,” said the House's Commission III speaker Bambang Soesatyo in a written statement, Sunday, September 4, 2016. Bambang noted the Commission III knows Budi Gunawan very well.

Controversial police general tapped to become spy chief
The Jakata Post, 2016 09 03
Jakarta— It appears that **President Joko "Jokowi" Widodo could no longer avoid the pressure of having to make a quick decision regarding the career of controversial police general Com. Gen. Budi Gunawan.** It took Jokowi one year before he decided to name Budi the deputy national police chief after he declined to inaugurate him in the chief's position in February 2015 over allegations that he was involved in a graft case. Facing pressure for Budi to take over as National Police chief when Gen. Badrodin Haiti retired in July, Jokowi again resisted and instead appointed Budi's junior, Gen. Tito Karnavian. When Jokowi decided to undertake another Cabinet reshuffle in July, speculation was rife that Budi would be given a ministerial position, but the prediction did not come to pass. **Jokowi finally relented and on Friday he officially nominated the senior police general to head the National Intelligence Agency (BIN), replacing current BIN chief Sutiyoso.** In his letter Jokowi claimed that the appointment of Budi was part of a regeneration of the intelligence agency, but many saw the decision as Jokowi finally caving into demands from the Indonesian Democratic Party of Struggle (PDI-P), which nominated him for the 2014 presidential election.

Japan doubles size of counterterrorism intelligence unit
Kyodo News, Staff reporter, 2016 09 02
Tokyo - The **Japanese government decided Friday to double the number of personnel serving in an intelligence-gathering unit aimed at preempting and preventing terror attacks**, as Tokyo gears up to host the Olympics and Paralympics in 2020. The unit, under the control of the office of Prime Minister Shinzo Abe, will be expanded to around 80 people from the existing roughly 40 following the decision at a Cabinet meeting. The move reflects the loss of seven Japanese who were among the 20 killed in an attack on a cafe in the Bangladeshi capital Dhaka in July, the government's top spokesman said after the decision. Around half the unit is made up of personnel from the foreign and defense ministries, police and others gathering intelligence region-by-region on Southeast Asia, South Asia, the Middle East and North and West Africa, and the other half consists of those with regional expertise who are dispatched to diplomatic missions.

Egypt and India must cooperate on terror
The Hindu, Suhasini Haidar, Kallol Bhattacherjee, 2016 09 02
New Delhi - **Visiting Egyptian President Abdel Fattah Al Sisi has said India and Egypt must work towards greater cooperation on terrorism**, even as he told External Affairs Minister Sushma Swaraj that he wished to take anti-terror cooperation to a "whole new level." "Egypt and India are stabilising forces in their regions," President Al Sisi, who landed in Delhi on Thursday, said in exclusive comments to The Hindu. "There is a mutual keenness to further enhance our cooperation in this important aspect of our bilateral relations, particularly in light of the emerging threats our respective regions are facing," he added.

India, UK cybersecurity watchdogs sign pact for cooperation (Canada).
Press Trust of India, 2016 09 01
New Delhi - **State-run cybersecurity bodies of India and the UK have signed a Memorandum of Understanding for close cooperation on counter cyberattacks these countries face**. "The Union Cabinet under the Chairmanship of Prime Minister Narendra Modi has been apprised of the MoU signed on May 20, 2016, between Indian Computer Emergency Response Team (CERT-In) and Ministry of Cabinet Office, UK, as represented by CERT-UK, a unit of the Cabinet Office on Cyber Security," an official statement today said. The MoU intends to promote closer cooperation between India and the UK for exchange of knowledge and experience in detection, resolution and prevention of security-related incidents, it added. Earlier

CERT-In signed MoUs with counterpart/similar organisations in about seven countries - Korea, **Canada**, Australia, Malaysia, Singapore, Japan and Uzbekistan. Ministry of External Affairs has also signed MoU with Cyber Security as one of the areas of cooperation with Shanghai Cooperation Organisation.

Return to Table of Contents/ Retour à la table des matières

Africa / Afrique

"Babar", la taupe française qui espionne l'Algérie depuis 2009 (Canada)
Le Matin (Algérie), Yacine K., 2016 09 05
Alger - La **France espionne l'Algérie. Les Etats-Unis espionnent la France. Tout le monde s'espionne. Même si les chefs d'Etat et de gouvernement jouent les vierges effarouchées, cette information est une réalité connue de tous. Surtout sur le volet économique où l'espionnage des entreprises et laboratoires ignore les pays amis. La nouveauté ce sont ces révélations confiées par Bernard Barbie**r, un ancien cadre des services d'espionnage français, Bernard Barbier, rapportés lors du Symposium central supélec. Cet ancien espion confirme les révélations faites déjà par Le Monde en mars 2014. Le quotidien vespéral français avait révélé que les services secrets français espionnait l'Algérie, le Canada, la Côte d'Ivoire, l'Iran grâce à un logiciel. Bernard Barbier a abondé dans le même sens que les anciennes révélations, rappelant que c'est grâce à un logiciel malveillant du nom de code Babar que la Direction générale des services extérieurs (**DGSE**, espionnage extérieur français) espionne un certain nombre de pays, dont l'Algérie. Selon cet ancien limier, le logiciel "Babar" a été détecté par les services canadiens qui ont retrouvé des traces dudit logiciel dans plusieurs pays, comme l'Iran, l'Espagne, la Grèce, la Côte d'Ivoire ou l'Algérie.

DGSN: liens avérés entre le Polisario et les membres du réseau de trafic de drogue démantelé
La Relève (Maroc), Journaiste maison, 2016 09 04
Boujdour, Maroc - **DGSN: liens avérés entre le Polisario et les membres du réseau de trafic de drogue démantelé près de Boujdour** . Les premiers éléments de l'enquête menée par la Brigade nationale de la police judiciaire (BNPJ) sur le réseau de trafic international de drogue, démantelé jeudi, ont démontré l'existence de ramifications régionales de ce réseau dans les camps de Tindouf et le nord du Mali. Les premiers éléments de l'enquête ont également permis d'établir des liens avérés de ses membres avec des responsables du Polisario et leur collusion avec des activités terroristes, indique **la Direction générale de la sûreté nationale (DGSN).** Ces investigations ont prouvé que le propriétaire de la drogue saisie, originaire du nord du Mali, a passé un accord avec l'un des trafiquants connu dans les camps de Tindouf sous le nom de "Robio" en vue de garantir l'opération de transport et d'acheminement de la drogue au Mali en contrepartie d'une importante somme d'argent, précise vendredi la DGSN dans un communiqué.

Return to Table of Contents/ Retour à la table des matières

Americas / Amériques

Brazil terror suspects considered chemical attack in Rio
Brazilian daily Folha de Sao Paulo via BBC Monitoring Americas, 2016 09 02

Rio de Janiero— The **group arrested in July by the Federal Police [PF] within the framework of Operation Hashtag under suspicion of planning terrorist attacks in Brazil thought of using chemical weapons during the Olympic Games**. The plan was to contaminate a water supply station. "A great opportunity to kill Americans, Iranians, Shi'is, Saudi Arabians, etc," said a member of the group. The plans were discussed by email and the Telegram application, among the members of the closed group Jundallah (Soldiers of God, in Portuguese), upholding the Islamic State. Fifteen suspects were arrested between 21 July and 11 August. Spread out in seven states, the group started to be monitored in March with the infiltration of an informant in the discussions of the group, after the PF received an alert from the FBI. Alisson Luan Oliveira, whose profile user name is Allison Musab, posted on Telegram the mass extermination proposal. Alisson suggested a pogrom based on a provocation by another member of the group, Mujahid Joelson Abdu-Salvador, possibly from Angola, according to the PF. "Won't there be any present for the kuffar [infidels] in these Olympics?" he wondered. "Your possibility of reaching Allah's paradise is in those Olympics," Abdu-Salvador insisted. If the biochemical attack did not work, Hortencio Hioshitake, who identifies himself as Teo Yoshi, suggests instead an attack similar to the one perpetrated in the United States in 2013, which left three dead and 264 injured. "Or do like the Chechens did during the Boston Marathon." "You guys know how to make homemade bombs, right?" Mara Salvatrucha (name of a gang that operates in the US and Central America) wondered. In response, Teo Yoshi says that these things have to be done secretly and warned that they are being watched by the **ABIN (Brazilian Intelligence Agency) and the PF.**

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

07-09-2016 to/au 13-09-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Government use of surveillance devices must be restricted: privacy experts
Globe and Mail, Colin Freeze, 2016 09 13
Toronto - **Canada must acknowledge, and then constrain, the government's use of portable surveillance devices** that can indiscriminately dredge data from people's smartphones without them knowing, privacy experts say. Everything that is known or suspected about the government's use of these machines - called "**IMSI catchers**," "cell-site simulators" or "Stingrays" - is chronicled in a comprehensive, first-of-its-kind, 130-page report written by privacy experts and released to The Globe and Mail. Federal police have used these devices for more than a decade, but the practice was confirmed only this year in a series of stories in The Globe. Now, researchers Christopher Parsons and Tamir Israel say it's time for civil society to debate the pros and cons of IMSI catchers, even if many government agencies still won't discuss them. "This ongoing secrecy has the effect of delaying important public debates," the report says. The report was commissioned by the Telecom Transparency Project and the Canadian Internet Policy & Public Interest Clinic. The **report follows Public Safety Minister Ralph Goodale's announcement last week that he is soliciting the public's views on the powers of police and spy agencies**. Other countries, such as Germany, have been more open about their use of IMSI catchers. An "IMSI," which stands for "international mobile subscriber identity," is a unique serial number now affixed to every smartphone's chip set. It is one of several digital identifiers that police build modern investigations around if they can tie a specific number to a specific suspect.

Fonctionnaires fédéraux en voyage : attention aux espions
Radio-Canada - Nouvelles (site web), Catherine Lanthier, 2016 09 12
Ottawa - « **La menace qui pèse sur vous en tant que fonctionnaire canadien en voyage officiel est bien réelle. » Le Service canadien du renseignement de sécurité (SCRS) vient tout juste de mettre à jour ses directives sur les voyages à l'intention des fonctionnaires fédéraux**. Obtenu par Radio-Canada Ottawa-Gatineau, ce document interne d'une quarantaine de pages insiste sur l'importance pour les employés du gouvernement d'être extrêmement prudents à l'étranger. Le SCRS soutient que « la menace terroriste qui pèse sur les Canadiens a changé » depuis les attaques survenues à Saint-Jean-sur-Richelieu et au Parlement canadien en octobre 2014.

Why the former CSIS director says the Liberals shouldn't touch Bill C-51
Global News, Monique Muise, 2016 09 12
Ottawa—The **former director of Canada's Security Intelligence Service says Bill C-51 should remain untouched**. He does, however, support the government's plan to re-examine the controversial piece of anti-terror legislation. "I would leave it as it is, but as a Canadian, I'm glad the government's carrying through on its promise to review things," **Richard Fadden** told the West Block's Tom Clark this weekend. "(Bill C-51) has been in effect for a while now, so Parliamentarians and others will be able to see the good, the bad and the ugly." Last week, the Liberals formally announced a review of the law as part of an overall consultation on national security. Fadden said he is aware that many Canadians have concerns about parts of the law that allow agencies and government bodies to share information. Privacy is an important consideration, he acknowledged, but it must be balanced with security.

Protocoles de partage d'informations entre le SCRS et ses partenaires
TVA Nouvelles, Michelle Lamarche, 2016 09 10
Ottawa - **Les espions du Service canadien du renseignement de sécurité (SCRS) ont peut-être la possibilité de perturber des actes terroristes potentiels, mais ils ont aussi l'obligation de partager l'information avec leurs partenaires**. Depuis que la loi antiterroriste confère aux espions le pouvoir d'interrompre des actes criminels, le SCRS a mis en place des protocoles pour informer les agences fédérales, comme la Gendarmerie royale canadienne (GRC) et Affaires mondiales Canada.. Des documents obtenus par le «Globe and Mail», grâce à l'accès à l'information, indiquent qu'à l'instar de la GRC, Affaires mondiales Canada et le SCRS ont ratifié un protocole facilitant le partage de l'information. La loi antiterroriste permet aux espions du SCRS d'intervenir pour arrêter un acte terroriste. Ils peuvent, par exemple, geler des avoirs, intercepter des biens, stopper des déplacements, interrompre des communications. La loi C-51 est entrée en vigueur en juin 2015. En mars dernier, le directeur du Service canadien de renseignement de sécurité, **Michel Coulombe**, expliquait que son département avait utilisé ces pouvoirs de perturbation à plus d'une vingtaine de reprises.

CSIS to brief other agencies on operations
Globe and Mail, CSIS to brief other agencies on operations, 2016 09 09
Ottawa - A **controversial law that allows Canada's spies to engage in terrorism-disruption campaigns may pose problems for federal police and diplomats**. For this reason, they are being given a peek at some CSIS operations - and even allowed to challenge them. Newly released records suggest that Bill C-51, the controversial 2015 omnibus bill that overhauled the Canadian Security Intelligence Service, has sent ripples throughout the federal-security bureaucracy. CSIS's so-called "threat-reduction activities" (or TRAs) have prompted fears of unintended fallout. To mollify concerns, the spy agency has committed to giving potentially affected agencies a heads up about what it is doing, according to records recently released to The Globe and Mail via access to information laws. For example, an "enhanced consultation memo" was recently signed between CSIS and Global Affairs Canada. While much is redacted in the undated document, CSIS promises to loop in foreign-affairs functionaries about things it is doing. "The Service will provide intelligence assessments ... of TRA measures which have a foreign policy component." On Nov. 24, 2015, **CSIS Director Michel Coulombe and RCMP Commissioner Bob Paulson cosigned a memo where they agreed to have their lieutenants brief each other on counterterrorism probes**. CSIS's "new mandate to reduce threats" could potentially increase the likelihood of the agencies "adversely affecting each other." Mr. Coulombe, the spy chief, told Parliament in March that such powers have been exercised only a couple of dozen times since the bill passed. Prior to that, he once testified that C- 51 could allow CSIS to "go into disrupting a financial transaction," or "disabling a mobile device" or "tampering with equipment."

Anti terror revamp to stretch into next year as Liberals launch consultation
Canadian Press, Jim Bronskill, 2016 09 08
Ottawa - The **Liberal government's promised changes to a controversial anti-terrorism law likely won't come until next year**, once officials have digested an array of public suggestions on revamping national security. The government opened an online consultation Thursday, soliciting feedback on everything from sharing information and **preventing attacks to conducting surveillance and ensuring intelligence agencies are accountable**. Public Safety Minister **Ralph Goodale** told a news conference in Edmonton the government also hopes House of Commons and Senate committees will hold public hearings on the national security framework. It means any legislation flowing from these reviews would not be tabled until December at the earliest and more likely in late winter or spring 2017. In the 2015 election campaign, the Liberals promised to repeal ``problematic elements'' of omnibus security

legislation, known as Bill C-51, ushered in by the previous Conservative government. The bill gave the **Canadian Security Intelligence Service** explicit powers to disrupt terrorist threats, not just gather information about them. The Trudeau government has committed to ensure all CSIS warrants respect the Charter of Rights and Freedoms, preserve legitimate protest and advocacy and define terrorist propaganda more clearly.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

Obama to be urged to split cyberwar command from the NSA
Washington Post, Ellen Nakashima, 2016 09 13
Washington— The **Pentagon and intelligence community are expected to recommend soon to President Obama that he break up the joint leadership of the National Security Agency and U.S. Cyber Command to create two distinct forces for electronic espionage and cyberwarfare**. The potential move is driven by a sense that the two missions are fundamentally different, that the nation's cyberspies and military hackers should not be competing to use the same networks and that the job of leading both organizations is too big for one person. Obama was on the verge of ending the "dual-hat" leadership in late 2013, but was persuaded to hold off when senior officials, including then-NSA Director Keith B. Alexander, argued against it on the grounds that **CyberCom** was still too dependent on NSA's capabilities to succeed on its own. Three years later, Defense Secretary Ashton B. Carter and Director of National Intelligence James R. Clapper are pressing for the split, with Carter seeking to build Cyber Command into a full-fledged fighting force that has its own network accesses to conduct attacks. Clapper, officials said, supports the idea in part to reduce tension over which force gets to use the networks — the spooks or the warfighters.And with the White House apparently eager to get it done before Obama's term ends, officials said that the decision appears all but certain.

Former CIA chief who urged Iraq war signs on as Trump adviser
Reuters, 2016 09 13
Washington--**Former CIA Director James Woolsey**, a vocal advocate of the 2003 U.S.-led invasion of Iraq who promoted allegations that Saddam Hussein harbored illegal weapons, **will serve as a senior national security adviser to Republican presidential candidate Donald Trump**, the campaign announced on Monday. Woolsey's hiring contrasted with Trump's repeated assertions that he was a stalwart opponent of the invasion, although he initially supported it. In the announcement, Woolsey said he supports Trump's plan to expand the U.S. military, which calls for ending Pentagon budget caps and spending billions of dollars for additional troops, ships and aircraft. "Mr. Trump's commitment to reversing the harmful defense budget cuts signed into law by the current administration, while acknowledging the need for debt reduction, is an essential step toward reinstating the United States' primacy in the conventional and digital battlespace," Woolsey said.

CIA director: Country is safer from large-scale terror attacks than on 9/11
CBS News, Emily Schultheis, 2016 09 12
Washington--As the **United States commemorates the 15th anniversary of the 9/11 terror attacks Sunday, CIA Director John Brennan said the country is far more secure today against large-scale terror attacks than it was that day in 2001**. "We've learned a lot, we've

done a lot," he said on CBS' "Face the Nation, citing increased cooperation on intelligence and national security issues. "And that's why today I believe it's much more difficult for these groups to carry out the type of attack that they did 15 years ago." Speaking about the fight against ISIS, Brennan said the U.S. and its allies have made significant inroads in the fight against the terror network. He pointed to territorial gains over the last "six to nine months" in the Middle East, as well as efforts to combat ISIS' spread in regions like West Africa or Asia, as proof that there's progress being made.

U.S. Adds New Task in Hostage Talks: Caring for the Families (Canada)
New York Times, Adam Goldman, 2016 09 12
Washington--When the United States became aware late last month of a **video showing an American woman and a Canadian man pleading to be saved from their Taliban captors**, the government did something it had not done well in the past. Before the video became public, a new hostage team led by the Federal Bureau of Investigation quickly alerted the couple's families to brace for the chilling footage. **The effort reflected a sweeping change in how the government handles hostages, a shift ordered last year by President Obama after hostages' families complained of officials' callousness and poor communication**. The new hostage team faces no small task as Americans continue to move through the world's many war zones. Officials say that more than 70 hostages who are Americans or legal permanent residents of the United States have been freed since the revamped effort came together at the F.B.I. headquarters, but it is unclear whether there has been any change in the rate that captives have been rescued. Members of the F.B.I.-led team and their counterparts at the State Department are still trying to bring home more than a dozen people, officials said.

FBI's directive quickly switched to cover terrorism
USA Today, Kevin Johnson, 2016 09 12
London--Five separate times during a short car ride with the two men he thought were his confederates, James Medina left little doubt about his resolve to bomb a south Florida synagogue as a bloody expression of his support for the Islamic State. "You know," the 40-year-old Hollywood, Fla., man allegedly said earlier this year. "It's my call of duty. And whatever happens, it's for the glory of Allah!" The subsequent criminal complaint outlined a now-familiar plot line in which government informant and undercover agent infiltrate an alleged criminal network and win the confidence of a suspected terrorist whose journey now ends more often than not in shackles. **Sting operations always have been a staple of FBI criminal investigations, dating to the federal government's earliest infiltration of the mafia and other organized crime networks. But its broad and controversial application in terror inquiries is the manifestation of a daunting directive issued in the aftermath of 9/ 11 attacks and a reflection of the evolving threat.** Pondering the very existence of the FBI in the post- 2001 world, the 9/11 Commission, created by Congress in the aftermath of the catastrophic assaults, urged the bureau to find its way into the then- unfamiliar culture of a new enemy embracing radical Islam that continues to represent an unparalleled threat.

Crafty world of cyberespionage
Washington Post, Dina Temple-Raston, 2016 09 11
Book Review: Not long ago, **a former National Security Agency director sat down with a mathematician who had come to work for him - and a pop quiz quickly ensued. "What's the most important thing about encryption?"** the mathematician asked the head of the NSA. "Scrambled text," his boss replied, thinking that preventing the enemy from reading a coded message was paramount. "Wrong," the visitor said. "The single most important thing is attribution." Attribution is so important, he continued, because only one person can give the order to fire nuclear weapons - the president - so it is critical to know that the order is coming

from him and no one else. "What's the second most important thing about encryption?" the mathematician continued. "Scrambled text," the director said hopefully. "No. It is the integrity of the data." That's because, he explained, a corrupted message, with a single digit wrong, could cause a nuclear missile to be launched at the wrong target. So begins just one of the fascinating episodes that appear in **BBC journaist Gordon Corera's terrifically engrossing new book, "Cyber Spies: The Secret History of Surveillance, Hacking, and Digital Espionage."**

FBI agent climbed the ranks but chose to end his career back in a field office
Washington Post, Ellen Nakashima, 2016 09 11
Baltimore - **Kevin Perkins, a 30-year-veteran of the FBI, says he's lucky to have been shaped by "two different organizations" -- the old-school bureau of J. Edgar Hoover and the one that grew out of the horrific terrorist attacks of Sept. 11.** The 2001 al-Qaeda assault changed the FBI into the agency we know today, focused not only on busting crime but also on using intelligence to prevent terrorist attacks. It also marked the midway point of Perkins's 30-year career that took him from investigating banking fraud in the 1980s to running the bureau's criminal investigative division to serving as associate deputy director -- the third-highest ranking official. And finally, to reassuming the leadership of the Baltimore field office. "The guys who taught me the ropes in the mid-'80s had all been hired by Hoover, working everything from bank robberies to Cosa Nostra and Mafia cases," he said. When he reached the management ranks, he said, "I had a front-row seat as a straphanger, sitting and watching bureau leadership make decisions after 9/11."

No looking back: the CIA torture report's aftermath
The Guardian (London), Spencer Ackerman, 2016 09 11
Analysis: "I want to be absolutely clear with our people and the world. The United States does not torture," said George W Bush on 6 September 2006. Bush was, for the first time, acknowledging the existence of the program that Senate intelligence committee staff investigator **Daniel Jones** would later expose as taking power drills to the heads of captured men; making them stand with their arms stretched above their heads for days at a time; leaving at least one of them naked until he froze to death; waterboarding them to the point of catatonia as bubbles rose from their open mouths; and inserting pureed food into their rectums while claiming it was necessary for delivering nutrients. **Details of those procedures were outlined in the 525 pages which CIA director John Brennan, Barack Obama and White House chief of staff Denis McDonough allowed to become public.** The CIA's response to Jones's report was split into two corps, one official and one not. The agency itself would no longer defend torture outright because that would contradict the Obama White House's position on the unacceptability of torture. Instead, the agency would say that tortured men produced valuable intelligence, just not necessarily as the result of torture, and that the Senate could not definitively prove the torture did not produce valuable intelligence. Brennan gave a press conference following the release of the report in December 2014. It began with him spending five minutes reciting the unfolding developments of the 9/11 **terrorist attacks and crescendoed with him calling the relationship between torture and useful intelligence " unknowable** ". Jones' boss, the driving force behind the report, California Democratic Senator Dianne Feinstein unexpectedly live- tweeted responses to Brennan's press conference as it progressed, creating the hashtag #ReadTheReport.

NSA's early Cold War struggles
Washington Post, David E. Hoffman, 2016 09 11
Book Review: The "one-time pad" is a simple but secure way to encipher a message. The text of the message is converted into numbers using a page of code. When the recipient gets the message, it is deciphered using the identical code. The page of code is used only once and

then torn from the pad and discarded, never to be used again. It is nearly impossible to break and was used effectively by the Soviet Union in the final years of World War II and just after. Code-breakers in the U.S. Army and Navy despaired at the difficulty of cracking it. "If the standard work of a codebreaker was looking for the proverbial needle in a haystack, the Russian problem required finding a wisp of straw in a haystack," **Stephen Budiansky writes in "Code Warriors," his richly detailed look at the rise of the National Security Agency and its long struggle to penetrate Soviet communications in the Cold War. Budiansky does an admirable job of depicting the early years of the NSA, but he runs up against walls of secrecy that still surround the history of code-breakers and snoops in the final stages of the great confrontation between East and West.** After using one-time pads successfully during World War II, the Soviet communications people got careless. They used some a second time, "an astonishing and monumental security blunder," Budiansky recalls.

A DC mystery behind a 9/11 newspaper column
CNBC News, Eamon Javers, 2016 09 11
Washington - On Wednesday, an alarming headline appeared on the website of **USA Today atop an opinion column written by former Homeland Security Secretary Tom Ridge. "15 years after 9/11, a gaping security gap,"** it said. The column was perfectly timed, coming just four days before the anniversary of the attack on the United States -- a moment when the tragedy was certain to be on the minds of millions of Americans. And Ridge, a former governor of Pennsylvania, had a tough message for his readers: America is not safe. "There remains a gaping hole in our national security preparedness, coming from a largely ignored source," Ridge wrote. The threat on Ridge's mind doesn't come from ISIS-inspired killers inside the United States, as in the recent attacks in Orlando and San Bernardino. Instead, the threat Ridge wrote about comes from the post office. Parcels coming into the United States are not adequately screened for threats from overseas, Ridge argued, leaving a dangerous security gap that could be exploited by terrorists. In the column, **Ridge said he was joining a new group called "Americans for Securing All Packages." That's something of a mystery**. But a little digging reveals a small example of the way money, power, and national security interact in Washington 15 years after the Sept. 11, 2001, attacks. On its website, Americans for Securing All Packages features a "Who We Are" section explaining that the group is a "coalition of families, health care advocates, security experts, businesses and non-profits who believe it is time to close a dangerous security gap that leaves our nation vulnerable to foreign attacks and invites illegal and toxic drugs into our communities." The group -- a nonprofit that does not have to disclose its donors -- officially debuted on the same day Ridge's column appeared.

The Time U.S. Spies Thought Al Qaeda Was Ready to Nuke D.C.
The Daily Beast, Shane Harris, 2016 09 10
Washington - On Christmas Eve 2003, **Gen. Michael Hayden, the director of the secretive U.S. National Security Agency, made a secure phone call to his British counterpart, David Pepper, the director of the Government Communications Headquarters. "Happy Christmas, David," Hayden said, speaking to Pepper from NSA headquarters at Ft. Meade, Md., about 20 miles from the Capitol in Washington, DC. Such social calls weren't unusual.** The **NSA and GCHQ** were the closest of allies in a global hunt for the phone calls, emails, and other electronic communications of spies and terrorists. But Hayden had more on his mind than season's greetings. In recent days, the NSA had been collecting what Hayden would later describe as a "massive amount of chatter"--phone calls and emails from terrorists--that suggested al Qaeda was planning multiple attacks inside the United States, timed to the holidays. "One more thing, David," Hayden said after the two men exchanged pleasantries. "We actually feel a bit under threat here. And so I've told my liaison to your office that should there

be catastrophic loss at Ft. Meade, we are turning the functioning of the American [signals intelligence] system over to GCHQ."

Intelligence Community 'Quite Upset' Over Donald Trump's Comments About Briefing, Says Retired Col. Steve Ganyard
ABC News, Liz Stark, 2016 09 10
Washington - **Former Deputy Assistant Secretary of State Col. Steve Ganyard said Donald Trump's comments about his classified intelligence briefing this week troubled some in the intelligence community**, saying, "Our friends in the intelligence community were quite upset to hear that sort of talk." "I think if there was any discomfort, it was not signaling any personal preference or policy. It was more because they understood that what they were saying might be used against them in a way that was untrue," he said, in response to Trump's claim that his briefers' body language revealed their frustration with President Barack Obama's leadership. Ganyard, who attended classified briefings while working at the State Department, joined this week's episode of the "Powerhouse Politics" podcast with ABC News White House correspondent Jonathan Karl and ABC News political director Rick Klein to discuss Trump's inflammatory comments about his latest intelligence briefing and possible ties to the Russian government.

Lunch with the FT: Edward Snowden, the world's most famous whistleblower
Financial Times, Alan Rusbridger, 2016 09 10
London - **Edward Snowden** has rounded on his hosts, attacking the Kremlin's human rights record and implicating Russia in two of the US government's latest major security hacks. In a Lunch with the FT -- carried below -- he complained Moscow had "gone very far, in ways that are completely unnecessary, costly and corrosive to individual and collective rights" and added that his greatest loyalty was still to the US. He **described the leak last month of NSA espionage tools, potentially by Russia as an "implicit threat" to the US government**. Efforts by hackers called the Shadow Brokers to auction off NSA computer code used to break into foreign networks were an attempt to show Washington how vulnerable it was, he added. Edward Snowden is not the easiest lunch date. The former National Security Agency operative doesn't fancy talking in a Moscow restaurant so -- via an intermediary -- we settle on meeting in my hotel and risk the room service. He will present himself at the agreed time. That's all I need to know. In the end he's 20 minutes late, dressed casually in black jeans and black V- neck, buttoned-up T-shirt carrying a pair of unbranded dark glasses. He eyes up the small, dimly lit room 203 of the Golden Apple "boutique" hotel -- half an hour's gentle stroll from the Kremlin -- with the look of a man who has spent too much time in such places. How does it compare with room 1014 of the Mira Hotel in Hong Kong, where in June 2013 -- having shared many of the NSA's most closely guarded secrets with a few handpicked journalists -- Snowden spent a week as the most wanted man in the world? "A bit smaller, but not dissimilar," he says.

CIA Chief: IS Likely to Remain in Iraq, Syria for Years
Voice of America, Elizabeth Cherneff, 2016 09 09
Washington - **Despite the shrinking of Islamic State-held territory in Iraq and Syria, the head of the Central Intelligence Agency is stressing that the group's influence is not going away anytime soon.** "I think ISIL [Islamic State] will remain a presence inside Iraq and Syria for quite a while," **CIA Director John Brennan** said Thursday during a national security summit in Washington. Brennan also highlighted the lasting impact of foreign fighters attempting to return to their home countries.

Spy games meet word games as officials warn Russia against election meddling
Baltimore Sun, Ian Duncan, 2016 09 09

Washington - **When some of the nation's top spies joined each other on stage at a conference Thursday, the question of whether Russia was behind the hacking of the Democratic National Committee and state elections systems soon came up**. The spies carefully skirted the question. We're working with our partners on it, **CIA director John Brennan said. It's really a policy question, NSA director Adm. Michael Rogers** said. "I'm going to continue the streak of not talking about that," FBI director James Comey said. Then he went on to talk about it in a rather backhanded way. The intelligence officials' comments Thursday mirrored those of other top government leaders this week as the United States tries to figure out what to do about what is widely suspected to be Russian meddling in the upcoming election without saying publicly the Kremlin is behind the attacks.

U.S. Voting System So 'Clunky' It Is Insulated From Hacking, FBI Director Says
Wall Street Journal, Devlin Barrett, 2016 09 09
Washington - The **head of the Federal Bureau of Investigation sought to calm fears that Russians or others could electronically sabotage** the nation's election in November, saying the 50-state voting system is so dispersed and "clunky" it would be difficult for hackers to affect the outcome. Appearing at a panel with other senior U.S. intelligence officials Thursday, **FBI Director James** Comey was asked about the concerns that hackers acting on behalf of the Russian government might try to manipulate the presidential election. "The beauty of the American voting system is that it is dispersed among the 50 states, and it is clunky as heck," said Mr. Comey. "A lot of people have found that challenging over the years, but the beauty of that is it's not exactly a swift part of the internet of things, and so it is hard for an actor to reach our voting process."

What Really Happened at Donald Trump's Intelligence Briefing
NBC News, Ken Dilanian, Robert Windrem, 2016 09 08
Washington - **As U.S. officials cast doubt on Donald Trump's claim he read the "body language" of intelligence officials at a recent briefing, NBC News has learned exclusive details of what unfolded in the room -- one of Trump's advisers repeatedly interrupted the briefers until Chris Christie intervened,** sources said. The Aug. 17 briefing is attracting fresh scrutiny after Trump said at NBC's Command-in-Chief Forum that he divined that intelligence officials were "not happy" with President Obama. However, a U.S. official pointed out that intelligence officers don't give policy advice, so it would be inaccurate to say that Obama failed to follow the advice of the intelligence community. A second U.S. official said analysts are trained not to allow their body language to betray their thinking. Meanwhile, four people with knowledge of the matter told NBC News that one of the advisers Trump brought to the briefing, **retired general Mike Flynn**, repeatedly interrupted the briefing with pointed questions. Two sources said Christie, the New Jersey governor and Trump adviser, verbally restrained Flynn -- one saying Christie said, "Shut up," the other reporting he said, "Calm down."

It's unlikely Trump briefers disparaged Clinton or Obama, ex- intelligence officials say
Washington Post, Greg Miller, 2016 09 09
Washington - **Did U.S. intelligence analysts betray disdain for President Obama and Hillary Clinton during recent classified briefings with Donald Trump, as the GOP candidate claimed Wednesday? Doing so would represent an almost inconceivable violation of training and tradition, former U.S. intelligence officials said**. They added, however, that those accused briefers may be quietly muttering and shaking their heads about at least one of the presidential candidates now. "Those selected for this task would have been the most professional of an elite corps of intelligence officers," said Paul Pillar, a former high-ranking CIA analyst. "One of the last things they would do is express either verbally or through body- language preferences" about candidates or policy. **Michael Morell**, a former deputy CIA

director who has endorsed Clinton, put it more bluntly, saying that Trump's comments "show that he's got zero understanding of how intelligence works." Trump was accompanied during his initial Aug. 17 briefing by New Jersey Gov. Chris Christie (R) and retired U.S. Army Lt. Gen. Michael Flynn, both avid supporters.

Men who allegedly hacked top government officials arrested
Washington Post, Rachel Weiner, Ellen Nakashima, 2016 09 08
Washington - **U.S. authorities have arrested two North Carolina men accused of hacking into the private email accounts of high-ranking U.S. intelligence officials**. Andrew Otto Boggs, a.k.a. "INCURSIO," 22, of North Wilkesboro, N.C., and Justin Gray Liverman, a.k.a. "D3F4ULT," 24, of Morehead City, N.C., were both arrested Thursday morning and will be extradited next week to the Eastern District of Virginia, where federal prosecutors have spent months building a case against a group that calls itself Crackas With Attitude. Along with Boggs and Liverman, authorities say the group included three teenage boys. One, a 17-year-old Briton, was arrested in February. The hacking collective has claimed to have gained access to the **private email accounts of CIA Director John O. Brennan and Director of National Intelligence James R. Clapper Jr**. The group regularly bragged about its escapades to reporters, explaining its methods and providing evidence of its activities. According to U.S. officials, the group also hacked into the accounts of former FBI deputy director Mark Giuliano; Amy Hess, the FBI executive assistant director for science and technology; Gregory Mecher, who is married to White House communications director Jen Psaki; and Harold Rosenbaum, chief executive of the CIA contractor Centra Technology.

DHS secretary: Ballot counts are largely safe from cyberattack
Politico, Jennifer Scholtes, 2016 09 08
Washington - **Homeland Security Secretary Jeh Johnson said Thursday it would be very difficult for hackers to alter Election Day ballot counts**. "It is so decentralized and so vast," the secretary said during a forum hosted by The Atlantic. "You've got state governments, local governments, county governments involved in the election process. It would be very difficult to alter the count." Johnson said federal officials are generally concerned, however, about the potential for state actors, hacktivists or cyber criminals to manipulate or interfere with online state election systems.

A View from the CT Foxhole: An Interview with John Brennan, Director, CIA
Combating Terrorism Center at West Point, Paul Cruickshank, Brian Dodwell, 2016 09 07
Interview - **Combating Terrorism Center: What is the intelligence picture with regard to al-Qa`ida attempting to move back into Afghanistan on the coattails of the Taliban? CIA Director John Brennan: Well I think if we believe that a lot of al-Qa`ida migrated into Pakistan over the last 15 years, they haven't done too well there**. And I think they are still searching for a place where they can feel more secure, and there are areas inside of Afghanistan that they believe may provide greater security because the Taliban may control certain areas. I think it's only going to be a temporary respite from the counterterrorism pressures that they're feeling. We see the number of Afghan forces that have died in combat going up. Yes, that's a reflection of increased fighting, but it also shows that it's Afghans who are fighting for their country once again. So if al-Qa`ida decides to move over into Afghanistan, I think they do so with some trepidation as well as uncertainty about what their future's going to hold. CTC: What's the current assessment of the Islamic State's capability to put together international terrorist attacks? Brennan: I think what they have demonstrated is the ability to put together a diversified investment portfolio, for lack of a better term. So it runs the gamut in terms of types of things that they're trying to gain traction with.

FBI, DHS issue advisory to law enforcement on possible terror targets
CBS News, Staff report, 2016 09 08
New York - The **FBI and the Department of Homeland Security (DHS) have issued a joint bulletin to law enforcement nationwide advising vigilance of civilian facilities as possible targets by ISIS inspired terrorists**, CBS News senior investigative producer Pat Milton reported. The bulletin, sent out on Aug. 31, said analysis indicates that homegrown violent extremists, and ISIS inspired terrorists, appear to have shifted their focus to target attacks on civilian venues. These sorts of venues include places like restaurants, theaters, churches, and sports arenas, with less focus on law enforcement, military and government facilities. The bulletin said that according to analysis, more than 75 percent of homegrown violent extremists disruptions and attacks over the last 12 months have focused on civilian targets, Milton reported.

Trump says intelligence officials' 'body language' showed they were unhappy with Obama
Washington Post, Karen DeYoung, 2016 09 08
Washington - **Donald Trump said Wednesday that he could tell from the "body language" of intelligence officials** who gave him two separate briefings on U.S. national security in recent weeks that they were "not happy" with what he described as the failure of President Obama and others in the administration to "follow what they were recommending." Trump said he "didn't learn anything" from the briefers that would change his views on how to defeat the Islamic State. He said earlier this week that he would task senior military officials with giving him a plan to deal with the militants within 30 days after he takes office. " **Timothy Barrett, spokesman for the Office of the Director of National Intelligence, which has briefed both Trump and Democratic presidential nominee Hillary Clinton, declined to comment on Trump's remarks.**

DHS secretary Johnson vows 'no stone unturned' on election security
Politico, Nick **Gass, 2016 09 06**
Washington - Faced with the potential threat of an election compromised by foreign hackers, Homeland Security Secretary Jeh Johnson on Tuesday sought to reassure Americans, pledging to "leave no stone unturned" when it comes to ensuring the integrity of the process. "Well first, we have a lot of confidence in the integrity of the election process itself," Johnson told MSNBC's "Andrea Mitchell Reports." "There are some 9,000 state and local jurisdictions that are involved in the election process, including national elections, we've looked at a fair amount of it. We've looked at what states and cities do." Johnson went on to say that "we have a lot of confidence in the process itself, we're in the mode now of wanting to leave no stone unturned, and so, what DHS, my department, has been going over the last several weeks is contacting state election officials to say, we want to leave no stone unturned."

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

Rendition victims challenge decision not to prosecute MI6 officer
The Guardian (London), Ian Cobain, 2016 09 12
London--**Lawyers representing a Libyan husband and wife who were kidnapped and flown**

to one of Muammar Gaddafi's prisons are seeking to overturn a decision that there was insufficient evidence to prosecute a former MI6 officer for his alleged role. Mark Allen, the head of counter- terrorism at the agency at the time of the so-called rendition operations, had set out his role in a letter to the Gaddafi government that came to light during the 2011 Libyan revolution. However the Crown Prosecution Service decided earlier this year that Allen - now Sir Mark - should face no criminal charges, a ruling that the victims said reflected poorly on British justice. Lawyers for the couple are now seeking a judicial review of the CPS decision, which they have denounced as a "see no evil, hear no evil" ruling that has put the government and its intelligence agencies above the rule of law.

British spy uncovered Hitler's secret war deal with Franco
London Times, Graham Keeley, 2016 09 12
London--An **MI6 spy discovered a secret deal between Hitler and General Franco about Spain entering the Second World War, prompting Churchill to bribe Spanish generals and business leaders to stay loyal to Britain**, a new book reveals. The spy, known as **Agent T,** was able to disclose what had been agreed between the Führer and Franco when they met in Hendaye in southwest France, in 1940. The meeting was to discuss the terms on which Spain might join Germany in the war against Britain.

'Met ignored extremism among my fellow Muslim officers'
Sunday Times (UK), Richard Kerbaj, 2016 09 11
London - A **former counterterrorism sergeant has attacked the Metropolitan police for failing to tackle extremist views among some of its Muslim officers for fear of being labelled "Islamophobic". Javaria Saeed**, a practising Muslim who worked in Scotland Yard's counterterrorism division, complained to her bosses after she witnessed a fellow Muslim officer saying female genital mutilation (FGM) -- illegal in the UK since 1985 -- was a "clean and honourable practice " and "shouldn't be criminalised". The same officer, a Muslim constable in the SO15 counterterrorism unit, also said female Muslim victims of domestic violence should not appeal to the police for help, but resolve their cases in a sharia court, except in "serious violent cases", according to Saeed.

Brexit won't harm UK security, says US former spy chief
The Scotsman, 2016 09 11
London - **Brexit will not make "one bit of difference" to Britain's intelligence relationship with the rest of Europe and the US, according to a former senior official with the National Security Agency. William Binney**, a technical director for the US intelligence agency turned whistleblower, said **GCHQ will continue to share data and resources with organisations around the world** following Britain's retreat from the EU. In an interview with Scotland on Sunday, Binney also warned that the UK Government's Investigatory Powers Bill is a guarantee of "failure" that will overlook intelligence about future terror attacks. The veteran intelligence official will be in Edinburgh this week for the UK premiere of A Good American, a documentary about his time in the NSA, which he believes could have prevented the 11 September, 2001, terror attacks. He spearheaded the development of ThinThread, a selective surveillance programme which, he says, would have flagged up the perpetrators of 9/11, but the system was jettisoned in favour of Trailblazer, a "bulk data" collection scheme that left analysts overwhelmed.

Return to Table of Contents/ Retour à la table des matières

Australia / Australie

Rampage sparks terror tips surge
Adelaide Advertiser, Simon Benson, 2016 09 13
Adelaide - **Intelligence officials have revealed that calls from the public to the national security hotline spiked 50 per cent in the 24 hours after the alleged ISIS-inspired lone wolf terrorist attack at the weekend**. The **deluge of tip-offs to ASIO and the Australian Federal Police has also risen about 40 per cent since April, to almost 70 a day**, The Advertiser can reveal. As the Government grapples with the rising terrorism threat, frightening CCTV footage has captured knife-wielding suspect Ihsas Khan on his bloody rampage - and how victim Wayne Greenhalgh, 59, didn't stand a chance. Mr Greenhalgh was stabbed repeatedly, losing some fingers and suffering deep puncture wounds to his chest and neck, as he walked his dog in the Sydney suburb of Minto on Saturday. He remains in a serious condition in hospital. Taken from inside a Minto hair salon, the footage shows Khan, 22 - who friends say was "lost in his own world" - hunt down Mr Greenhalgh.

United we stand: intelligence ties 'key to safety'
The Australian, David Crowe, 2016 09 08
Vientiane - **Australia will seal a major defence alliance with Singapore next month** by giving the city-state's leader a rare invitation to address federal parliament, cementing a $2 billion agreement as terror attacks and China's maritime claims fuel anxiety over regional security. Malcolm Turnbull has asked his Singaporean counterpart, Lee Hsien Loong, to address the joint sitting of parliament in early next month during an official visit that will formalise the deployment of 14,000 troops from Singapore to Australia every year. **The Prime Minister will also tighten security co-operation with another key neighbour today, offering Indonesian president Joko Widodo more access to valuable intelligence on foreign fighters who pose threats to the region** -- and warning that Asia should learn from the failure in Europe to share information. The security initiatives come as Mr Turnbull meets leaders at the East Asia Summit in Laos against the backdrop of North Korean missile tests off the coast of Japan and a push by China to dissuade the gathering from rebuking it about its militarisation of the South China Sea. The summit includes the Association of South East Asian Nations members, Australia and major regional powers such as China, Japan and the US. This year's meeting concludes tonight.

"Flaws" in govt anti-terror funding round
Australian Associated Press, Rashida Yosufzai, 2016 09 07
Canberra - **Federal Labor has seized on a scathing audit outlining flaws on how the federal government picked organisations to help prevent radicalisation**. Only 21 of the 42 programs awarded almost $1 million in funding as part of a **counter-terrorism strategy** should have been successful, the Australian National Audit Office said. That's if the Attorney-General's Department had picked those that properly met the criteria needed for funding. The initiative was about backing community-based and non-government groups to help people steer away from violent extremism. But the department pushed through 46 of the 59 applications that did not properly meet the criteria - which led to 10 of those being fully approved. The report said the process through which applications were given funding was flawed in "significant respects". As well, many of the funded organisations have yet to indicate whether they'll register onto a directory connecting people at risk of radicalisation with help - a key requirement.

ASIO evidence at siege inquest kept secret
Australian Associated Press, Daniel McCulloch, 2016 09 07

Sydney - **Could Australia's intelligence agency have done more to stop gunman Man Haron Monis before the fatal Sydney Lindt Cafe siege?** A coronial inquest has been examining what the **Australian Security and Intelligence Organisation (ASIO)** knew about Monis and whether it should have taken action against him before he staged the December 2014 siege. All evidence relating to ASIO has been gathered in private, and the information may never be made public, it has been revealed. The inquest has examined whether Monis should have been detected, kept under surveillance or on a security watch list. It has also looked at whether Monis should have been predicted to commit a politically motivated attack, and what role ASIO played during the Martin Place siege.

Govt sets defence innovation priorities
Australian Associated Press, Staff reporter, 2016 09 07
Canberra - The **government has spelled out priorities for improving defence capabilities through clever ideas, with boosting intelligence, surveillance, electronic warfare and cyber heading the list.** Defence Industry Minister Christopher Pyne says the new $640 million Defence Innovation Hub to be launched later this year will drive growth in defence industry innovation. The government has set six areas for research and innovation, with three given top priority for 2016-17. "In the intelligence, surveillance, reconnaissance, electronic warfare, space and cyber capability stream we will focus on improving intelligence collection, analysis and dissemination," he said in the keynote address to the Land Forces conference dinner in Adelaide. Mr Pyne said that would include biometric data and cyber innovation to support intelligence capability development. Next priority is capabilities to better enable defence operations, including command and control systems, satellite communication and simulation.

Return to Table of Contents/ Retour à la table des matières

New Zealand / Nouvelle-Zélande

Spy bill lacking some robust privacy protection
New Zealand Herald, Gehan Gunasekara, 2016 09 07
Op-ed: The **much-anticipated New Zealand Intelligence and Security Bill** is before a Parliament select committee. **There is unlikely to be loud applause from Edward Snowden, however, as the bill does little to address the concerns regarding mass surveillance he exposed in 2013** and the subsequent mischiefs that have come to light including the GCSB spy agencies spying on New Zealand residents. The bill follows the recommendations of the independent Cullen-Reddy Report as to how these should be addressed and it does implement many of them. The devil, however, is in the detail. On the one hand the bill strengthens privacy protections by expanding the number of the Privacy Act's rules that now apply to the intelligence agencies. Thus an individual may complain that information about them that was used, say, in a security clearance, was out of date, inaccurate or misleading, and another may complain that information about them was retained longer than necessary by the intelligence agency. Note: Gehan Gunasekara is an associate professor in commercial law at the University of Auckland and researches and teaches privacy law.

Return to Table of Contents/ Retour à la table des matières

International

China / Chine

China, Canada pledge to boost security cooperation
Xinhua News Agency, Staff reporter, 2016 09 13
Beijing - **China and Canada on Monday pledged to strengthen security cooperation at a high-level dialogue held in Beijing**. It was the first **China-Canada High-Level National Security and Rule of Law Dialogue**, a mechanism established during Canadian Prime minister Justin Trudeau's visit to China from late August to early September. According to a joint statement released after the meeting, the two sides exchanged views on fighting terrorism, cyber crime, organized crime, consular affairs and other issues. The two sides have confirmed their future cooperation framework. Some common goals are expected to be reached under the framework, such as initiating a discussion on an extradition treaty and finalizing an agreement on sharing and returning recovered assets. The dialogue was co-chaired by Wang Yongqing, secretary-general of the Commission for Political and Legal Affairs of the Communist Party of China (CPC) Central Committee, and Daniel Jean, National Security Advisor to the Canadian Prime Minister.

Beijing, Ottawa to work out an extradition treaty
China Daily, 2016 09 13
Beijing— **China and Canada agreed on Monday to start discussions on a bilateral extradition treaty** that would facilitate the return of corrupt fugitive Chinese officials who remain at large in Canada. The agreement was reached at the China-Canada High-Level National Security and Rule of Law Dialogue in Beijing, where discussions were held on ways to improve cooperation on issues such as law enforcement, combating transnational organized crime, judicial cooperation and exchanges on the rule of law.In depth talks of an extradition treaty and the signing of an agreement on sharing the recovered stolen assets will occur in the coming months, while negotiations are finalized on a yearlong memorandum of understanding on a pilot project in which Chinese experts will be invited to help identify Chinese immigrants who use fraudulent means to enter Canada. In recent years, the United States, Canada, Australia and Singapore have become popular destinations for corrupt fugitive Chinese officials. **They lack bilateral extradition treaties and have legal differences with China, complicating their return, according to the Ministry of Public Security.**

Rising Uighur militancy changes security landscape for China
Associated Press, 2016 09 09
Beijing— They have been praised by the leader of al-Qaida and wooed by the head of the Islamic State group. They have distinguished themselves on battlefields in Syria and are accused of carrying out a devastating bombing in Thailand. In **the past two years, militants belonging to the Uighur ethnic group native to the vast Xinjiang region in western China have shown signs of becoming a force in Islamic extremism globally**, a development that is reshaping both the ground war in Syria and Chinese foreign policy.The predominantly Muslim, Turkic-speaking people — ethnically distinct from China's Han majority — have chafed for decades under Beijing's heavy-handed rule. Uighur separatists belonging to the **East Turkestan Islamic Movement (ETIM),** a militant group based in the rugged tribal areas of nearby Afghanistan and Pakistan and allied with al-Qaeda, have been blamed for attacks in Chinese cities, often using crude but effective weapons such as knives, Molotov cocktails and speeding vehicles. **Chinese anti-terrorism expert Li Wei** said the extremist threats that China faces domestically and from abroad are now "inextricably linked, just like with other countries,"

leading China to expand its dealings in Syria and Afghanistan. I think the international community would agree that Syria is a nexus of global jihad that does threaten the entire world," said Li, **director of the anti-terrorism research center at the China Institute of Contemporary International Relations, a think tank under the Ministry of State Security, China's main intelligence agency.**

Return to Table of Contents/ Retour à la table des matières

Russia / Russie

Russian Investigative Committee official Nikandrov subjected to pressure in detention facility – lawyer

Interfax News Agency, 2016 09 12

Moscow— **Denis Nikandrov, deputy chairman of the Russian Investigative Committee's Main Directorate for Moscow, who is charged with corruption, is being subjected to pressure in a detention facility,** Nikandrov's lawyer said. "**Russian Federal Security Service [FSB] operatives constantly visit Nikandrov** in the detention facility and pressure him into self-incrimination," the lawyer said in court, where the extension of Nikandrov's arrest it being considered. In turn, Nikandrov also said that FSB officials threatened him with illegal criminal prosecution. "The FSB officials requested that the article under which FSB official Budantsev [former FSB official, defendant in the case of a shootout on Rochdelskaya Street] was charged be re-classified, but I refused. They threatened me with criminal prosecution for that," he said.

Kremlin blocks leading pollster amid spy claims

London Times, Marc Bennetts, 2016 09 07

Moscow - **Russia has clamped down on the country's only independent pollster, the Levada Centre, days after it published an opinion poll indicating declining support for President Putin's party before this month's parliamentary elections**. The Moscow-based pollster was officially blacklisted as a "foreign agent" after a justice ministry inspection discovered that it had received £94,000 in funding from the US defence department in the past three years. **The label, which has clear connotations of espionage in Russia,** was introduced in 2012 for non-governmental organisations that receive funding from abroad and are engaged in "political" activities. It has been previously been used to put pressure on human rights organisations and independent election monitors, as well as other groups that fail to toe the Kremlin's line. Lev Gudkov, director of the Levada Centre, told The Times that the justice ministry's ruling would make it impossible for the organisation to maintain the trust of respondents and that it could be forced to close down.

Russian Security Services Say 'Spy Pen' Found in Pokemon Go Player's Home

Moscow Times, Staff report, 2016 09 06

Moscow - **Russian security services say they found a "spy-pen" in the home of video blogger Ruslan Sokolovsky**, who was recently detained for filming himself playing Pokemon Go in a Yekaterinburg cathedral. Police have charged Sokolovsky with committing an extremist act and offending religious sensitivities. If convicted, he could face several years in prison. Russia's Investigative Committee said the pen could be used to receive illegal information from abroad. Other potentially incriminating items in the suspect's apartment include a video camera, a tripod, and a professional microphone. Police are also investigating magazines published by the video blogger, which they say contain illustrations which incite religious hatred. Earlier this year, Sokolovsky launched a self-titled magazine for atheists.

Return to Table of Contents/ Retour à la table des matières

Europe

Non à la surveillance de masse

24 Heures (Suisse), Journaliste maison, 2016 09 13

Berne - Au nom de la sécurité, de **nombreux États renforcent leurs dispositifs de surveillance.** Cela semble particulièrement justifié dans une perspective d'efficacité numérique et face à la menace terroriste. Mais on oublie ou on admet trop facilement que certaines mesures de surveillance piétinent plusieurs droits humains fondamentaux. **La nouvelle loi sur le renseignement (LRens),** sur laquelle nous votons le 25 septembre prochain, n'échappe pas à cette tendance. Parmi la palette de mesures que la loi met à disposition du **Service de renseignement de la Confédération (SRC),** deux sont particulièrement problématiques. L'exploration du réseau câblé permettra au SRC d'enregistrer tous les flux de données et de les analyser au moyen de mots-clés. Le service de renseignements aura ainsi accès à une quantité énorme de données et au contenu de communications électroniques telles que les e-mails, la téléphonie ou les recherches via Internet. Toutes les personnes se trouvant en Suisse seront touchées par ces mesures de surveillance.

Isis Operatives Learn Tricks of Spycraft

Wall Street Journal, Sam Schechner and Benoit Faucon, 2016 09 12

Paris--In recent months, **Europe has been convulsed by a string of simple yet lethal attacks**. Some were committed by people who appear to have received little direct training from Islamic State. The suspects in a failed plot in France last week were "remotely controlled" from Syria by the group, prosecutors said Friday. **Officials worry such attacks could be a way to distract intelligence services while militants prepare more complex plots**. The Paris attackers communicated sparingly -- electronic silences sometimes lasted weeks -- as they crossed the continent in September and October en route to their deadly rendezvous in Paris, security officials said. When they did communicate, they at times called or sent text messages on disposable cellphones they used once and tossed. "Try to make it so that even if the idolatrous dogs intercept and decrypt your messages . . . the only information they will be able to find is your username and password," advised Islamic State's French-language magazine Dar Al Islam this spring. **Patrick Calvar, head of France's main domestic intelligence agency**, told French parliament investigators in May that Islamic State had become a hierarchical, militarized organization, drawing expertise from experienced jihadists and veterans of Iraqi security forces.

15.000 radicalisés en France selon Valls

Charente Libre, Journaliste maison, 2016 09 12

Paris - **Lors de son passage hier à l'émission le «Grand rendez- vous» Europe 1/iTELE/Les Echos, le Premier ministre a revu à la hausse le nombre de personnes radicalisées en France** Le Premier ministre **Manuel Valls** a comparé Nicolas Sarkozy à l'ex-président américain George W. Bush, lors de sa participation hier à l'émission le «Grand rendez-vous» Europe 1/iTELE/Les Echos. Dans une interview au Journal du Dimanch e, le président du parti Les Républicains (LR) prône notamment d' «adapter l'Etat de droit à la réalité de la menace» . «Nous sommes le 11 septembre (quinzième anniversaire des attentats d'Al Qaïda qui ont fait près de 3.000 morts). La réponse à l'époque (du) Patriot Act (...) n'a pas mis à l'abri les Etats-Unis de la menace et des actes terroristes» , a-t-il dit. Pour le chef du gouvernement, l'ancien chef de l'Etat «se trompe sur la forme en faisant croire aux Français, et

de manière terrible, qu'avec lui, au fond, il n'y aurait plus d'attentats» . Parlant d'une menace «maximale» , avec des **attentats déjoués «tous les jours» et environ 15.000 radicalisés**, Manuel Valls a insisté sur les mesures déjà prises et amorcé l'annonce d'un plan pénitentiaire, avec la création de «10.000 places dans les dix ans» en prison, notamment pour des cellules individuelles et «unités dédiées» pour les radicalisés.

Poroshenko expecting from intelligence stepping up cooperation with NATO, EU
Interfax News Agency, 2016 09 10
Kyiv— **Ukrainian President Petro Poroshenko congratulated intelligence officers on professional holiday on September 7 and described the tasks intelligence officers have**. "As for the future expectations from the military intelligence in the framework of the implementation of the provisions of the National Security Strategy of Ukraine, the President stressed the need to bring the structure of military intelligence into conformity with NATO standards taking into account the experience of hostilities in eastern Ukraine. It is also necessary to expand human intelligence capabilities, build capacity of electronic, space and geospatial intelligence, primarily in the temporarily occupied territories of Ukraine, strengthen analytical activities and establish cooperation with special services of the countries-members of NATO and the European Union," the press service of the head of state has reported. Poroshenko visited the Technical Intelligence Center of the Chief Intelligence Directorate of the Ministry of Defense of Ukraine that processes information on the activities of the Armed Forces of the country-aggressor in Crimea and the occupied territories of Ukraine. The president examined new intelligence means. New facts of violation of the Minsk agreements revealed by modern means of intelligence have been shown to the president. **According to Poroshenko, the establishment of the center is a significant contribution to the development of the unified system of state intelligence.**

Nazarbayev cites economy, security as reasons behind cabinet reshuffle
EFE News Service, 2016 09 09
Astana— **Kazakh President Nursultan Nazarbayev on Friday said security concerns and a sluggish economy were behind his decision the previous day to reshuffle his cabinet and name his prime minister as the new head of the country's national intelligence agency**. "There is a need to strengthen and enhance the level of security," Nazarbayev told a full session of his cabinet a day after **naming Prime Minister Karim Massimov to the post of Chairman of the National Security Committee,** or NSC. The decision follows several shooting attacks over the summer blamed on religious extremists, the recent arrest of several jihadist cells in the Muslim nation and the Kazakh government's promise to crack down on violent religious extremism.

Terrorisme: 260 personnes interpellées depuis le début de l'année (Cazeneuve)
Agence France-Presse, Journaliste maison, 2016 09 09
Paris - **Deux-cent soixante personnes, en lien avec des filières ou opérations terroristes, ont été interpellées depuis le début de l'année, indique le ministre de l'Intérieur Bernard Cazeneuve** dans un entretien au quotidien La Presse de la Manche paru vendredi. "Depuis le début de l'année, plusieurs attentats ont été déjoués et 260 individus en lien avec des filières ou opérations terroristes ont été interpellés", annonce Bernard Cazeneuve. "A l'heure actuelle, 689 français ou résidents habituels en France sont actuellement présents sur le théâtre des opérations terroristes en Syrie et en Irak", ajoute-t-il.

Germany to pour cash into mass surveillance
Deutsche Welle, Staff report, 2016 09 08

Berlin - **Germany's spies will be working with significantly increased resources next year, if a budget report leaked to three media outlets is approved. The federal domestic intelligence agency, the Verfassungsschutz (BfV) is bidding for** an 18-percent budget boost in 2017, up to 307 million euros ($345 million), while the **foreign intelligence agency BND will get a 12-percent rise to 808 million euros**, according to a report released Thursday by the "Süddeutsche Zeitung" along with public broadcasters NDR and WDR. A special parliamentary committee must now approve the increase - which, like all secret service budgets, are classified - but opposition parties have already voiced their concern. The majority of the increased funds are expected to be plowed into mass surveillance - particularly decrypting what the report calls "non-standardized telecommunications" - meaning widely-used messaging services, such as WhatsApp. Such online services appear to be a particular concern to the BND. "Encryption means that of the more than 70 available communication services ... only less than ten can be gathered and the content read," the budget plan read. The BND says it needs much of the extra money - some 73 million euros over the next few years - to set up "Panos," a new project specifically aimed at decrypting such messaging systems by finding weaknesses in the apps. The **leaked plan also says the intelligence agencies need extra money to buy expertise from "external companies and service providers**." In the leaked plan, the BfV said it needs extra money because its own resources are currently inadequate to fulfill its mission.

How Hungary's intelligence agency tried to intimidate a journalist into becoming an informant
Hungarian Free Press, Christopher Adam, 2016 09 08
Ottawa - A **Hungarian journalist, known only as "G,"** was heading to work in December 2015. As he approached the offices of his media firm, two men suddenly came up to him and flashed identifications indicating that they **were agents of the Constitution Protection Office (Alkotmányvédelmi Hivatal - AH). The internal intelligence agency, which bears an uncomfortable resemblance in name (and apparently in practice as well) to the dreaded communist era AVH,** was established in 2010, shortly after Prime Minister Viktor Orbán returned to power. It replaced the Office of National Security, which operated from 1990 until 2010. The two men informed "G" that they had to speak with him privately about a matter that concerned his personal safety. The journalist asked the men to explain to him what was going on, but the agents insisted that this must be done privately and at a different location. The journalist obliged, but when they arrived at their destination, the agents attempted to pressure the journalist into signing a declaration, in which he agrees to keep everything disclosed confidential. "G" had no choice but to sign the document. Note: Christopher Adam received a B.A. in history from Concordia University, an M.A. in East/Central European and Russian-Area Studies from Carleton University and a PhD in history from the University of Ottawa. His research focuses on the history of the Hungarian diaspora during the postwar period. Christopher is the founding editor of the Hungarian Free Press, as well as the founder and editor-in-chief of the Kanadai Magyar Hírlap Hungarian-language paper, which won Hungary's 2015 Free Press (Szabad Sajtó) Award. Christopher resides in Ottawa, Canada.

German Intelligence Plans 12% Budget Increase for Communications Monitoring
Sputnik (Russia), Staff report, 2016 09 08
Moscow - **Germany's Federal Intelligence Service (BND) plans a 12 percent increase in spending on communications monitoring, including the deciphering of encrypted communications**, in 2017, Der Spiegel reports. The 2017 BND budget for the purpose is projected to be 808 million euros (about $909 million), the news magazine said on Wednesday citing secret budget documents. The twelve percent increase over the current year comes amid BND plans to boost its response to the widespread use of messenger services such as WhatsApp, Der Spiegel explained. The services encrypt the messages of its users making it

difficult for intelligence services to capture the content. **BND** is planning to overcome this difficulty, which is necessary amid the rise of cybersecurity and terrorism threats. (Full report).

Iran spy head welcomed by German officials
Jerusalem Post, Benjamin Weinthal, 2016 09 08
Berlin - **German intelligence authorities met with Iran's Minister of Intelligence Mahmoud Alavi in Berlin on Tuesday**, according to the Tasnim News Agency in Tehran, a paper with close links to the Revolutionary Guards Corps. Dr. Kazem Moussavi, an Iranian exile in Germany, said on Wednesday Alavi is in the Federal Republic is to lay the groundwork for a visit by President Hassan Rouhani this month. "**The Iranian regime is planning to intensify the monitoring and cracking down on members of the opposition in Germany in order to prevent protests against the visit of Hassan Rouhani**, Iran's president of executions. It would be a huge scandal if German security authorities collaborated in these efforts. Alavi should be brought to justice rather than enjoying an official reception," Moussavi said. In **July, a Berlin court convicted an Iranian man of espionage on behalf of Iran's regime.**

3.000 euros d'amende pour un commissaire de la DGSI soupçonné d'avoir giflé une avocate
Agence France Presse, 2016 09 06
Paris— Un **commissaire de police a été condamné mardi à 3.000 euros d'amende pour avoir giflé une avocate lors d'une garde à vue au siège de la Direction centrale du renseignement intérieur (DCRI, devenue DGSI),** une sanction dont il va faire appel. Le tribunal correctionnel de Nanterre l'a déclaré coupable de "violences volontaires par une personne dépositaire de l'autorité publique sur un avocat dans l'exercice de ses fonctions", en acceptant que cette condamnation ne figure pas au bulletin numéro 2 de son casier judiciaire. Le policier de 58 ans, qui nie les faits, est en outre condamné à verser près de 9.000 euros de dommages et intérêts à l'avocate pour son préjudice - douleur, arrêt de travail, dépenses de santé - et un euro à l'ordre des avocats des Hauts-de-Seine, également partie civile. **Le commissaire, dont l'identité est protégée en raison de ses fonctions à la DGSI, "va faire appel du jugement",** a réagi auprès de l'AFP son avocat, Me Thibault de Montbrial. Le conseil de l'avocate n'a pas souhaité faire de commentaires.

Un commissaire condamné pour avoir giflé une avocate dans les locaux de la DGSI
Le Parisien, 2016 09 06
Paris— Un **commissaire de la Direction générale de la sécurité intérieure (DGSI) a été reconnu coupable** ce mardi, par le tribunal correctionnel de Nanterre, **d'avoir giflé une avocate au cours d'un interrogatoire dans les locaux des services de renseignements.** Il a été condamné à une peine d'amende de 3 000 € et au versement de 10 000 € de dommages et intérêts à l'avocate. Une sanction très inférieure à celle que le procureur avait requise à l'audience, le 28 juin dernier, puisque le magistrat avait demandé deux mois d'emprisonnement avec sursis contre le policier, en plus de la peine d'amende. L'avocat du policier, Me Thibault de Montbrial, annonce déjà qu'il fera appel. Il n'avait pas réussi à faire parler le client de l'avocate, soupçonné de liens avec un terroriste Tandis que le commissaire avait nié la gifle, donnée dans les locaux mêmes de la DGSI, à Levallois le 1er avril 2014, le procureur s'est notamment appuyé sur le « témoignage direct » du client de l'avocate alors interrogé dans les sous-sols du bâtiment. L'homme était questionné sur ses éventuels liens avec un kamikaze impliqué dans un attentat commis en Bulgarie en 2012, mais n'avait pas livré la moindre réponse.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

German daily interviews former Saudi intelligence chief

Die Welt via BBC Monitoring Europe, 2016 09 10

[Interview with the former chief of Saudi Arabia's intelligence service, Prince Turki bin Faisal al Saud, by Sascha Lehnartz; place and date not given: "For Me, Democracy Is a Problematic Term"] The **former chief of Saudi Arabia's intelligence agency, Prince Turki, discusses the political vision of his country - and the problems with Syria and Iran**. Biography: Prince Turki bin Faisal al Saud, aged 71, studied political science (among others, in Georgetown with [former US President] Bill Clinton), Islamic law, and law in Princeton and Cambridge. He is one of the founders of the King Faisal Foundation. Prince Turki bin Faisal al Saud is a member of the Saudi royal family and served as head of the intelligence agency of the Kingdom of Saudi Arabia from 1977 to 2001. He was later appointed ambassador, among others, to the United States. [Lehnartz] Your Royal Highness, in Geneva, the United States and Russia are once again struggling to reach agreement on a ceasefire in Syria. Would Saudi Arabia support such a scheme? [Prince Turki] I am not an official representative of the Saudi Government. Hence, I cannot give an official answer as to whether Saudi Arabia will support such an initiative. What I can tell you is that the Kingdom is in the vanguard of countries that are seeking a peaceful solution for Syria. It has supported all UN Security Council efforts, Geneva 1 and 2, the latest initiative for a ceasefire that was agreed in Geneva. Hence, I would not be surprised if the Kingdom were to support every new attempt to end the fighting in Syria.

Soviet documents 'show Abbas was KGB agent'

Times of Israel, Tamar Pileggi, 2016 09 08

Jerusalem - **Palestinian Authority President Mahmoud Abbas was a Soviet spy in Damascus in the 1980s, Israel's Channel 1 television reported** Wednesday, citing information it said was included in an archive smuggled out of the USSR. According to Channel 1's foreign news editor Oren Nahari, the famed Mitrokhin archive, kept by **KGB defector Vasily Mitrokhin**, revealed that Abbas was a Soviet mole in Damascus in 1983. The documents -- obtained by Israeli researchers Isabella Ginor and Gideon Remez -- purportedly show that Abbas, code-named Krotov (mole), worked under Mikhail Bogdanov, who was then stationed in Damascus and is today Vladimir Putin's envoy to the Middle East. Bogdanov was caught in a diplomatic tussle earlier this week after trying to broker a summit between Abbas and Prime Minister Benjamin Netanyahu in Moscow, who both claimed a willingness to meet while decrying the other for allegedly refusing.

Soviet Document Suggests Mahmoud Abbas Was a K.G.B. Spy in the 1980s

New York Times, Peter Baker, 2016 09 08

Jerusalem - **Mahmoud Abbas, the president of the Palestinian Authority, and President Vladimir V. Putin of Russia** may have more in common than an interest in Middle East peace talks. According to a newly discovered Soviet document, **Mr. Abbas may have once worked for the K.G.B., too**. The possibility, trumpeted by the Israeli media on Wednesday night and just as quickly dismissed by Palestinian officials, emerged from a document in a British archive listing Soviet agents from 1983. A reference to Mr. Abbas is tantalizing but cryptic, just two lines identifying him by the code name "Mole." At the end of his entry are two words: "K.G.B. agent." The suggestion that Mr. Abbas may have been on Moscow's roster more than three decades ago might have been just a historical curiosity but for the fact that it comes at the same time that Mr. Putin has been trying to organize new talks between Mr. Abbas and Prime Minister Benjamin Netanyahu of Israel.

Ibrahim meets Iraqi ambassador, British Official
National News Agency, 2016 09 08
Beirut— **General Security Chief General Abbas Ibrahim** welcomed on Thursday before noon at his office the Defence Senior Advisor for Middle East Affairs at the UK Ministry of Defence Thomas Beckett accompanied with Britain's Ambassador to Lebanon Hugo Shorter. Discussions reportedly featured high on security issues in Lebanon and the region as well **as the existing cooperation between the British Embassy and the General Security.**

Iran intelligence minister travels to Germany
Press TV, 2016 09 07
Tehran - **Iranian Intelligence Minister Mahmoud Alavi has made an unannounced trip to Germany**, with observers describing the unprecedented trip -- about which little detail has been made public -- as highly significant. According to a brief press release that appeared on the website of the **Iranian Intelligence Ministry** on Tuesday, Minister Alavi and his accompanied delegation traveled to the Federal Republic of Germany at the invitation of "pertinent authorities" in the European country. The timing of the trip was not made available. In Berlin, Alavi "met with German intelligence officials and discussed issues of mutual interest," according to the press release. The minister also met with personnel at the Iranian Embassy in Berlin. The unprecedented visit by the Iranian intelligence minister to the heart of Europe comes at a sensitive juncture when the Takfiri terrorist group of Daesh has been posing a growing threat to countries worldwide.

Return to Table of Contents/ Retour à la table des matières

Asia / Asie

South Korea spy agency seen concerned over North's advances in miniaturizing warheads
Reuters, Staff reporter, 2016 09 09
Seoul - **South Korea's intelligence agency is concerned that North Korea is advancing faster to miniaturize warheads on missiles**, a lawmaker said after receiving an agency briefing on the North's latest nuclear test. Kim Byung-kee, a member of the South Korean parliament's intelligence committee, cited the spy agency as saying the North's nuclear test was intended to project a strong image of its leader, Kim Jong Un, on the anniversary of the country's 1948 foundation as a republic, as well as defy international sanctions.

Challenges ahead for new spy chief
The Jakarta Post, 2016 09 09
Jakarta— The **House of Representatives unanimously approved Thursday President Joko "Jokowi" Widodo's nomination of National Police deputy chief Comr. Gen. Budi Gunawan as the National Intelligence Agency (BIN) chief, replacing Sutiyoso**. Budi's nomination for the spy agency's top post surfaced after Jokowi appointed Tito Karnavian National Police chief in June. Indeed, the nomination of Budi, a 1987 graduate of the Police Academy, may give a boost to the regeneration process within the police force. On the other hand, this decision might pose a risk of politicization to the BIN, as Budi is known for his close ties to the ruling Indonesian Democratic Party of Struggle (PDI-P). In fact, there is nothing new with the politicization issue because Sutiyoso was chairman of the minority Indonesian Unity and Nationhood Party (PKPI).In general, there are three causes for concern related to politicization of the intelligence agency.

Budi Gunawan vows to improve spy agency
Jakarta Post, Marguerite Afra Sapiie, 2016 09 08
Jakarta - **Budi Gunawan vows to improve spy agency National Police deputy chief Comr. Gen. Budi Gunawan delivers his plans during a confirmation hearing over his nomination as the new chief of the National Intelligence Agency (BIN)** at the House of Representatives' Commission I overseeing defense and foreign affairs on Sept. 7. The sole candidate for the spy chief position, Comr. Gen. Budi Gunawan, vows to improve State Intelligence Agency (BIN) performance in order to optimize the agency's role in the protection of national security. The National Police deputy chief said during the confirmation hearing at the House of Representatives' Commission I overseeing security and foreign affairs that he aimed to improve BIN's professionalism, objectivity and integrity should he take helm of the agency as the country's coordinator of intelligence affairs. He also wants to improve some aspects of BIN so that the agency could play a greater role in facing new global challenges.

FBI wants to interrogate Bangladesh militants
Dhaka Tribune, Sheikh Shahariar Zaman, 2016 09 07
Dhaka - The **Federal Bureau of Investigation has expressed interest to work closely with the Bangladeshi investigators dealing with recent militant attacks**, a Foreign Ministry source says. As part of the process, the FBI wanted to let its members interrogate militant suspects arrested in recent months. However, the Bangladesh government has not shown any interest in this regard. "They [the FBI] have told us that they have much knowledge and expertise in this matter and that they want to understand the militants' psychology. But the government has not yet responded positively," a Foreign Ministry official said, declining to be named. According to the official, who was not authorised to talk to media on the matter, the West believes that the Islamic State or other foreign terrorist groups are directly involved in the recent terror attacks in Bangladesh.

Afghan MPs blame recent attacks on weak intelligence
Afghan Ariana TV via BBC News South Asia, 2016 09 07
Kabul— [Presenter] A **number of MPs believe that weakness in the security bodies has resulted in an escalation of insecurity in the country, adding that despite all the measures in place, terrorists can achieve their goals.** The MPs have said that senior security officials have failed to prevent attacks, suggesting fundamental changes in the fight against terrorism. The MPs stressed that currently the country is in need of ministers who can value each drop of the bloodshed by the security forces. Rafi Sediqi with more details: [Correspondent] The upsurge in insecurity has raised many concerns and one of the reasons for the worsening security situation is said to be **weakness in the management of security bodies**. A number of MPs have said that currently the country is in need of security ministers who can stand firmly against terrorists' attacks. [MP Ramazan Bashardost, captioned] In this country and in the current situation, **we need the ministers of defence, interior and head of the National Directorate of Security to go to the most remote areas with a gun and fight along with the security forces**. They should defend their land but they are more concerned about their land cruisers, bodyguards, palaces and other privileges. I am sorry to say that this [sort of] minister could never represent the people.

Return to Table of Contents/ Retour à la table des matières

Africa / Afrique

Mkhwebane a step closer to protector's office

Business Day (South Africa), 2016 09 08
Cape Town— **Advocate Busisiwe Mkhwebane** cleared a crucial hurdle on Wednesday night, when an overwhelming majority of the National Assembly gave her the nod to succeed Thuli Madonsela. It is now up to **President Jacob Zuma to confirm her as the country's next public protector**. Once that is done, Mkhwebane will begin her seven-year term in two months' time.The **DA objected to her candidacy, raising concerns about her links with the country's intelligence agencies**. Among other jobs listed on her CV, **Mkhwebane worked in the State Security Agency (SSA).**

Edo 2016: Don't undermine Nigeria's democracy, group tells Police, SSS
The Premium Times, 2016 09 08
Abuja— A **Civil Society Organisation has condemned the attempt by the Police and State Security Service (SSS) to force the postponement of the Edo State Governorship Election** scheduled for Saturday. In a statement issued to journalists in Abuja, the Youth Initiative for Advocacy, Growth and Advancement, YIAGA, warned the two agencies against undermining Nigeria's democracy and the sovereignty of the Independent National Electoral Commission, INEC. The **Police and the SSS had on Wednesday issued a joint statement asking INEC to postpone the election**. The security operatives said the call was to prevent alleged attack planned by insurgents on the state during the election. The call has been condemned by various stakeholders including the People Democratic Party, PDP, who described the move as bizarre and shocking.

Mkhwebane denies she was a spy
Sowetan, 2016 09 07
Cape Town—**Proposed public protector Busisiwe Mkhwebane has denied DA allegations that she was a spy on behalf of the State Security Agency (SSA) while working as a South African immigration officer in China.** "I never worked for SSA. I only joined the SSA on July 4, 2016," Mkhwebane said in reply to a question yesterday afternoon. Mkhwebane's appointment is scheduled to be proposed to President Jacob Zuma by Parliament this afternoon. The National Assembly will debate the proposed appointment of Mkhwebane, who at this stage, has the support of all political parties except the DA, after a parliamentary ad hoc committee proposed her appointment.

Return to Table of Contents/ Retour à la table des matières

Americas / Amériques

Mexico's Finance Minister Resigns in Wake of Trump Visit
The Wall Street Journal, David Luhnow, 2016 09 07
Mexico City— Donald Trump's recent visit to Mexico, widely seen in the country as a humiliation, claimed a high-profile political victim on Wednesday with the resignation of Finance Minister Luis Videgaray, President Enrique Peña Nieto's closest adviser. Mr. Videgaray, who played a key role in helping orchestrate the Trump trip, was succeeded by José Antonio Meade, the country's social development minister and former finance chief, Mr. Peña Nieto told a news conference. Mr. Videgaray's departure is a blow to the president. The former investment banker was widely seen as the brains behind the Mexican president and the driving force behind a series of high-profile overhauls in the past few years, including opening Mexico's closed oil industry to private investment for the first time since 1938. The cabinet reshuffle is the first step by the president in trying to limit the damage from the Trump visit, said **Guillermo Valdés, a**

former head of Mexico's intelligence agency. "It's the least he could do to try to recover some credibility given that he has 27 months left in power," he said.

Brazil Rio Paralympics will have less security than Olympics
Folha de Sao Paulo via BBC Monitoring Americas, 2016 09 07
Rio de Janiero— **Despite official denials. the 2016 Paralympics will open in the Brazilian city of Rio de Janeiro today amid a "climate of demobilisation of the security forces"**, with a reduced security contingent protecting the event compared to the Olympic Games in August, Brazilian newspaper Folha de Sao Paulo reported on 7 September. "Officially, the bodies responsible for the vigilance of the event are denying it, but the reduction in the force for the event shows that the [security] risks are considered less this time [compared to the Olympics]," the newspaper said in an article written by a correspondent in Rio. Folha said one of the first decisions taken after the closing of the Rio Olympics on 21 August was to reduce the size of the National Force security contingent protecting the sports arenas and the athletes' village in the city to 4,200 members from the 6,000 that were there for the Olympic Games. Less competition arenas were being used for the Paralympics. In addition, **the numbers of Federal Police and members of the Brazilian Intelligence Agency (Abin) were reduced by nearly 20 per cent for the Paralympics,** the newspaper said.

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

14-09-2016 to/au 20-09-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Ministerial directive on use of evidence obtained from torture still on books
CBC News, Nazim Baksh and Terence McKenna, 2016 09 20
Even as Ottawa remains locked in a decade-long legal battle with three Canadians who were tortured in Syria in a post-Sept. 11 crackdown on terror suspects, Canada's intelligence service is still allowed to act on information obtained through torture. Public Safety Minister Ralph Goodale could rescind the ministerial directive that one of his predecessors, Conservative Vic Toews, issued in 2009. **But in a statement to CBC's the fifth estate, Goodale said he "continues to assess ministerial directives to ensure that they both protect our rights and freedoms, and keep Canadians safe."** The original directive was updated in 2010 to specify that **CSIS is only allowed to use information derived from torture in "exceptional circumstances where CSIS may receive urgent, perishable information from a foreign agency linked to a specific and imminent security threat to Canada or Canadians**." When the directive made headlines in 2012, interim Liberal Leader Bob Rae called it "unprecedented in our history." "It, I think, reflects a complete breach of our international obligations with respect to torture," he said. "And I think it shows a government which has simply lost its way in terms of Canadian values. "This is not how we do business in Canada." **Abdullah Almalki, Ahmad Elmaati and Muayyed Nureddin** were never arrested in Canada for suspected terror offences, but all three were targeted by CSIS and the RCMP and eventually detained and tortured in Syria. Documents obtained by the fifth estate and The National show CSIS and the RCMP not only knew the men would be tortured, but co-operated with Syrian officials in their interrogations.

Appel à une enquête sur la torture de Canadiens en Syrie
Le Devoir, Philippe Orfali, 2016 09 20
Ottawa--Le **Canada doit faire " toute la lumière ", une fois pour toutes, sur le rôle joué par le gouvernement fédéral et ses agences de sécurité dans la torture de certains de ses citoyens, a exigé lundi le Nouveau Parti démocratique** (NPD), au premier jour de la rentrée parlementaire, alors qu'émergeaient de nouveaux détails sordides concernant la torture de trois Canadiens par la Syrie. Une commission d'enquête avait conclu dès 2008 que **le Service canadien du renseignement de sécurité (SCRS) avait joué un rôle " indirect " dans la torture d'Abdullah Almalki, Muayyed Nureddin et Ahmad El Maati,** trois ressortissants canadiens soupçonnés de liens avec al-Qaïda, arrêtés par le renseignement militaire syrien et détenus jusqu'en 2004. Mais des milliers de documents classés secrets obtenus par les avocats des trois hommes et transmis au réseau anglais de Radio-Canada établissent désormais que le SCRS et la Gendarmerie royale du Canada (GRC) ont coopéré de près avec Damas et les tortionnaires syriens des trois hommes.

Prepare for threat of quantum computing to encrypted data, Canadian conference told
IT World Canada, Howard Solomon, 2016 09 20
Toronto— The **race to create new cryptographic standards before super-fast quantum computers are built that can rip apart data protected by existing encryption methods isn't going fast enough,** two senior Canadian officials have warned a security conference. "I think we are already behind," **Scott Jones, deputy chief of IT security at the Communications Security Establishment (CSE), responsible for securing federal information systems**, told

the fourth annual international workshop on quantum-safe cryptography in Toronto on Monday. Quantum computing – or more accurately, computers that use quantum mechanics – is not a dream, Jones and others told the conference of business executives, crypto academics, IT companies and government officials. One prediction is there's a one in seven chance that by 2026 a quantum computer will exist that can break RSA-2048 encryption. It may take longer — or, if there's an advance, shorter. "Quantum represents a fundamental change and challenge to encryption for all of us," Jones said, noting that encrypted transactions are the backbone of security and trust on the Internet. **His comments were backed by David Sabourin, CSE's manager of cryptographic security**, who said that if the 2026 prediction is right "we're in trouble." Speaking on a panel of government experts, Sabourin noted the U.S.-based National Institute of Standards and Technology (NIST) will close its call for proposed new and more quantum-secure public key encryption algorithms next year.

The Torture Files: Documents show CSIS and RCMP's role in post- 9/11 torture of 3 Canadians in Syria
CBC News, Nazim Baksh and Terence McKenna, 2016 09 19
Thousands of pages of secret files obtained by CBC reveal how Canada's police and intelligence service not only knew three Canadians were being tortured in Syrian jails in a post-Sept. 11 crackdown, but co-operated with Syrian officials in their interrogations. **The files also show a Canadian ambassador helped deliver questions the RCMP and CSIS wanted put to the Canadians imprisoned in Syria**, a country with a dismal human rights record. The revelations are featured in "The Torture Files," a joint investigation by The National and the fifth estate that airs this week. Abdullah Almalki, Ahmad Elmaati and Muayyed Nureddin were never arrested in Canada for suspected terror offences, but to this day there is a cloud of suspicion hanging over them. Ten years ago, they each filed $100-million lawsuits against the government. Maher Arar, another Canadian arrested and tortured in Syria in the wake of al-Qaeda's deadly attacks on New York and Washington, received an apology and a $10.5-million settlement from the federal government in 2007. Lawyers representing Almalki, Elmaati and Nureddin fought and eventually won a lengthy court battle with the RCMP and CSIS to gain access to thousands of heavily redacted files, amounting to hundreds of thousands of pages.

Media groups push to intervene in Vice Media fight with RCMP
Canadian Press, Colin Perkel, 2016 09 18
Ottawa - **Forcing journalists to act as investigators for police would undermine the critical role news outlets play in a free society, a coalition of media organizations argue** in documents filed with Ontario's top court. Journalists, the group argues, must be able to gather news by communicating with citizens who are in an adversarial relationship with the state. "If journalists or media organizations are too easily conscripted into serving as the de facto 'investigative arm of the police,' they will be unable to perform their vital societal role," they say. "Important stories will go untold." The **filings with the Court of Appeal come in support of a coalition request to intervene in a case involving an RCMP demand for Vice Media to turn over materials related to a terrorism investigation.** The information is related to stories journalist **Ben Makuch wrote about accused terrorist Farah Shirdon**.

PM urged China to free Garratt: source
Globe and Mail, Nathan Vanderklippe, 2016 09 17
Ottawa - **Prime Minister Justin Trudeau insisted in several meetings with China's top leaders that a new relationship would be difficult to forge between the two countries without the release of a Canadian man held for two years on suspicion of being a spy**, a senior government source says. By the time Mr. Trudeau's first official visit to China was over, the release of **Kevin Garratt** seemed all but guaranteed, according to the official who had

knowledge of the Prime Minister's discussions with Chinese President Xi Jinping and Premier Li Keqiang. But the assurances Mr. Trudeau received in return cast his visit to China in a new light. Instead of leaving Beijing with only relatively small gains, his doggedness allowed him to achieve one of his central ambitions - even if critics say the deportation of Mr. Garratt is a minor achievement next to more serious concerns about China's treatment of foreign investors and its own people. Mr. Trudeau's insistence was reflected in a visit from **Michel Coloumbe, director of the Canadian Security Intelligence Service, who in an unusual step was dispatched to meet his Chinese counterpart** four months ago to personally attest that Mr. Garratt was not a spy for Canada. Co-ordinated efforts from Foreign Minister Stephane Dion and Canada's ambassador to China, Guy SaintJacques, on top of previous attempts by Stephen Harper in 2014, helped to secure the release of a man whose lengthy detention in China on questionable charges had raised questions among Canadians, and anger in Ottawa.

Canada goes extra mile to secure Kevin Garratt's release from China
Globe and Mail, Nathan Vanderklippe & Laura Stone, 2016 09 16
Ottawa - The **sudden release of a Canadian held for two years in China on suspicion of spying** comes after a high-stakes campaign to secure his freedom, **including an unusual and unannounced visit four months ago by the director of the Canadian Security Intelligence Service,** who met with Chinese officials to try to persuade them that **Kevin Garratt** wasn't a spy. On Thursday, a bearded Mr. Garratt landed in Vancouver and embraced his family, a free man. He had been accused by Chinese authorities of stealing military and defence research secrets and charged with espionage. His release puts a sudden end to a major irritant between Canada and China less than a week before Premier Li Keqiang arrives in Ottawa for an official visit, and caps an extraordinary effort by the government of Canada, its embassy in Beijing and two prime ministers to push for Mr. Garratt's release. **The visit to China by CSIS director Michel Coulombe, Canada's top spy, was one element of that effort, according to multiple sources with knowledge of the meeting.** When Mr. Garratt was indicted in January, China's state media said investigators had found evidence he had accepted tasks to gather intelligence for Canada. Mr. Coulombe met with Geng Huichang, the minister in charge of China's powerful state security apparatus, to deliver the message in person that Mr. Garratt, a Pentecostal pastor, did not work for CSIS.

Canadian Held Two Years on Spy Charges in China Returns Home
New York Times, Ian Austen, 2016 09 16
Ottawa - A **Canadian man who worked with a charity that provided food to North Koreans returned to Canada on Thursday after being held in China on espionage charges** for just over two years. The family of the man, Kevin Garratt, who is from Vancouver, British Columbia, said in a brief statement that he was deported after a court hearing in Dandong, China, on Tuesday. "The Garratt family thanks everyone for their thoughts and prayers, and also thanks the many individuals who worked to secure Kevin's release," the statement said. Mr. Garratt's detention dampened relations between Canada and China, particularly under the previous Conservative government. Early this month, Prime Minister Justin Trudeau raised Mr. Garratt's case during a visit to China. Mr. Garratt and his wife, Julia Dawn Garratt, were operating a coffee house in China near the border with North Korea as part of a Christian aid mission when they were both arrested in August 2014. **Chinese officials later said that they were being held on "suspicion of stealing and spying to obtain state secrets."**

Dutch police to get Canadian BlackBerry data
National Post, Joseph Brean, 2016 09 16
Ottawa - After a police raid on a Toronto technology company, **Canada has agreed to share a massive stash of encrypted BlackBerry Ltd. messages with Dutch police investigating an**

underworld conspiracy involving robberies, drug trafficking, attempted murder and assassinations. But rather than simply hand over the messages, from 20,000 different users, an Ontario judge this week imposed restrictions designed to prevent a "fishing expedition" by police in the Netherlands or any other country. The ruling ensures the data will remain under Canadian control, and not be shared further without a court's approval. The fear is that unfettered disclosure would expose innocent people to the unjustified attention of police, just because they used an encrypted Black-Berry. "Canada remains the home of this data," Judge Ian Nordheimer wrote.

Goodale to host UK terror watchdog, national security committee
iPolitics.ca, Amanda Connolly, 2016 09 16
Ottawa - **Public Safety Minister Ralph Goodale will host the U.K.'s terrorism legislation watchdog and members of its Intelligence and Security Committee (ISC) next week in Ottawa** for a meeting that will include discussion about the government's new national security committee of parliamentarians. The meeting will come as Parliament resumes from its summer sitting and is expected to dive into debate on Bill C-22, which was tabled on June 16 and announced the framework for the government's nine- member committee of appointed parliamentarians who will "review and scrutinize" the **activities of national security agencies**.

Everything We Know About Canada's Efforts to Track Would-Be Terrorists
Vice News, Tamara Khandaker, 2016 09 15
Despite being hailed as a powerful tool to stop would-be terrorists from committing violence or leaving to fight abroad, just one person in Canada is currently on a terrorism-related peace bond. According to a list provided to VICE News by the **Public Prosecution Service of Canada, police are pursuing peace bonds against nine others**, all of whom were arrested and are currently out on bail, living with varying degrees of limited freedom. Prior to August, there was one more name on the active peace bond list: **Aaron Driver**, who was shot to death by police while allegedly attempting to carry out a terrorist attack. The rarity of the bonds' application, and Driver's death, raise a number of questions about the efficacy of peace bonds to keep watch over people deemed at high risk of committing acts of terror. VICE News has spent weeks gathering details of the peace bonds process, obtaining bail conditions, interviewing lawyers assigned to these cases, and tracking down individuals who have come in contact with the regime. In many cases, even as the Crown proceeds with the peace bond process--before a judge hears the application and before the prosecution can prove their case--the court orders strict and limiting bail conditions.

Cyberattacks could cause border chaos, officials say
Toronto Star, Alex Boutilier, 2016 09 15
Ottawa - **Border officials warn a cyberattack on their facial recognition or fingerprints databases could result in barring innocent travellers from Canada** - or letting the wrong people in. In documents prepared for **Public Safety Minister Ralph Goodale in November, Canada Border Services Agency (CBSA)** officials said they need to "keep pace with emerging security vulnerabilities" to systems governing who can enter the country. The agency's growing use of "biometric" data - such as fingerprints, facial recognition and retinal scans - was cited as an example. "A malicious cyberattack, for example, could infiltrate the back-end of a biometric identification system and produce false acceptances and/or rejections," reads the document, obtained by the Star under access to information law.

Canada given lukewarm grade on anti-money laundering efforts
Globe and Mail, Christina Pellegrini and David Berman, 2016 09 15

Canada's anti-money laundering efforts have improved in recent years but significant gaps leave the country open to illicit financial activities, according to an evaluation from an organization that develops policies to protect the global financial system. The importance of anti- money laundering efforts has risen in recent years, as authorities attempt to cut the financial lifelines to criminals and terrorists. The **Financial Action Task Force** (FATF), an intergovernmental body that develops standards for combating money laundering around the world, gave Canada a lukewarm assessment - its first since a 2007 evaluation.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

Extradition for FBI Asperger's hacker

The Advertiser, Martin Robinson, 2016 09 18

Washington - An **accused British superhacker should be extradited to the US to face trial where he could be jailed for 99 years**, a judge has ruled. **Asperger's sufferer Lauri Love, 31, allegedly hacked huge amounts of data from US agencies, including the FBI and NASA**, between 2012 and 2013. Judge Nina Tempia yesterday agreed with the American authorities and ruled Love, who lives with his parents in Suffolk, should face a cyber-hacking trial in the US. Love, who will appeal to the High Court, said after the judgment: "If you have come for justice, then you have missed it." His case is "almost identical" to that of fellow hacker Gary McKinnon, whose extradition was blocked by **then Home Secretary Theresa May** in 2012.

Inside the fight to reveal the CIA's torture secrets

The Guardian (London), 2016 09 18

Analysis - **Daniel Jones** had always **been friendly with the CIA personnel** who stood outside his door. When he needed to take something out of the secured room where he read mountains of their classified material, they typically obliged. An informal understanding had taken hold after years of working together, usually during off-peak hours, so closely that Jones had parking privileges at **an agency satellite office not far from its McLean, Virginia, headquarters**. They would ask Jones if anything he wanted to remove contained real names or cover names of any agency officials, assets or partners, or anything that could compromise an operation. He would say no. They would nod, he would wish them a good night, and they would go their separate ways. After midnight in the summer of 2013, **Jones deliberately violated that accord. Jones, a counter-terrorism staffer, had become the chief investigator for the Senate intelligence committee, the CIA's congressional overseer, on its biggest inquiry**. For five years, he had been methodically sifting through internal CIA accounts of its infamous torture program, a process that had begun after the committee learned - thanks to a New York Times article, not the agency - that a senior official had destroyed videotapes that recorded infamously brutal interrogations. The subsequent committee inquiry had deeply strained a relationship with Langley that both sides badly wanted to maintain.

'A constitutional crisis': the CIA turns on the Senate

The Guardian (London), Spencer Akerman, 2016 09 18

Analysis - It was 11pm, in the chill of January, but **Daniel Jones** needed a run around the Capitol. During the winter of early 2014 Jones's only chance for serenity was these late hours. The CIA was demanding his boss, **Senate intelligence committee chairwoman Dianne Feinstein**, fire him. Feinstein's Republican colleagues, once supportive of Jones, were

demanding he testify. Testimony was treacherous. Sheldon Whitehouse, a Rhode Island senator and former federal prosecutor, warned Jones that asserting his rights against self-incrimination or seeking a lawyer's counsel could give committee Republicans a political lever against his highly controversial work. The CIA would soon formally insist that the US justice department actually prosecute Jones, the Senate staffer who had devoted over six years of his life to investigating the CIA's infamous post-9/11 torture program. **Jones, a former FBI counter-terrorism analyst**, wanted to testify. The CIA had pushed him past the point where he could back down. Its lies, documented in a 6,700-page secret report which Jones was constantly rewriting that winter, were compounding: to Congress, to Barack Obama, to George W Bush, to the press, to the public. The lies were not random misstatements…The CIA had gone "into war mode" with its congressional overseers, Jones told the Guardian. There was no choice but to work deeply into the night, leaving Capitol Hill at 3 or 4 in the morning, with breaks only for a run, and then back to work by 8 or 9 to repeat the cycle. Less than a year had passed since the CIA had communicated to the Senate that its exhaustive torture report, drawn from millions of the agency's own documents, was significantly incorrect.

Edward Snowden characterized as 'serial exaggerator' in House intelligence committee report
Washington Times, Andrea Noble, 2016 09 16
Washington - A **House intelligence committee report on Edward Snowden characterizes the former National Security Agency contractor not as a whistleblower but as a "serial exaggerator"** whose theft of 1.5 million classified government documents has done **tremendous damage to national security**. A 4-page summary of the classified report released by the House committee on Thursday says the bulk of the documents taken "have nothing to do with programs impacting individual privacy interests" but rather pertain to military, defense and intelligence programs. "A review of the materials Snowden compromised makes clear that he handed over secrets that protect American troops overseas and secrets that provide vital defenses against terrorists and nation-states," the report states. "Some of Snowden's disclosures exacerbated and accelerated existing trends that diminished the IC's capabilities to collect against legitimate foreign intelligence targets, while others resulted in the loss of intelligence streams that had saved American lives."

House Intelligence Committee Urges Obama Not to Grant Snowden Pardon
New York Times, Charlie Savage, 2016 09 16
Washington - **Lawmakers on the House Intelligence Committee unanimously signed a letter to President Obama on Thursday asking him not to pardon Edward J. Snowden**, the former intelligence contractor who leaked troves of information about **National Security Agency surveillance and data collection in 2013**. "We urge you not to pardon Edward Snowden, who perpetrated the largest and most damaging public disclosure of classified information in our nation's history," the bipartisan letter said. "If Mr. Snowden returns from Russia, where he fled in 2013, the U.S. government must hold him accountable for his actions." The committee also said it had completed a 36-page report summarizing the results of its multiyear investigation into the leaks and their effect. The report was classified, but the panel released a three-page executive summary that portrayed Mr. Snowden as a "serial exaggerator and fabricator" who is "not a whistle- blower."

Polygraph panic: CIA director fretted his vote for communist
CNN.com, Tal Kopan, 2016 09 16
Washington - At his **first polygraph test to enter the CIA**, the future director had a secret. John Brennan on Thursday recalled being asked a standard question for a top security clearance at his **early CIA lie detector test: Have you ever worked with or for a group that**

was dedicated to overthrowing the US? "I froze," Brennan said during a panel discussion about diversity in the intelligence community at the Congressional Black Caucus Foundation's annual conference. "This was back in 1980, and I thought back to a previous election where I voted, and I voted for the Communist Party candidate," Brennan was responding to a question about barriers to recruiting diverse candidates for the intelligence fields, including whether past records of activism could hurt someone applying for a clearance later in life.

U.S. gives 'no free pass' to Russia, other nations on cyberespionage, Justice official warns
Washington Post, Ellen Nakashima, 2016 09 16
Washington - A **senior Justice Department official this week issued a thinly-veiled warning to Russia that significant acts of cyberespionage** will not be ignored. That would include the Democratic National Committee hack, which would be considered an act of political cyberespionage of the sort the United States traditionally has not publicly attributed to a culpable foreign spy agency. That set of intrusions, disclosed by the DNC in June, has been **linked to the Russian government by FBI investigators**, though the U.S. government has not publicly acknowledged that. Nonetheless, said Assistant Attorney General for National Security John Carlin, if Russia or any other country thinks "there's going to be a free pass, that we can't figure out what they're doing in cyber-enabled espionage, I think the message should be clear: You're wrong. You can and will be held accountable."

As Russia reasserts itself, U.S. intelligence agencies focus anew on the Kremlin
Washington Post, Greg Miler, 2016 09 15
Washington - **U.S. intelligence agencies are expanding spying operations against Russia on a greater scale than at any time since the end of the Cold War**, U.S. officials said. The mobilization involves **clandestine CIA operatives, National Security Agency cyberespionage** capabilities, satellite systems and other intelligence assets, officials said, describing a shift in resources across spy services that had previously diverted attention from Russia to focus on terrorist threats and U.S. war zones. U.S. officials said the moves are part of an effort to rebuild U.S. intelligence capabilities that had continued to atrophy even as Russia sought to reassert itself as a global power. Over the past two years, officials said, the United States was caught flat-footed by Moscow's aggression, including its annexation of Crimea, its intervention in the war in Syria and its suspected role in hacking operations against the United States and Europe. U.S. spy agencies "are playing catch-up big time" with Russia, a senior U.S. intelligence official said. Terrorism remains the top concern for American intelligence services, the official said, but recent directives from the **White House and the Office of the Director of National Intelligence (ODNI)** have moved Russia up the list of intelligence priorities for the first time since the Soviet Union's collapse.

Comey: US could respond to Russia out of public view
The Hill, Joe Uchill, 2016 09 14
Washington - **FBI Director James Comey on Wednesday pushed back on claims the U.S. was not doing enough to fend off Russian hackers**, noting his agency can respond outside of the public eye. Comey was asked at a Center for Strategic and International Studies event in Washington why there was no visible response to Russian cyber threats and whether that meant the government was unable to handle them. "We have a variety of tools that we as a government can use to deter behavior on the internet outside of norms -- and that can involve a variety of things, only some of which could be visible to the public," he said, quickly clarifying he was speaking in broader terms than just Russia.

FBI's Comey: Twitter fuels 'monster of a bias'
Politico, Louis Nelson, 2016 09 15
Washington - **FBI Director James Comey lamented on Wednesday the loss of public trust in government institutions like the one he runs and blamed "echo chambers" like Twitter for making his job more difficult.** "My children, again, discipline me not to go on Twitter because apparently people say bad things about me on Twitter. But **things like Twitter offer us the opportunity only to encounter views consistent with our own, 24 hours a day,**" Comey explained at a Center for Strategic and International Studies event Wednesday. "There's an opportunity to feed that monster of a bias, that confirmation bias, all the time. So it accelerates that fractionalizing of our society, and it makes it much harder for people like me, like you, like the people in here, to speak reason to folks about our institutions." Comey, a Republican once appointed deputy attorney general by President George W. Bush, and the bureau he helms have been a regular target of GOP attacks over the FBI's decision to recommend against charges following the investigation into Hillary Clinton's use of a personal email server as secretary of state.

CIA Director John Brennan to Birmingham students: 'I don't want the agency to just look like me'
Alabama.com, Ivana Hrynkiw, 2016 09 14
Birmingham, Ala. - **The Director of the Central Intelligence Agency visited Birmingham high school students today to discuss what working for the agency is like and the possibility of starting a CIA ambassador program** at Ramsay High School. Brennan stressed that character and integrity are two of the most important things he looks for in potential officers. "Make sure you're taking care of how you're doing on the personal front... integrity can be quashed in a matter of minutes."

DNI Declines Required Damage Assessment of Clinton's Leaked Email Secrets
Washington Free Beacon, Bill Gertz, 2016 09 14
Washington - The **U.S. intelligence community declined to conduct a required assessment of the damage to national security caused by former secretary of state Hillary Clinton** sending and receiving secrets on a private email server. **"ODNI is not leading an [intelligence community]-wide damage assessment and is not aware of any individual IC element conducting such formal assessments," Joel D. Melstad, a spokesman for the of the Office of the Director of National Intelligence, said**. The most sensitive classified information leaked and possibly obtained by foreign intelligence services included ultra-secret information on U.S. drone strikes, according to American intelligence officials. James Clapper, the director of national intelligence, agreed with security officials who argued against the need to carry out the damage assessment.

Pardon for former NSA contractor Snowden seen unlikely
Reuters, Staff report, 2016 09 14
Washington - The **U.S. government will not budge on its demand that former National Security Agency contractor Edward Snowden return** to face prosecution for stealing thousands of classified intelligence documents, despite new calls for President Barack Obama to pardon him, U.S. officials said on Tuesday. The officials said they expect Snowden's supporters to use the Thursday release of "Snowden" - directed by veteran filmmaker Oliver Stone - to mount a public campaign demanding a pardon before Obama leaves office in January.

Spy agencies concerned about possible U.S. election hacks: NSA chief
Reuters, Staff report, 2016 09 13

Washington - **American intelligence agencies are concerned about reports that foreign governments may be attempting to undermine the Nov. 8 U.S. elections through cyber attacks, Admiral Mike Rogers**, the **director of the National Security Agency, said** on Tuesday. "We continue to be actively concerned," Rogers told a Senate hearing, responding to a question from Senator John McCain, chairman of the Senate Armed Services Committee. Marcel Lettre, Under Secretary of Defense for Intelligence, testified that the government is taking any such activities "quite seriously" and said an "aggressive investigation" is under way. Rogers said he could not provide specifics about spy agencies' current assessment of the alleged hacking in a public setting. But he added, "I will say this, that it continues to be an issue of great focus ... for the **foreign intelligence community**, attempting to generate insights into what foreign nations are doing in this area." Under further questioning, Rogers declined to characterize the activity as by a foreign nation-state.

U.S. Spies Think China Wants to Read Your E-Mail
Bloomberg View, Eli Lake, 2016 09 13
Column - **For more than a decade, the U.S. military and intelligence community has quietly warned that the world's largest telecom equipment manufacturer, Huawei, is an arm of the People's Liberation Army** and that its phones, circuits and routers are instruments of Chinese eavesdropping. Now **these agencies are starting a formal review, led by the FBI and the NSA, examining the national security implications of Huawei's potential participation** in building the U.S. 5G wireless network, according to current and former U.S. intelligence officials. These officials told me that while the two largest U.S. telecom providers -- AT&T and Verizon -- have yet to join up with Huawei on this project, the prospect of such a partnership is real and alarming. They spoke on condition of anonymity because the intelligence assessment was ongoing and classified.

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

Spies will join fight against slavery gangs, May declares
London Times, Francis Elliott, Fiona Hamilton, 2016 09 20
New York - **Britain's intelligence agencies are to pursue slavery gangs alongside terrorists and drug traffickers**, Theresa May has announced. **MI6 and GCHQ will be given extra resources to disable networks in the countries most involved in the modern slave trade,** such as Albania, Vietnam and Nigeria. MI5, the domestic intelligence agency, is to work with police to free those trafficked to Britain for exploitation in brothels, nail bars, carwashes and elsewhere. The new anti-slavery taskforce, which will begin work next month, is intended to serve as a model for other countries. The prime minister called on world leaders to do more to "rid our world of this evil" as she brought one of her key priorities as home secretary into Downing Street. Home Office figures suggest that between 10,000 and 13,000 immigrants have been lured to Britain or smuggled in illegally to live in slum conditions and work for low wages. Globally, 45 million people are exploited as part of a trade in humans estimated to cost the world economy $150 billion.

MI6 failed to check on torture claims by Lee Rigby killer
London Times, Fiona Hamilton, 2016 09 16

London - **MI6 has been criticised for "serious failings" in its response to allegations that one of the killers of Lee Rigby had been tortured by Kenyan authorities**. **Sir Mark Waller**, the intelligence services commissioner who scrutinises **MI6, MI5 and GCHQ**, spoke out after investigating the handling of claims by **Michael Adebolajo**, who killed Fusilier Rigby outside the army barracks in Woolwich, southeast London, in May 2013 with fellow extremist Michael Adebowale. After the murder it emerged that Adebolajo had been arrested in November 2010 in Kenya where he was believed to have been en route to fight with al-Shabaab, the Somali terrorist group. He later claimed that he was mistreated before being deported on suspicion of terrorism.

GCHQ's 'Great British Firewall' raises serious concern - privacy groups
The Guardian (London), Ewan MacAskill, 2016 09 14
London - **Privacy groups have expressed serious concern at the prospect of a "Great British Firewall" proposed by the surveillance agency GCHQ** to protect major British companies against malicious hackers. They said they were worried that it could be used to deny freedom of speech, with the government potentially able to designate sites they disapprove of as "malware". There is also concern about the prospect of handing over such power to GCHQ, given its track record of intrusion working in tandem with the **US National Security Agency (NSA)**. Thomas Falchetta, a legal officer for Privacy International, said: "Given the broad scope of GCHQ's hacking operations both domestically and abroad, this seems like the fox protecting the chicken." GCHQ insisted that privacy concerns would be "hardwired" into the project and companies would have a choice about whether to participate or not.

GCHQ blocks 58,000 scam emails from government addresses every day
London Daily Telegraph, Cara McGoogan, 2016 09 13
London - The **UK's intelligence agency GCHQ has stepped up the fight against online scammers** and created a tool that blocks malicious emails that appear to be sent from government addresses, but are in fact run by cyber criminals. The blocking system can identify when "gov.uk" emails are being sent from IP addresses not associated with an official government computer and block them. GCHQ has been testing the system on emails from the fake "taxrefund@gov.uk" address, which was sending 58,000 messages a day.

Spymasters plan to build 'Great British Firewall'
Financial Times, Sam Jones, 2016 09 13
London - **Ambitious new plans are being drawn up by GCHQ to create a "Great British Firewall"** to block malicious websites countrywide and combat a doubling of serious cyber attacks threatening national security over the past year. Though still in its infancy, the scheme is intended to be a flagship project for the new National Cyber Security Centre -- a public-facing arm of GCHQ which will open next month to better co-ordinate the UK's digital defence efforts. The NCSC plan envisions private-sector internet service providers, such as BT, Sky or Virgin Media, voluntarily complying with its proposals, circumventing any need for legislation. Consumers will be able to opt out of the censorship should they wish in order to allay concerns over civil liberties.

Return to Table of Contents/ Retour à la table des matières

Australia / Australie

Intelligence agencies to be reviewed New era Security reshaping plan (Canada)
Canberra Times, David Wroe, 2016 09 18
Canberra - The **Turnbull government is set to embark on a major independent review of the nation's intelligence agencies** as Australia faces an unprecedented array of security challenges ranging from terrorism to the rise of China and cyber-spying. **Prime Minister Malcolm Turnbull's department has confirmed that it is putting in place arrangements for the first major intelligence review since 2011** and the third since the September 11, 2001 terrorist attacks on the US, which prompted a reshaping of intelligence efforts in Australia and among its allies. The review is expected to tackle the unprecedented need for the nation's six intelligence agencies to balance immediate security intelligence requirements to combat terrorism including "lone wolves" with longer-term considerations about geo-strategic changes flowing from the shift in power and wealth to the Indo-Pacific region. A spokeswoman for the Department of Prime Minister and Cabinet, which is setting up the review, told Fairfax Media: "We are working through a proposal for a periodic review and the details involved. It is expected that these considerations will take at least several weeks." It will **be headed by a senior retired intelligence official**. Sources have raised the name **of Allan Gyngell, who led the Office of National Assessments - the agency that collates intelligence into briefings for the Prime Minister and the national security committee of cabinet - from 2009 until 2013.** Dr Blaxland, a senior fellow at the Australian National University's Strategic and Defence Studies Centre, said cyber security was a major organisational challenge because intelligence agencies needed to co-operate on capabilities that were usually top secret with a wide range of organisations including other government departments and critical industries.Australia's intelligence community is made up of **ASIO, ONA, foreign intelligence outfit ASIS, the Defence Intelligence Organisation, the Australian Geospatial Organisation and the Australian Signals Directorate**. Australia's international intelligence co- operation will also likely be scrutinised in the review. The "five-eyes" arrangement in which Australia shares intelligence with the US, Britain, **Canada** and New Zealand is considered by insiders more vital than ever with each country constrained by resources amid a growing workload. Co-operation with regional democracies such as Japan and South Korea has also grown strongly in recent years.

PM talks up counter-terror collaboration
Australian Associated Press, Jennifer Rajca, 2016 09 18
Canberra - **Malcolm Turnbull intends talking up international collaboration in the battle against terrorism** during meetings in the US. The prime minister arrived in New York on Saturday ahead of the 71st session of the United Nations General Assembly, making his first stop the 9/11 memorial and museum with wife Lucy. Later reflecting on the attacks 15 years ago which were many months in the making, he warned the nature of terrorism continues to "mutate". "We have to ward ourselves against attacks like (9/11) in the future," Mr Turnbull told reporters. But there is also the threat of lone wolves, who are rapidly radicalised. "That's why we have to be relentless in our defence of our freedom," he said. Countries have to be ever vigilant in the face of the evolving threat.

Intelligence agencies recruiting hackers
Canberra Times, Henry Belot, 2016 09 17
Canberra - **Federal intelligence agencies are hiring hackers to test the security of government infrastructure and to attack foreign targets**. The recruitment drive, which offers recruits "a licence to hack", comes after a number of attacks on government agencies including the Department of Human Services during the census collection period. Other **targets include Austrade, the Defence Science Technology Group and the Bureau of Meteorology**, which was breached last year by Chinese-based hackers. Another 97 federal departments have

reportedly been told to encrypt more data amid hundreds of attempted intrusions every month. A Defence spokesman said the recruitment of hackers - termed "penetration specialists" -- was not a response to the census attack but a long-term commitment to boost capabilities. Earlier this year, Prime Minister Malcolm Turnbull announced a $230 million cyber security plan to "deter and respond to malicious cyber activities". Recruitment material calls on candidates to "be a force for good and defend Australia from the dark side", or to "go covert" and "catch Australia's phishing foes". The **Australian Signals Directorate** has been scouting schools, universities and technical colleges for talented students, with many now working for the intelligence agency. Professor Austin, an executive with the Australian Centre for Cyber Security, has also called for a national cyber security college to bolster the intelligence workforce.

Terror teams seek data access to identify threats
The Australian, Paul Maley, 2016 09 14
Sydney - **Counter-terrorism authorities could be given greater access to intelligence on criminals,** local police reports, medical data and welfare information to better identify potential terrorists. The government is examining ways information that might help identify people with extremist tendencies could be cross-checked with other data bases to home in on potential terrorists. The work was announced by **Malcolm Turnbull** in July and spearheaded by then counter-terrorism co-ordinator Greg Moriarty, who since has become the Prime Minister's foreign policy adviser. Since then, work has focused on examining the personality and behavioural traits of terrorists or extremists with a view to identifying potential markers, The Australian has been told.

Australia to extend money laundering laws
Reuters, Staff reporter, 2016 09 14
Sydney - The **Australian government is reviving long-stalled plans to extend anti-money laundering and counter-terrorist financing laws** to capture lawyers, accountants, real estate agents and jewellers, Justice Minister Michael Keenan said. The law reforms have been repeatedly shelved since mid-2007 after opposition from some of the affected sectors - most notably the legal profession. The first tranche of the anti-money laundering laws were put in place a decade ago to compel banks, fund managers and casinos to report the source of their money flows, but the anticipated follow-up to cover other sectors did not eventuate. The Australian government is preparing to release proposals to the public for consultation.

Return to Table of Contents/ Retour à la table des matières

New Zealand / Nouvelle-Zélande

MPs' emails continue to be monitored by Parliamentary Service until issue resolved
Stuff.co New Zealand, 2016 09 14
Auckland— Parliament has five options for dealing with Parliamentary Service's blocking and screening of MPs emails **- one of which is to scrap the encrypted system used by MPs altogether**. Speaker of the House, David Carter, addressed MPs concerns about their emails being monitored by Parliamentary Service on Wednesday after an investigation was called for on Tuesday. The issue was revealed when Labour MP Chris Hipkins had an email he was trying to send to a Fairfax journalist blocked on Monday night… An MP who had fallen victim to Parliamentary Service's snooping before was "shocked" by revelations it was up to its old tricks. **UnitedFuture leader Peter Dunne** had his email conversations with then-Fairfax journalist

Andrea Vance wrongly handed over to a ministerial inquiry by Parliamentary Service in 2013. The then-head of Parliamentary Service, Geoff Thorn, resigned amid the fallout. **Dunne had already quit as a minister prior to the ministerial inquiry after refusing to hand over his emails for an investigation into the leaking of a Government Communications Security Bureau (GCSB) report.**

Return to Table of Contents/ Retour à la table des matières

International

China / Chine

China says Canadian man it released treated 'based on law'
Agence France-Presse, Nomaan Merchant and Rob Gillies, 2016 09 16
Beijing - **China said Friday that a Canadian citizen it detained for two years over spying allegations was allowed to leave the country after a local court issued a verdict in his case**, but it refused to say what the verdict was or why he was detained at all. **Kevin Garratt's** return to Canada was announced Thursday by Prime Minister Justin Trudeau, who said he had pressed Garratt's case with top Chinese officials. Garratt had been indicted by prosecutors in Dandong, a city on the North Korean border where he and his wife ran a popular coffee shop and conducted Christian aid work for North Koreans. He and his wife, Julia, were arrested in August 2014 by the state security bureau. While his wife was released on bail, Garratt remained in custody. China's Ministry of Foreign Affairs, in a faxed statement Friday, said Garratt had been treated "according to law." It said China "fully guaranteed all kinds of procedural rights of Kevin Garratt, and fully respected and implemented the consular rights of the Canadian side," the ministry said. But the ministry declined to say what investigators found or what the outcome of the trial was.

Return to Table of Contents/ Retour à la table des matières

Russia / Russie

FSB warns 2 Russians trying to sell fake military secrets to CIA
ITAR-TASS World Service, Staff report, 2016 09 20
Moscow - **Two residents of a remote Siberian town Borzya in the Zabaykalsky region tried to feed the U.S. Central Intelligence Agency (CIA) with fabricated "secret information"** in exchange for money, a source in the regional directorate of Russia's **Federal Security Service (FSB) told TASS on Sept. 20**. "In 2015, a Borzya resident born in 1993, left a message on the CIA website suggesting to pass some secret information on the Russian military to the U.S. intelligence. He soon got an answer as the CIA took this proposition seriously and went for it," said the source. "In particular, the agency started inquiring about the military facilities' routine. However, the CIA representatives chose to avoid the topic of money at the time," said the source. Then the adventurous young man, who was working as programmer and could not know any military secrets, turned to a 20-year-old friend who was doing compulsory military service in one of the local bases.

Putin forms super-spy agency just like Stalin's
London Times, Tom Parfitt, 2016 09 19
Moscow - **Russia is to create a new spy ministry that unites several agencies into one powerful structure reminiscent of the Soviet KGB**. President Putin wants to strengthen control over the country's disgruntled elites and dampen flashes of protest despite a resounding win in parliamentary elections yesterday for the pro-Kremlin United Russia. With deep symbolism, the new **Ministry of State Security** (MGB) will carry the same name as the Stalin-era intelligence agency which existed between 1946 and 1953, before the creation of the KGB (Committee for State Security). The new mega-spy agency will combine domestic and overseas espionage operations under one roof. The plan was reported by Kommersant newspaper citing anonymous state officials. **Dmitry Peskov**, Mr Putin's spokesman, said that he could not confirm it, but he did not issue a denial.

Russia 'to revive the KGB' after Putin wins biggest majority
London Daily Telegraph, Marc Bennetts, 2016 09 20
Moscow - **Russia plans effectively to revive the KGB under a massive shake-up of its security forces**, a respected business daily has reported. A State Security Ministry, or MGB, would be created from the current Federal Security Service (FSB) , and would **incorporate the foreign intelligence service (SVR) and the state guard service (FSO), under the plans**. It would be handed all-encompassing powers once possessed by the KGB, the Kommersant newspaper said, citing security service sources. Like the much-feared KGB, it would also oversee the prosecutions of Kremlin critics, a task currently undertaken by the Investigative Committee, headed by Alexander Bastrykin, a former university classmate of President Putin. **The Kremlin has not commented.**

Law Enforcement; State Security Ministry may be established in Russia after extensive law enforcement reform – newspaper
Interfax News Agency, 2016 09 19
Moscow— A **state security ministry may be formed on the basis of the Federal Security Service and the Foreign Intelligence Service** as a result of the pending extensive reform of law enforcement and security agencies in Russia, while the Russian Investigative Committee may again become a part of the **Prosecutor General's Office** that currently supervises its activity, and functions of the Emergency Situations Ministry will be divided between the Defense Ministry and the Interior Ministry, the newspaper Kommersant said on Monday. Preparations for the reform started shortly after the president liquidated the Federal Migration Service and the Federal Drug Control Service and assigned their functions to the Interior Ministry, while the Interior Ministry Forces and some other police units were merged into the Russian National Guard, sources told the newspaper. "In fact, the **Federal Security Service** is planned to regain functions of the Soviet State Security Committee. The new entity is due to acquire the status of a state security ministry," the newspaper said with the reference to its source.

Russia May Create Ministry for State Security and Close Emergencies Ministry
Sputnik (Russia), Staff report, 2016 09 19
Moscow - **Russia may create the Ministry for State Security at the premises of the FSB that would gain the powers of the Foreign Intelligence Service (SVR)** and the majority of the Federal Guard Service's (FSO) departments, the Russian Kommersant newspaper reported, citing its sources. The Russian Investigative Committee could be returned to the Prosecutor General's Office, the newspaper added. According to the media outlet, the Ministry of the Russian Federation for Civil Defense, Emergencies and Elimination of Consequences of Natural Disasters could be closed down and its powers could be transferred to both the Defense Ministry and the Interior Ministry.

Russian hacking an issue of revenge and respect
Washington Post, Andrew Roth, 2016 09 17
Moscow - The **recent spate of embarrassing emails** and other records stolen by **Russian hackers is President Vladimir Putin's splashy response to years of what he sees as U.S. efforts to weaken and shame him on the world** stage and with his own people, according to Russia experts here and in the U.S. intelligence world and academia. Putin is seeking revenge and respect, and trying to reassert Russia's lost superpower status at a time of waning economic clout and an upcoming Russian election, according to interviews with specialists here and in Washington, with a senior U**.S. intelligence official**, recently retired CIA operations officers in charge of Russia, and the last three national intelligence officers for Russia and Eurasia analysis in the **Office of the Director of National Intelligence**. "He's saying, if you think you have the chops to do this - well, we do, too!" said Fiona Hill, a national intelligence officer for Russia during the George W. Bush and Obama administrations who is now at the Brookings Institution.

Return to Table of Contents/ Retour à la table des matières

Europe

Filières lyonnaises en Syrie : un suspect de Meyzieu sur les vidéos de l'État islamique
Le Progrès (Lyon), R.S., 2016 09 20
Lyon, France - **Plusieurs individus sont récemment apparus dans les procédures antiterroristes, suspectés d'avoir emprunté des filières de djihadistes depuis la région lyonnaise**. Les **enquêteurs de la DGSI** estiment avoir notamment identifié Brahim Nejara sur une vidéo de l'État islamique (EI), diffusée le 24 novembre 2015. Intitulé Paris s'est effondré , le film salue les attentats du 13 novembre et promet de nouvelles attaques. Plusieurs témoins ont confirmé la corpulence et le bégaiement de cet homme originaire de Meyzieu, qui se vante d'entraîner des troupes de Daesh au "free fight", qu'il pratiquait dans une salle de boxe de la région lyonnaise. Selon l'enquête de la DGSI, il serait parti en Syrie en décembre 2013, dans un 4X4 à 27 400 , achetés par des crédits à la consommation.

Les espions tchèques en Suisse se font pincer
24 Heures (Suisse), Gilles Simond, 2016 09 20
Berne - Le **Conseil fédéral rend publique une nouvelle affaire d'espionnage « Les services secrets tchèques, comme d'ailleurs ceux d'autres pays de l'Est, vouent un intérêt tout particulier à notre pays »** , constate la **Feuille d'Avis de Lausanne**,ce 20 septembre 1961. « Ce dernier, fort heureusement, reste vigilant et perfectionne sans cesse ses moyens de contre-espionnage » , rassure Jean-Pierre Chuard, correspondant à Berne du quotidien. La preuve? Une grave affaire impliquant des ressortissants tchécoslovaques - la quatrième depuis 1954 - a été révélée le jour précédent par le Conseil fédéral, à l'issue d'une séance extraordinaire. Ce dernier « a décidé de protester énergiquement auprès du gouvernement tchécoslovaque contre l'activité d'espionnage exercée par deux fonctionnaires de la légation de Tchécoslovaquie à Berne » . Jaroslav Lis, fonctionnaire de chancellerie, et Vaclav Smisek, attaché culturel, avec statut de diplomate, « ont incité un ressortissant tchécoslovaque occupé comme employé de laboratoire dans une grande entreprise suisse à travailler pour le **service d'espionnage tchécoslovaque** et à livrer sans interruption des informations sur les recherches faites dans les domaines de la physique et de la chimie, ainsi que sur les travaux de développement » , écrit le Département fédéral de justice et police.

Renseignement Impossible de savoir combien de personnes seront espionnées
24 Heures (Suisse), Arthur Grosjean, 2016 09 20
Berne - La **nouvelle loi permettra d'intercepter les données numériques**. Reste à savoir qui sera sur la liste C'est le jour et la nuit. Quand on pose la question du nombre des personnes qui seront espionnées avec la nouvelle loi sur le renseignement, soumise au vote le 25 septembre, les réponses divergent du tout au tout. Ce ne sera que quelques dizaines de cas par année, clament les partisans. Ce seront au contraire des millions, s'émeuvent les opposants. Pourquoi une telle différence de chiffres? C'est ce que nous avons voulu savoir. D'abord, une question de base. Combien de personnes sont surveillées par année par **le Service de renseignement de la Confédération (SRC)? Impossible de le savoir, car l'information est classée confidentielle**. Il apparaît cependant, dans le rapport de gestion du Conseil fédéral 2015, que le Département de la sécurité établit une liste détaillée des opérations secrètes et des groupements soupçonnés de menacer la sûreté intérieure ou extérieure. La liste est soumise pour approbation au Conseil fédéral, et à la Délégation des commissions de gestion pour information.

German prosecutors charge man with spying for Indian intelligence
DPA News Agency, 2016 09 20
Karlsruhe, Germany (dpa)--**German prosecutors have charged a 58-year-old civil servant with espionage on behalf of India's foreign intelligence** agency. The German national is suspected of "occupation as a secret service agent and disclosure of official secrets in 45 cases," the federal prosecutor's office in Karlsruhe said in a statement. The man is accused of spying on Indian nationals in Germany - mainly political dissidents and **Sikh extremists** - while working at a foreigners' registration office in the western state of North Rhine-Westphalia. He was apprehended by German authorities in February and has been in custody since. The date of the trial - set to take place in Berlin - has yet to be announced.

Dutch security service calls for end to chat app encryption
NL Times, Janene Pieters, 2016 09 19
The Hague - **Dutch intelligence service AIVD wants to restrict encryption on chat services like WhatsApp and Telegram as much as possible, head of the service Rob Bertholee said** in an interview with the Volkskrant. According to him, being able to read suspected person's communication is essential for "protecting the legal order". With this position, the AIVD is standing counter to the government. Dutch politics find strong encryption very important for protecting privacy and calls restricting its availability "undesirable". Bertholee does not understand this position. "Then you as government also have to accept that we are no longer able to read the communication of terrorists." **The AIVD head also does not understand why companies and privacy organizations** so strongly hammer on the privacy of users of chat services. "I also think that privacy protection is very important, but would the people who set privacy as an extreme goal be just as enthusiastic in pursuing it if they were the victims of an attack?" According to him, the threat towards the Netherlands has "never been this big".

Germany's intelligence agency illegally gathered data
Irish Times, Derek Scally, 2016 09 19
Berlin - **Germany's foreign intelligence agency (BND) illegally collected and stored masses of data from innocent German citizens who were unwittingly dragged into mass surveillance dragnets.** A leaked, classified report by the Federal Data Protection Commission (FDPC) found that, for every **BND** targeted surveillance operation, the intelligence agency was sucking up and storing data of 15 citizens not part of any investigation. "These infringements of constitutional rights are conducted without any legal basis and thus harm the constitutional right of informational self- determination of [innocent] people," the FDPC report adds.

Shouting at Americans: A Peek Into French Signals Intelligence (Canada)
Council on Foreign Relations, Alex Grigsby, 2016 09 16
Comment: Something remarkable happened a few months ago. **Bernard Barbier, the former head of signals intelligence (SIGINT) between 2006 and 2014 at France's foreign intelligence agency (DGSE),** gave a speech at one of France's top engineering schools in which he reflected on his career and **imparted some of his wisdom to students**. He also **said some things that he probably shouldn't have, like confirming that France was behind the Animal Farm advanced persistent threat, commenting on the SIGINT capabilities of European allies, and reacting to the revelation that the U.S. National Security Agency (NSA) had compromised the networks of the French presidency**. Last week, Barbier's speech surfaced on YouTube but was quickly taken down (UPDATE: A new version of the video is up here. H/T Boing Boing). However, it was up long enough for French daily Le Monde to transcribe some of the highlights. Here they are, paraphrased and translated from the original French. 1. "I got the order from Mr. Sarkozy's successor [current President Hollande] to shout at the Americans ... it was a great moment in my professional career" Barbier recalls that he was first informed of a possible compromise at the Élysée palace in 2012, when a former colleague working IT security at the palace reached out for analysis on a piece of malware. With the help of a new metadata capability the French obtained in 2012 and Edward Snowden's revelation of the NSA's QUANTUM capability in 2013, Barbier's staff concluded that the attack on the Élysée was the work of the United States. Barbier recalls: 2. "And yes, it was a Frenchman" In 2014, Le **Monde published documents from the Snowden archive revealing that Canada's SIGINT agency, the Communications Security Establishment (CSE), suspected that Paris was behind a cyber espionage campaign that began in 2009 targeting Iran's nuclear program but also targeting computers in Canada**. CSE was able to attribute the campaign to the French based on some reverse engineering revealing that the malware developer used references to a French children's cartoon character, Babar the Elephant.. (Note: Alex Grigsby is the assistant director for the Digital and Cyberspace Policy program at the Council on Foreign Relations.)

SBU to be reformed in line with NATO standards
Ukrinform, Staff report, 2016 09 15
Brussels - The **Security Service of Ukraine (SBU) will be included in the program of Ukraine-NATO cooperation on defense reform and security. Acting Head of Mission of Ukraine to NATO Yehor Bozhok said in an exclusive interview** with own Ukrinform correspondent in Brussels. "We include the SBU reform in the course of our cooperation with NATO," the diplomat said.

German intelligence agency says terror perpetrators are 'controlled from afar'
Deutsche Welle, Staff report, 2016 09 14
Berlin - After the arrest of three Syrian terror suspects residing in northern German refugee shelters, **Hans-Georg Maassen** has sounded the alarm. **"We are concerned about the new type of perpetrator who seems to be acting alone," the head of Germany's domestic intelligence agency, the Federal Office for the Protection of the Constitution (BfV),** told journalists in Berlin on Wednesday. Maassen said these potential attackers are presumably given orders by foreign terror leaders through encrypted instant messaging services. "This scenario is especially challenging for security authorities - as is the uncovering of sleeper cells," he stressed.

Bulgaria's Security Agency Deemed 181 Asylum Candidates 'Dangerous' in 2015
Sofia News Agency, Staff report, 2016 09 14

Sofia - The deputy head of Bulgaria's domestic security and counter-intelligence agency has said as many as 181 asylum candidates were considered a "threat to national security" last year. The State Agency for National Security (DANS) also took steps for the expulsion of 29 foreign nationals, its deputy chairman Oleg Petkov has told daily 24 Chasa. As many as 17 300 migrants were interviewed over the same period, Petkov has explained. (Profilers from DANS, the State Intelligence Agency, and the State Agency for Refugees are to hold interviews with all asylum candidates). His organization barred three foreign nationals from traveling via Bulgaria last year on suspicion they were willing to join a terrorist organization.

L'espion qui parlait trop
L'Express, E. Pa., 2016 09 14
Paris - **Les propos tenus par Bernard Barbier, l'ex-directeur technique de la sécurité extérieure (DGSE)**, devant les élèves de l'école Supélec, **ont déplu dans son ancienne maison**, tenue au secret. Diffusée sur YouTube, la conférence dans laquelle l'espion confirme le piratage de l'Elysée par les Américains (L'Express du 20 novembre 2012) a été retirée à sa demande. Mais elle a été copiée et rediffusée, suscitant des remous à Washington.

Le poste très stratégique du " dernier " commissaire européen britannique
Le Monde, Cécile Ducourtieux, 2016 09 14
Strasbourg - **En attendant le Brexit, l'ex-ambassadeur du Royaume- Uni en France, Julian King, sera chargé des questions de sécurité** Si l'on m'avait dit, il y a quelques mois encore, que je serais présent ici parmi vous, je ne l'aurais probablement pas cru. La situation est tout à fait singulière. " C'est par ces mots que Julian King, le probable futur commissaire britannique, a entamé son audition au Parlement de Strasbourg, lundi 12 septembre. M. King n'a pas hérité d'un portefeuille insignifiant, ridicule ou humiliant. Certains avaient évoqué pour lui, brièvement, le rôle de gestionnaire en chef des bâtiments de la Commission... Mais, à 52 ans, ce diplomate de carrière, pur produit du Foreign Office, s'est vu attribuer un tout nouveau maroquin, sur un **sujet stratégique : la sécurité.** Le poste a été créé sur mesure pour celui qui était encore, au début de l'été, ambassadeur du Royaume-Uni en France. Parmi ses priorités, renforcer les moyens financiers et humains d'Europol (l'agence des polices européennes) ou s'assurer que les décisions prises en matière de sécurité sont appliquées.

Résistances islamiques au Renseignement
Le Temps (Suisse), Valérie de Graffenried, 2016 09 14
Berne - **Nicolas Blancho et son Conseil central islamique suisse s'opposent à la loi sur le renseignement**. Le conseiller fédéral Guy Parmelin s'en est étonné. Le propre service d'analyse et de prévention du CCIS a été très peu sollicité « Dans cette campagne, je suis étonné de l'opposition du Conseil central islamique suisse. Je constate que l'organisation de Nicolas Blancho combat cette loi et c'est un signal plutôt inquiétant. » Cette petite phrase, le conseiller fédéral **Guy Parmelin l'a récemment lâchée dans Le Matin Dimanche, à propos de la loi sur le renseignement (LRens),** soumise en votation le 25 septembre. Avant d'ajouter: « Je ne vais pas aller jusqu'à dire que son organisation a quelque chose à se reprocher, car ce n'est certainement pas le cas. Mais cette campagne était aussi l'occasion pour certains milieux de prouver qu'ils condamnent le terrorisme et les risques de dérives en la matière. » Entrer dans les mosquées Nicolas Blancho et ses camarades combattent effectivement la **LRens**. Parce qu'ils se sentent dans le viseur du **Service de renseignement de la Confédération (SRC)** Cette loi permettra aux collaborateurs du SRC de procéder à des écoutes téléphoniques, d'infiltrer des ordinateurs grâce à des mouchards, de poser des caméras dans des appartements privés ou encore de pénétrer des mosquées.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Volkswagen Teams Up With ex-Shin Bet Chief on Cyber Security
Haaretz, 2016 09 15
Jerusalem - **Volkswagen is forming a company with the former head of Israel's Shin Bet intelligence agency to develop cyber security systems for internet-connected cars** and self-driving vehicles, the partners said in a statement on Wednesday. The new company, CyMotive Technologies, will be 40 percent owned by the German automaker and 60 percent by **Yuval Diskin and two former colleagues who also had senior posts in the Shin Bet**. The statement did not say how much Volkswagen would invest in the venture, which has an office in a suburb of Tel Aviv and will also open one in Wolfsburg, Germany. Building on its expertise in technology, Israel has emerged as a leader in the race to keep cars secure and prevent the nightmare scenario of a hacker commandeering your vehicle. International groups including Harman International Industries and IBM have already bought local companies or invested in research centers.

Israel suffers serious blow to intelligence gathering abilities
Jerusalem Post, Yaakov Lappin, 2016 09 15
Jerusalem - Unless operators succeed in stabilizing the systems onboard the **advanced Ofek-11 military satellite, launched on Tuesday from Palmahim Air Base, the defense establishment faces a real disappointment in its hopes to move forward Israel's space-based intelligence capabilities.** Little is known about the Ofek-11 satellite, other than the fact that it carries a payload of an advanced Elbit Systems-made electro-optic camera, and has a sophisticated propulsion system made by Rafael Advanced Defense Systems, which runs on hydrazine fuel. The satellite orbits the Earth every 90 minutes, and would have given IDF Military Intelligence, as well as other defense agencies, advanced visual intelligence abilities, enabling Israel to keep close tabs on developments in areas controlled by its enemies near and far..

Romanian ex-secret service agent held over plot against anti-graft chief
Times of Israel, Raoul Wootliff, 2016 09 15
Jerusalem - A **former Romanian secret service agent has been arrested for allegedly masterminding an operation that used an Israeli private intelligence firm** to intimidate a key anti-corruption official, prosecutors said on Wednesday. Daniel Dragomir is accused of trying to target people "he considered responsible" for his prosecution in 2015 on charges including money laundering. He is alleged to have asked a representative of Israeli firm Black Cube to hack the email of people including **Laura Kovesi, head of the National Anti-corruption Directorate (DNA),** in the hope of finding compromising information, prosecutors said. Kovesi, a 42-year-old former professional basketball player, is spearheading an unprecedented anti-corruption drive in one of Europe's poorest and most graft-prone nations. Probes by the DNA have cost a string of prominent Romanians their jobs in recent years.

Shortage of security professionals hindering UAE's cyber crime fight
The National (UAE), Jennifer Bell, 2016 09 14
Abu Dhabi - The **UAE must invest in training its own security professionals as a priority in the war against cyber crime**, as the global pool of skilled workers is shrinking, experts say. The Arab Gulf States Institute in Washington said **cyber attacks in the region cost US$1**

billion (Dh3.67bn) a year – an amount predicted to grow. The institute said the Middle East was fertile ground for cyber crime, with its wide use of technology and high-value targets. Mike Weston, vice president of Cisco Middle East, said that although there were more than a million cyber security positions available worldwide, the shortage of professionals to fill them was likely to grow rapidly.

Return to Table of Contents/ Retour à la table des matières

Asia / Asie

NICA: 170 job vacancies up for grabs

The Philippine Star, 2016 09 20

Manila— The **National Intelligence Coordinating Agency (NICA) is set to fill 170 job vacancies to perform its mandate and carry out its operations**. The agency is hiring analysts, researchers, information technology (IT) and technical personnel, lawyers and medical and dental staff, an advertisement published yesterday in The STAR showed.The advertisement said those who would be hired would be “part of the change” and would “contribute to national development.” NICA is looking for 10 analysts, 10 junior analysts, and 20 senior analysts. Analysts will be tasked to process and analyze information on national security concerns as well as prepare, review and update reports for policy makers, according to a job description posted on the NICA website.

Expert urges Korea to step up fight against money laundering

Korea Herald, Song Su-hyun, 2016 09 19

Seoul - The **head of a new international educational institute on anti-money laundering urged Korea to upgrade its legal system to better combat illegal financial transactions and terrorism financing.** Kevin Stephenson, the inaugural director of the Training and Research Institute under the **Financial Action Task Force**, or FATF TREIN, slated for official launch in Busan on Tuesday, acknowledged the efforts the Korean government has made so far to root out illegal financial transactions, but asked for more to be done. "Korea has done a great job by joining FATF as a full member in 2009 and successfully completing the FATF presidency," Stephenson said at a press conference Monday in Seoul. "However, since the FATF standards have been enhanced, Korea needs to upgrade its legal system and put more focus on effectiveness. Korea should focus on achieving more money laundering convictions and confiscating more proceeds of crime

Film Shines Light on South Korean Spy Agency's Fabrication of Enemies

New York Times, Cho Sang Hun, 2016 09 18

Seoul - They were beaten and forced to make false confessions. Many spent years in prison. Some were executed. Most were forgotten for decades. **Over six decades, scores of people were arrested by the South Korean authorities and accused of spying for North Korea, only to be exonerated**, sometimes decades later, long after many of them had served lengthy prison sentences. There has never been an official tally of the exact number of people affected, but a new film has documented almost 100 cases, some of which involved alleged spy rings with multiple people. The cases have mainly disappeared from public memory, but the new documentary, by the investigative journalist Choi Seung-ho, is lifting a veil on what he sees as one of the most shameful legacies of **South Korea's counterintelligence authorities**. Just before the closing credits of the film, **"Spy Nation**," a list of the names of the falsely accused scrolls down the screen. It is an eloquent indictment of the abuse of power engaged in by South

Korea's counterespionage agencies, especially the National Intelligence Service, in the name of fighting the Communist threat from North Korea.

Return to Table of Contents/ Retour à la table des matières

Africa / Afrique

La menace terroriste est "plus préoccupante" au niveau de la bande sahélo-sahélienne
All Africa, Journaliste maison, 2016 09 19
Paris - La **menace terroriste** est "plus préoccupante" au niveau de la bande sahélo-sahélienne qui **nécessite la poursuite du dialogue et la coopération entre l'Algérie et la France**, a indiqué lundi à Paris le président du Conseil de la nation, Abdelkader Bensalah. "Force est de constater que la menace terroriste est encore plus préoccupante au niveau de la bande sahélo-sahélienne, objet de nos discussions d'aujourd'hui", a-t-il précisé, soulignant que la situation est aggravée par "la prolifération de la criminalité organisée sous toutes ses formes, ainsi que par des actions subversives d'organisations terroristes transnationales visant la déstabilisation aussi bien de cette région, que celles de l'Afrique du Nord et du bassin occidental de la Méditerranée".

Return to Table of Contents/ Retour à la table des matières

Americas / Amériques

Light coverage/couverture légère.

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

28-09-2016 to/au 04-10-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Spies use C 51 to gather intelligence from Canadians detained overseas
Canadian Press, Jim Bronskill, 2016 10 04
Ottawa - **Canada's spy agency is using controversial powers under the C-51 anti-terrorism legislation to gather intelligence from Canadians held in foreign prisons,** a newly released memo reveals. **Amnesty International Canada and the NDP are expressing concerns about the potential pitfalls of the previously unknown information-sharing arrangement between the Canadian Security Intelligence Service and Global Affairs Canada**. In the House of Commons, **Public Safety Minister Ralph Goodale** stopped short of defending the arrangement Monday, saying a federal national security review would ensure the government's approach is consistent with ``what Canadians want.'' The spy service and Global Affairs made the sharing deal this year through the Security of Canada Information Sharing Act _ part of the omnibus security legislation known as C-51, says a secret May memo to Goodale from **CSIS director Michel Coulombe.** The provisions, ushered in by the previous Conservative government, expanded the exchange of federally held information about activity that ``undermines the security of Canada.'' ``Information collected by (Global Affairs Canada) through the provision of consular services can be directly relevant to investigations of threats to the security of Canada,'' says the heavily censored CSIS memo, obtained by The Canadian Press under the Access to Information Act. The sharing arrangement between CSIS and Global Affairs underscores the concerns raised by the privacy commissioner and reaffirms the NDP's desire to see C-51 repealed, said Matthew Dube, the party's public safety critic. ``The appropriate safeguards aren't in place.'' Neither Global Affairs Canada nor CSIS would discuss the sort of information the spy service hoped to obtain through the new sharing arrangement. Both agencies say they carry out their duties in accordance with relevant legal and privacy obligations.

The darker side of Intelligence
The Province (Vancouver), Dana Gee, 2016 10 04
Column: **The Romeo Section** Oct. 5, CBC 9 p.m. For its second season, creator Chris Haddock has planted the espionage thriller The Romeo Section firmly against the veiled landscape of dark government activity. **Set in Vancouver, the CBC-produced series' central storyline has operative Wolfgang McGee (Andrew Airlie) investigating an alleged terrorist incident. In doing so, he opens doors into the shadowy side of intelligence**. "I think there has been a lot of effort over the years by government agencies to keep the public's prying eyes off what is going on," said Haddock about the show's focus. To some, the government involved in shady, below-the-radar activities is the currency of conspiracy theorists. But a truly functioning democracy demands that the citizenry question authority. "Everyone treats conspiracy as a nasty word, but really, that is what we humans do," said Haddock, who has a long list of credits including DaVinci's Inquest, Intelligence and Boardwalk Empire. "If somebody is a conspiracy theorist, they might just be a good thinker. You can't just automatically dismiss them. "They said Edward Snowden was a conspiracy theorist until he comes up with the evidence," added Haddock from the set during the shooting of Season 2's eighth episode. "This is a guy who has done wet work in the field," said Airlie. "He's served some real time in some very dangerous scenarios and done things that most Canadians would like to believe that we don't do. **Sure, the CIA does stuff like that but CSIS doesn't do things like that**."

Balancing rights and security
National Post, Ralph Goodale, 2016 10 03
Op-ed: **Last week, the House of Commons began debate on Bill C-22 - a measure which is "long overdue" according to Wesley Wark, a national security professor at the University of Ottawa.** This legislation creates a special committee of members of Parliament and senators with extraordinary access to classified information, and a mandate to ensure that the government is effective at keeping Canadians safe, while equally safeguarding their rights and freedoms. It's a major boost in the accountability of those responsible for our collective security. The committee will be independent and non-partisan. Only four of its nine members (seven MPs and two senators) will be from the government. Ministers and parliamentary secretaries are not allowed. It will have the resources to get the job done. It will set its own agenda and report when it sees fit. **Unlike existing national security review bodies, it will not be siloed to one agency - the committee will be able to examine any department or agency responsible for any aspect of national security or intelligence, going wherever the evidence takes them.** It fills a major gap. Canada is the only "Five Eyes" country (Canada, the U.S., Britain, Australia and New Zealand) without a parliamentary review mechanism. Such a mechanism has been recommended repeatedly over the past decade - in two parliamentary reports, by two independent inquiries and by the auditor general. We've tried to learn from the experience of others, while crafting an approach for Canada that best suits our circumstances. The University of Ottawa's Craig Forcese - an expert on national security law - says the model in Bill C-22 " ... will be a stronger body than the U.K. and Australian equivalents." It will set a new standard. Note: Ralph Goodale is Canada's minister of public safety.

Canada's CIA Had No Policy for Collecting and Using Massive Amounts of Data
Motherboard Blog, Jordan Pearson, 2016 10 01
Ottawa- The **Canadian Security Intelligence Service** (CSIS), the country's CIA equivalent, **used large datasets to track and identify persons of interest without a policy to guide their collection, retention, or use, according to a new report from Canada's intelligence watchdog.** CSIS is tasked with tracking terror suspects within and outside of Canada, and the investigation was undertaken in the context of new, and incredibly broad, powers bestowed upon the spy agency by the controversial Bill C-51. The **Communications Security Establishment**, CSIS' sister organization and Canada's answer to the NSA in the US, **stopped sharing metadata with foreign spying partners under similar circumstances last year** when an internal review concluded that the agency had handled data improperly. The new report also suggests that CSIS employed overly generous interpretations of the law in order to collect more data than it was supposed to.

Mali: le Canada planifie son soutien aux opérations françaises
45eNord.ca, Nicolas Laffont, 2016 10 01
Ottawa - Le **ministère de la Défense nationale a indiqué** à 45eNord.ca dans un courriel que même si ce n'est pas encore finalisé «**les Forces armées canadiennes travaillent actuellement sur des plans pour assurer la continuité du transport aérien soutien stratégique aux efforts antiterroristes français dans la région du Sahel**. Comme ce fut le cas avec la récente contribution des FAC en 2015, les avions de transport aérien seront probablement utilisés pour le transport de troupes et de matériel français».

CSIS suspends some bulk data mining programs pending new guidelines
Globe and Mail, Colin Freeze, 2016 09 30
Ottawa - **Canada's domestic spy service has halted its "bulk collection" of data after criticisms were raised within government about the lawfulness of such technique**. A watchdog agency's new report about the Canadian Security Intelligence Service speaks of

littleknown CSIS data- mining programs, and of how some have recently been suspended because of a lack of clear rules and guidelines surrounding them. CSIS is said to have wanted to leverage big pools of data "to identify previously unknown individuals of interest by linking together types of information that have mirrored threat behaviour," according to the report. But after concerns raised in the report, "CSIS agreed to halt ingesting bulk data sets pending" new rules. **These findings are from the Security Intelligence Review Committee (SIRC), the watchdog agency that tabled its annual report in Parliament on Thursday**. The cryptic discussion of CSIS's "data management and exploitation activities" is intriguing on several levels. Talk of spies "ingesting" data in "bulk" has had connotations of intelligence officials indiscriminately amassing citizens' telecommunications records. Yet CSIS officers, who work to track terrorists within Canada, are generally understood to handle cases one wiretapping warrant at a time. This makes them more like conventional police detectives than the foreignfocused signals-intelligence - or "sigint" - spies who deal in volume. This week, the federal Privacy Commissioner called for Parliament to pass new laws after finding Canada's other intelligence agency had been careless with records about the logged telecommunications of Canadians. **Communications Security Establishment** (CSE), a foreignfocused "sigint" agency, says that whenever it collects Canadians' telecommunications trails, it does so only "incidentally." That's because it is pursuing foreign records in enormous volumes. While CSIS and CSE have vastly different mandates, they also have adjacent headquarters.

Military will bolster French counterterror operation
Canadian Press, Lee Bethiaume, 2016 09 30
Ottawa - As the Liberal government contemplates which United Nations peacekeeping mission to join, the **Canadian military is gearing up to support a major French counterterrorism operation in northern Africa.** Defence officials say planning is underway for Canada to send military transport aircraft to help France in its fight against Islamic militant groups in five countries: Mauritania, Mali, Burkina Faso, Niger and Chad. About 3,000 heavily armed French troops have been hunting al Qaedalinked fighters in the region, called the Sahel, since August 2014. Code-named Operation Barkhane, the mission has also been recently tasked with supporting UN peacekeepers in Mali if required.

New Democrats want Trudeau government to rescind torture directive
Canadian Press, Jim Bronskill, 2016 09 29
Ottawa - The **NDP is calling on the Liberal government to immediately rescind a directive that allows security agencies to use information that may have been obtained through torture**. The Liberals _ who opposed the ministerial directive while in opposition _ say it will be reviewed as part of a sweeping examination of national security policy. "The input of all Canadians, including all members of Parliament, is most welcome," said Scott Bardsley, a spokesman for Public Safety Minister Ralph Goodale.. The **policy applies to the Canadian Security Intelligence Service, the RCMP, the Canada Border Services Agency, the Communications Security Establishment and National Defence.** Human rights advocates have roundly criticized it as effectively condoning the torture of people in overseas prisons, contrary to international law and Canada's United Nations commitments.

C-51: de l'information échangée sans garde-fou
Le Devoir, Hélène Buzzetti, 2016 09 28
Ottawa - Sitôt adoptée, sitôt utilisée. **L'appareil gouvernemental a eu recours à la Loi antiterroriste (C-51) dès les premiers mois de son entrée en vigueur, mais les ministères fédéraux n'ont pas pris les précautions qui s'imposaient**, déplore le **commissaire à la protection de la vie privée du Canada, Daniel Therrien.** Le projet de loi C-51, adopté dans la controverse en 2015, n'a pas seulement accordé de nouveaux pouvoirs aux forces policières et

au Service canadien du renseignement de sécurité (SCRS). Il a aussi autorisé les 128 institutions fédérales (ministères, agences, Gendarmerie royale du Canada, etc.) à s'échanger des informations qu'elles détiennent sur des citoyens canadiens. **Dans son rapport annuel déposé mardi, Daniel Therrien révèle que, au cours des six premiers mois d'application de la loi, de l'information a été communiquée à 58 reprises.**

Canada's anti-terrorism legislation is a failure, says visiting professor
New Brunswick Telegraph Journal, John Chilibeck, 2016 09 28
Fredericton - **Ottawa's anti-terrorism legislation that was quickly put together following deadly attacks in 2014 has always bugged Kent Roach**. The University of Toronto law professor has spent much of his career working on terrorism cases, including as director of research for the inquiry into the **Air India bombing of 1985** that killed 329 people, most of them Canadians.. **Roach and Craig Forcese, a law professor at the University of Ottawa, both testified to House of Commons and Senate committees before the bill was passed, but their advice was largely ignored**. They have since published the book False Security: The Radicalization of Canadian Anti-Terrorism, in which they argue the law was hastily and poorly drafted, with the government making no transparent attempt to learn from the security failures that might have led to the two October 2014 attacks. Justin Trudeau's Liberal government has promised to revise the anti-terrorism legislation next year and provide more oversight, but based on a green paper released last week that sets the stage for more debate and discussion, the two professors have little faith the right changes will be made. Another major flaw, he says, is the legislation gives Canada's spy agency, the Canadian Security Intelligence Service, too many powers to withhold evidence from police. He says this could lead to fewer prosecutions of terrorists. "**We want CSIS and the RCMP sharing information and working together,**" he said. "If there's one thing we've learned in Canada, we are not very good at terrorism prosecutions."

Privacy watchdog urges Ottawa to pass 'metadata' legislation
Globe and Mail, Colin Freeze, 2016 09 28
Toronto - **Canada's privacy czar is calling on the Liberals to fulfill a promise to pass laws constraining the federal spies who are allowed to capture records of Canadians' phone and Internet activities.** The **Communications Security Establishment needs new legislation because it has not been careful enough in handling such material, says Daniel Therrien, the Privacy Commissioner of Canada.** "The National Defence Act should be amended," he said in an interview. "I would want some clarity around the standards used to collect and share 'metadata.' Right now, the act is completely silent on this." "Metadata" is the name federal officials give to phone logs, Internet exchanges and similar activity that spy agencies can electronically intercept in bulk. The substance of the underlying communications and the identities of communicators are not known. CSE has been tasked with providing intelligence about foreigners to the Canadian cabinet since the 1940s.

Feds failed to assess privacy implications of C-51 info-sharing: watchdog
Canadian Press, Jim Bronskill, 2016 09 28
Ottawa - The **government hasn't done enough to protect the privacy of "law-abiding Canadians" from new information-sharing powers in the omnibus security legislation known as C-51, says a federal watchdog. Privacy commissioner Daniel Therrien** said Tuesday he was surprised that many federal agencies did not examine the effect the powers in the controversial Conservative bill would have on people's personal information. In his annual report, Therrien recommended agencies carry out formal privacy impact assessments _ a key tool required under government policy when departments set up any new program or activity involving personal information. The **Security of Canada Sharing Information Act**, part of C-

51, expanded the exchange of federally held information about activity that "undermines the security of Canada." Therrien also **called** Tuesday **for amendment of the National Defence Act to clarify the powers of Canada's cyberspy agency, the Communications Security Establishment, along with specific legal safeguards to protect the privacy of Canadians.**

Watchdog warns terror bill threatens privacy
Toronto Star, Alex Boutilier, 2016 09 28
Ottawa - **Law-abiding Canadians are at risk of having their personal information scooped up by broad new powers granted to Canada's security agencies**, according to a new report. **Privacy commissioner Daniel Therrien** said Tuesday that the federal government failed to assess the privacy implications of the new information-sharing powers granted to 17 departments and agencies under Bill C-51.. Under Bill C-51, the controversial terrorism laws brought in by the previous Conservative government, several security and law enforcement agencies can share information on "activities that undermine the security of Canada." The broad powers were granted to security agencies such as CSIS and the RCMP, but also to departments handling immigration, health, foreign affairs and transportation. Therrien's office found the powers had been used a total of 110 times over six months.

Ex-CSIS official backs Canada's attempt to get cyber promise from China
It World Canada, Howard Solomon, 2016 09 28
For several years **Western governments have blamed official Chinese or Chinese-government backed groups for hacking into databases of public and private organizations**. But a year ago the U.S. president Barack Obama and Chinese president **president Xi Jinping** signed an agreement not to direct or support cyberattacks that steal corporate data for economic benefit. Now **Canada wants to do the same**. A spokesman for Public Safety minister Ralph Goodale told the Globe and Mail that this country will try to get a similar agreement, which has also been negotiated between China and the United Kingdom. **The idea has the support of Ray Boisvert**, a former assistant director for intelligence at the **Canadian Security Intelligence Service** (CSIS) who now has his own security consulting company. "I do support this type of approach," he said in an email to ITWorldCanada.com.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

U.S. intelligence community opposes limits to privacy watchdog: memo
Reuters, Dustin Volz, 2016 10 04
Washington - The **U.S. intelligence community does not support pending congressional legislation that would curtail the authority of a privacy watchdog that advises the president on government surveillance programs, according to an unclassified memo** seen by Reuters. The position amounts to a rare show of support for the Privacy and Civil Liberties Oversight Board, or PCLOB, from the spy agencies it is designed to oversee. It came in a letter to the leaders of congressional intelligence committees that outlined opposition to several sections of an annual intelligence funding bill awaiting action in Congress. President Barack Obama's senior advisers would recommend a veto of the bill if Congress does not address the concerns raised, the letter said. The intelligence community "strongly opposes" part of the proposed legislation seeking to limit the jurisdiction of PCLOB to the privacy rights of Americans, and not foreigners, the letter, signed by Director of National Intelligence James Clapper, reads.

Keith Gartenlaub, Target in China Spy Probe, Appealing Porn Sentence
Newsweek, Jeff Stein, 2016 10 03
New York - A **former Boeing engineer who was convicted on a controversial pornography possession charge after the government failed to make a Chinese espionage case against him says he is appealing his sentence. Keith Gartenlaub**, a senior computer systems manager at Boeing's Long Beach, California facility, came under suspicion in 2013 after an FBI agent read a magazine article suggesting China had a spy inside the aerospace company. The agent's concerns were heightened when he learned that Gartenlaub and his Chinese-born wife made frequent visits to Shanghai, according to court documents. Armed with a secret warrant from the **Foreign Intelligence Surveillance Court**, which authorizes highly classified investigations, **FBI agents** obtained Gartenlaub's emails and phone records, broke into his house to copy his computer files and began following the couple around. But after 21 months the agents could not make a case that either was involved with spying for China. They did, however, find caches of child pornography on four of Gartenlaub's hard disks, two of which came from a beach house he previously shared with friends.

Tunisian men detail CIA black site torture involving electric chair and more
The Guardian (London), Spencer Ackerman, 2016 10 03
New York - **Two Tunisian men held in secret CIA prisons for more than a year have told a leading human rights organization they were tortured with gruesome and previously unknown techniques**. The men, who were released to Tunisian custody in 2015, described being threatened with placement in an electric chair at a black site prison in Afghanistan in 2002; being beaten with metal batons while their arms were suspended by a bar above their heads; and having their heads pushed into barrels of water. One of the men, Ridha al-Najjar, was a pivotal detainee for the CIA, which believed him to be a bodyguard for Osama bin Laden. Najjar was the first man taken by the CIA to the black site, which was code-named Cobalt and was where at least one detainee is known to have died. His interrogation became a template for others at the site, according to the CIA inspector general. Najjar said the interrogators forcibly inserted something into his anus. According to a footnote in the 2014 Senate intelligence committee's investigation into torture, John Brennan, now CIA director, was among the senior CIA officials briefed in the summer of 2002 on the interrogation plan for Najjar. According to the Senate report, the plan included isolation, "'sound disorientation techniques', 'sense of time deprivation', limited light, cold temperatures, and sleep deprivation".

Pentagon Paid for Fake 'Al Qaeda' Videos
The Daily Beast, Crofton Black & Abigail Fielding-Smith, 2016 10 02
Washington - The **Pentagon gave a controversial UK PR firm over half a billion dollars to run a top secret propaganda program in Iraq**, the Bureau of Investigative Journalism can reveal. **Bell Pottinger's** output included short TV segments made in the style of Arabic news networks and **fake insurgent videos which could be used to track the people who watched them,** according to a former employee. The agency's staff worked alongside high-ranking U.S. military officers in their Baghdad Camp Victory headquarters as the insurgency raged outside. Bell Pottinger's former chairman Lord Tim Bell confirmed to the Sunday Times, which has worked with the Bureau on this story, that his firm had worked on a "covert" military operation "covered by various secrecy documents." Bell Pottinger reported to the **Pentagon, the CIA and the National Security Council on its work in Iraq**, he said. Bell, one of Britain's most successful public relations executives, is credited with honing Margaret Thatcher's steely image and helping the Conservative party win three elections. The **agency he co-founded has had a roster of clients including repressive regimes and Asma al-Assad, the wife of the Syrian president.**

Shadow Brokers' Whine That Nobody Is Buying Their Hacked NSA Files
Motherboard Blog, Joshua Kopstein, 2016 10 02
Washington - The **hacking group responsible for stealing a large cache of National Security Agency hacking tools is very upset that no one seems to be bidding on their pilfered** files. Early Saturday morning, the person or group which calls itself **"TheShadowBrokers"** authored another bizarre rant, expressing their annoyance at the seeming lack of interest in ponying up bitcoins to release the full set of stolen files. "Peoples is having interest in free files ...

U.S. spies finally embracing iPhones, wireless connections
Bloomberg, Nafeesa Syeed, 2016 10 02
Washington - **U.S. spies are catching up to the masses in their gradual embrace of 21st-century technology,** from installing wireless connections in secure facilities to wielding iPhones and tablets, according to an official with the **U.S. National Geospatial-Intelligence Agency**. "We'd be cutting off our noses to spite our faces by denying us those kinds of tools," Matt Conner, deputy chief information security officer of the agency, said in an interview. The NGA provides intelligence to other parts of the government from battlefield maps to satellite imagery of national disasters. It's among agencies that are working with the Director of National Intelligence to study how to maximize the use of secure wireless networks and devices, while still maintaining the cover that spies need.

Extremist Imam Tests F.B.I. and the Law's Limits
New York Times, Scott Shane, 2016 10 01
Washington - For more than a decade, **Suleiman Anwar Bengharsa** has served as a Muslim cleric in Maryland, working as a prison chaplain and as an imam at mosques in Annapolis and outside Baltimore. An **affidavit filed in federal court by the F.B.I. says that Imam Bengharsa, 59, supplied $1,300 in June 2015 to a Detroit man who used it to expand his arsenal of firearms and grenades**. The man, Sebastian Gregerson, 29, a Muslim convert who sometimes calls himself Abdurrahaman Bin Mikaayl, was arrested in late July and indicted on explosives charges. Nearly a year ago, in fact, the F.B.I. said in a court filing -- accidentally and temporarily made public in an online database -- that **agents suspected the two men were plotting terrorism.** "Based on the totality of the aforementioned information and evidence, there is reason to believe that Bengharsa and Gregerson are engaged in discussions and preparations for some violent act on behalf of" the Islamic State, an agent wrote.

Effort to recognize World War II spies hung up in Congress
Associated Press, 2016 10 01
McLean, Va— **Spies don't work for fame or acclaim.** But **after 75 years, the men and women who served behind the enemy lines in Nazi Germany and the Pacific theater during World War II wouldn't mind some recognition**. Legislation to award the spies the Congressional Gold Medal has passed the Senate and has more than 300 sponsors in the House, yet the bill is being held up by House Republicans, who recently enacted rules that require a special waiver to grant the medal to groups of people. "I would be extremely proud to get a gold medal for what we did for our country," said Frank Gleason, 96, **one of the few remaining veterans of the Office of Strategic Services,** the World War II-era forerunner to the CIA. "What we did was a little exciting." The holdup frustrates a group of veterans whose numbers continue to dwindle as time marches on. "We're all in our mid 90s," said Irv Refkin, 95, who was recruited by OSS because of his German language abilities, which he used to gather intelligence. "We're not going to be here that long."

FBI files reveal how Clinton server was created in K Street lab
Fox News, Catherine Herridge & Pamela K. Browne, 2016 10 01
Washington - If Hillary Clinton's 'homebrew' server ever got the Mary Shelley treatment, **IT specialist Bryan Pagliano** would make a fine Dr. Frankenstein - **FBI documents reveal new details about how he painstakingly created the machine over a series of months while working in a room along Washington's storied K Street**. According to files released last Friday evening, Pagliano worked to design and build the now-infamous server inside a room once used as part of Clinton's campaign headquarters. On the street known as Washington's power corridor, Pagliano even used computer remnants from Clinton's failed 2008 presidential bid, where he had worked as an **IT specialist**. Pagliano was one of five people who received limited immunity from the Justice Department, has taken the Fifth and refused to testify before Congress.

FBI partly blames Snowden for reduction in email, phone surveillance
Washington Times, Andrea Noble, 2016 09 30
Washington - The **FBI's use of a surveillance statute to collect Americans' phone and email records has declined since details about the program were leaked by Edward Snowden in 2013, a watchdog report has found**. The FBI's use of Section 215 of the Patriot Act to obtain "business records" as part of national security investigations peaked in 2012, with the **Foreign Intelligence Surveillance Court approving 212 orders** seeking records, according to a report released Thursday by the Justice Department's inspector general's office. The program was publicly disclosed in June 2013 after the **former National Security Agency contractor** leaked information to the press. That year, the number of orders authorized by the court dropped to 179. The number of orders approved by the court has continued to decrease annually, with 142 orders approved in 2015.

New U.S. 'secret' clearance unit hires firm linked to 2014 hacks
Reuters, 2016 09 30
Washington— A **U.S. government bureau set up to do "secret" and "top secret" security clearance investigations has turned for help to a private company whose login credentials were used in hack attacks that looted the personal data of 22 million current and former federal employees,** U.S. officials said on Friday. Their confirmation of the hiring of **KeyPoint Government Solutions** by the new **National Background Investigations Bureau (NBIB)** comes just days ahead of the bureau's official opening, scheduled for next week. Its creation was spurred, in part, by the same hacks of the Office of Personnel Management that have been linked to the credentials of KeyPoint, one of four companies hired by the bureau. The officials asked not to be named when discussing sensitive information. KeyPoint representatives did not respond to requests for comment sent by email and left on the company CEO's voice-mail.

Lawmakers Aim to Narrow Terror-Victims Bill
Wall Street Journal, Kristina Peterson, Carol E. Lee, 2016 09 30
Washington - **Leading lawmakers said Thursday they were working on ways to mitigate possible unintended consequences of legislation letting Americans sue foreign governments over terrorist attacks**, just one day after both the House and Senate soundly overrode President Barack Obama's veto of the bill. Some lawmakers expressed buyer's remorse over the legislation, which would enable victims of the Sept. 11, 2001 terror attacks and their families to sue Saudi Arabia, worrying that the bill could spark reciprocal lawsuits and put Americans abroad in the legal crosshairs of foreign governments.

Ex-CIA, FBI Official to Head New Background Check Agency

CQ Today, 2016 09 29
Washington— The **Obama administration on Thursday named a former senior security official with the FBI and CIA to lead the newly created agency to handle federal background checks** as the government overhauls a system that has been plagued by delays and plundered by hackers. **Charles S. Phalen Jr. will head the new National Background Investigations Bureau**, which the White House began setting up in January in an effort to streamline the clunky security clearance process and prevent security breaches like the one that compromised millions of files at the Office of Personnel Management. The NBIB takes over responsibility for handling federal background checks from the Federal Investigative Services. That transition will officially begin on Oct. 1. Phalen, who most recently worked as vice president for corporate security at Northrop Grumman, said his top priority was accelerating the pace of background investigations.

The FBI Wanted to Target Yemenis Through Student Groups and Mosques
The Intercept, Cora Currier, 2016 09 29
Washington - The **FBI envisioned infiltrating mosques and Muslim student associations to look for young Yemenis to serve as informants**, according to an internal presentation obtained by The Intercept. The document suggests that agents scour Facebook "to find individuals who are dramatically increasing their levels of piety -- that's the demographic you want." "Since we're looking for young people re-engaging with their Islamic faith," it continues, "the local MSA [Muslim Student Association] is a great place to start." The 24-slide presentation, prepared for a Source Development Unit in the **FBI's Directorate of Intelligence**, is titled "Responding to the Yemeni Threat: Scenarios for CHS Development," using the bureau's lingo for informants, which it calls "confidential human sources." The document is undated, but from references in the text, it appears to have been prepared around 2010 or 2011 by **Centra Technology Inc**., a company selling intelligence services. Centra Technology has had regular contracts with the FBI since 2008, including for training courses vaguely described in contract records as "analytic tools and techniques." Centra did not respond to a request for comment.

Veteran CIA man to lead new background investigations bureau
Washington Post, Joe Davidson, 2016 09 29
Column - If the **new National Background Investigations Bureau (NBIB)** needs a director who has suffered the onerous process of getting permission to know Uncle Sam's secrets, **Charles Phalen** fits the bill. He is the first director of NBIB, announced in January to strengthen and modernize a clearance process that has suffered from backlogs, cheating by a major contractor and high-profile lapses. Phalen's resume depicts him as natural for the gig. He joined the CIA in 1981 and left 30 years later as director of security. During that period, he also had stops of about three years each at the FBI and the National Reconnaissance Office. "Personnel security has been in my blood," said Phalen, 65, a Fairfax County, Va., resident, by telephone. He takes office Thursday.

CIA Director Calls 9/11 Legislation 'Badly Misguided'
The Atlantic, Claire Foran, 2016 09 29
Washington - **CIA Director John Brennan warned against the national security risks of legislation that would allow families of victims of the September 11, 2001 terror attacks to sue the government of Saudi Arabia** on Wednesday. "I think the legislation is badly misguided and doesn't take into account the negative impact on U.S. national security," Brennan told Jeffrey Goldberg at the Washington Ideas Forum presented by The Atlantic and the Aspen Institute. Brennan added: "We all recognize that the emotions associated with 9/11 are still quite palpable [and] .... the victims' families are still seeking justices, but the 9/11 commission report said that there was no evidence that the Saudi government as an institution or senior Saudi

officials, individually, were responsible for the 9/11 attack." The CIA director cautioned that the implications of the legislation extend far beyond potentially damaging the relationship between the United States and Saudi Arabia.

Donald Trump proves he is unfit, unserious and unprepared on national security
Washington Post, Michael Vickers, Michael Morell, 2016 09 29
Op-ed - **Donald Trump showed again during Monday's presidential debate the many ways in which he is unfit to be president**. But nowhere did he reveal himself to be as temperamentally unfit, unserious, **unprepared and incoherent as he did on the topic of national security**. Trump continued to question the global alliance system that has served U.S. national security interests so well since World War II. He continues to see our relationships with our closest allies and partners solely in terms of cost -- who is paying how much of the bill. He does not see all the benefits that have accrued to the United States from this system, including the stability of Europe and East Asia that has made this a more secure and prosperous nation.. Note: Michael Vickers was undersecretary of defense for intelligence from 2011 to 2015 and assistant secretary of defense for special operations, low- intensity conflict and interdependent capabilities from 2007 to 2011. Michael Morell was deputy director of the CIA from 2010 to 2013, and twice served as acting director during that time. They have both endorsed Democrat Hillary Clinton for president.

Pentagon's 5,000-Strong Cyber Force Passes Key Operational Step
Bloomberg News, Nafeesa Syeed, 2016 09 29
Washington - A 5,**000-person Pentagon force created to bolster military computer networks and initiate cyber attacks against terror groups should be ready to carry out its mission by the end of the week**, a key step in improving the U.S.'s ability to respond to hacks by overseas adversaries. The **Cyber Mission Force** will reach "initial operational capability" by Friday, said Colonel Daniel J.W. King, a Cyber Command spokesman, in an e- mail.

The Legend of Saint Comey
Wall Street Journal, Editorial Board, 2016 09 29
Editorial - **No one has cultivated an image of public virtue better than FBI director James Comey**, so he was in high dudgeon Wednesday when mere mortals like elected Member of Congress challenged his investigation of Hillary Clinton's email violations as Secretary of State. "You can call us wrong, but don't call us weasels. We are not weasels," Mr. Comey declared Wednesday at a House Judiciary Committee hearing. Weasels or not, Mr. Comey did little to rebut the suspicion that he handled the Clinton probe with tender loving political care. Recall that in July Mr. Comey held a remarkable press conference in which he announced that Mrs. Clinton shouldn't be prosecuted for mishandling classified information. But it isn't his job to make prosecutorial decisions. That's the duty of Justice Department prosecutors.

Hackers have attempted more intrusions into voter databases, FBI director says
Washington Post, Matt Zapotosky, 2016 09 28
Washington - **Hackers have attempted more intrusions into voter registration databases since those reported this summer, the FBI director said** Wednesday, and federal officials are urging state authorities to gird their systems against possible other attacks. Testifying before the House Judiciary Committee, FBI director **James B. Comey** said that the bureau had detected scanning activities -- essentially hackers scoping out a potential attack -- as well as some actual attempted intrusions into voter registration databases. He said those attempts were beyond what had been made public in July and August, likely referring to hacking efforts in Illinois and Arizona, though he offered no other specifics. "

CIA Director: We 'have to assume' terrorist activity in the U.S.
CNN.com, Tom Kludt, 2016 09 28
Washington - The **director of the CIA said Wednesday despite the government's best efforts, the likelihood of terrorist activity in the United States is strong**. "So I think we have to assume there's something here in the states," said **John Brennan**, in an interview for CNN's "Erin Burnett OutFront" that will air Wednesday night. "We have to be relentless in terms of going after them." Brennan, who was appointed to lead the CIA shortly before President Barack Obama's second term, said "it's impossible to say" whether ISIS has operatives or cells in the United States, and he credited the "tremendous advances in information sharing and interaction between federal officials" in making it difficult for terrorists to operate in the country.

FBI defends prior reviews of terror suspects
USA Today, Kevin Johnson, 2016 09 28
Washington - **FBI Director James Comey defended the bureau's pre- attack reviews of operatives in recent U.S. terror strikes** - including the gunman in the Orlando massacre and the suspect in the bombing campaign in New York and New Jersey - **telling a Senate panel Tuesday that the agency has the resources to keep pace with the threat**. Questioned at one point about whether the bureau could have thwarted the Orlando attack and the recent New York bombing by pushing harder when agents were alerted to prior suspicious behavior by suspects in both cases, Comey repeatedly told Sen. Rand Paul, R- Ky., that the lawmaker's descriptions of the FBI's actions were "wrong."

FBI probes hacks targeting phones of Democratic Party officials: sources
Reuters, Mark Hosenball, 2016 09 28
Washington - The **FBI is investigating suspected attempts to hack mobile phones used by Democratic Party officials as recently as the past month**, four people with direct knowledge of the attack and the investigation told Reuters. The revelation underscores the widening scope of the U.S. criminal inquiry into cyber attacks on Democratic Party organizations, including the presidential campaign of its candidate, former U.S. Secretary of State Hillary Clinton. U.S. officials have said they believe those attacks were orchestrated by hackers backed by the Russian government, possibly to disrupt the Nov. 8 election in which Clinton faces Republican Party candidate Donald Trump. Russia has dismissed allegations it was involved in cyber attacks on the organizations. The more recent attempted phone hacking also appears to have been conducted by Russian-backed hackers, two people with knowledge of the situation said.

Fewer than one in five State Dept employees with security clearance completed classified info training
Fox News, Catherine Herridge, 2016 09 28
Washington - **Fewer than one in five employees with a security clearance at the State Department has completed the mandated training for handling classified information as required** by a 2009 Executive Order signed by President Obama, according to a new report from the government watchdog with oversight. "Based on training records obtained from the Foreign Service Institute, the OIG (Office of the Inspector General) found that less than 14 percent of security-cleared employees had completed the required training within the timeframe considered in this review. Moreover, only 20 percent had completed the training even one time since the outset of the training program," the report said.

Senior national security official to leave Justice Department
Reuters, Staff report, 2016 09 27
Washington - A **senior U.S. Justice Department official who oversaw efforts to prosecute Islamic State sympathizers and pursue cyber criminals is leaving the Obama**

administration next month, he told Reuters on Tuesday. **Assistant Attorney General John Carlin, chief of the national security division at the Justice Department, is departing on Oct. 15,** less than a month before the U.S. presidential election. Carlin, 43, confirmed his departure, expected to be announced later on Tuesday, in an interview with Reuters. The departure comes as the Obama administration has struggled to develop clear guidelines on how to pursue hacking amid growing threats posed by foreign nation-states and criminal groups. He declined to say where he was headed next. **Carlin said he intended to spend time with his family before starting a new job, likely involved in cyber security.**

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

Islamist terrorists tried to kill MI5 spy
London Daily Telegraph, Ben Farmer, 2016 10 03
London - A **former MI5 spy has revealed he was nearly kidnapped and beheaded by Islamist extremists who had plotted to kill a British intelligence operative**. The spy narrowly escaped being lured into a trap by fanatics he was following and it was later discovered they had made preparations to film his execution. The incident is recalled in a new book by the former intelligence officer who spent years carrying out street surveillance on Islamist, **IRA, Russian and Chinese targets in the UK**. The author, writing under the pen name **Tom Marcus**, said he was now so worried about his son's safety that his clothes and sleeping back were fitted with tracking devices. According to his book, Soldier Spy, which has been vetted by MI5 to prevent security breaches and is published later this week, he was nearly killed while following an Islamist terrorist cell. Unknown to him, the extremists had used counter surveillance techniques to watch who was following them and had lured him into an alleyway. When his controllers realised what was happening the operation was quickly abandoned.

MI5 missed chance to foil Paris and Brussels terrorists: Undercover operation was halted three months before meeting between ringleader and British extremists
Daily Mail (UK), Rebecca Camber, Duncan Gardham, 2016 10 04
London - **Police and MI5 could have prevented the Paris and Brussels terrorist atrocities after a secret operation targeting British suspects linked to the plot was launched months before the attacks.** But senior officers decided to halt the undercover probe three months before one of the coordinators of the Paris attacks crossed the Channel to meet extremists in Britain, it can now be disclosed. The decision meant that investigators missed a key meeting between a group of alleged Islamic State supporters in Britain and Mohamed Abrini last summer - which could have led them to the Brussels-based cell before they carried out a wave of shootings and bombings, killing 130 people in Paris last November. Dubbed the 'man in the hat', Abrini was later caught on camera fleeing Brussels airport after the bombing in March and he is accused of coordinating both the Paris and Brussels attacks.

National Cyber Security Centre HQ operational
SC Magazine (UK), Staff report, 2016 10 03
London - The **UK's new National Cyber Security Centre (NCSC) officially opens for business today as a public-facing part of GCHQ that acts as a focal point for the government to deliver authoritative advice on tackling cyber-security issues**. It will be based in the Nova office and shopping complex near Victoria Station in London, not in

Cheltenham at GCHQ, as originally announced last year, though it will also have offices there.. While this operational centre will focus on defensive work, it will be able to call on offensive capabilities developed by GCHQ and the Ministry of Defence. According to Evening Standard reports, the NCSC will have a staff of 700, more than half of whom will be based in the new HQ, moving in to the building later this year and in early 2017. It is **led by CEO Ciaran Martin who was director general cyber at GCHQ, with Dr Ian Levy, former technical director of cyber-security at GCHQ, becoming technical director at the NCSC**. The NCSC's website is scheduled to go live tomorrow (4 October).

The MI5 spy who saved children from a UK bomb attack
BBC News, Monica Soriano, Justin Parkinson, 2016 10 03
London - Tom Marcus is still jittery three years after retiring as a spy, he tells the BBC's Victoria Derbyshire programme. Walking down the street, he sometimes sees suspicious behaviour where there is none - shady people lurking in doorways; unusual bulges in coats; nervous, furtive glances. **Tom - not his real name, it can't be used for security reasons - saw plenty during his eight years as an MI5 surveillance officer to make him suspicious**. In the end, the job caught up with Tom. He **suffered nightmares about being attacked and was diagnosed with post-traumatic stress disorder (PTSD), returning to civilian life in 2013**. He feels he's recovered now. He also struggled to find another job. Because of the anonymity required by MI5, Tom, who joined the Army at the age of 16 before moving on to the security services, has a large gap in his CV. "It's been hugely difficult to get a job," he says. "Working as an MI5 surveillance officer is seen as a job for life - so when you have to come out it's very difficult to figure out what job you can do. "You can't answer the question about what you've been doing for the last 10 to 15 years in a job interview properly because you'd be breaking the Official Secrets Act."

Met set to lose anti-terror job to 'British FBI'
Sunday Times (UK), Tom Harper & Richard Kerbaj, 2016 10 02
London - **Scotland Yard may be stripped of responsibility for counterterrorism in a shake-up of policing after Sir Bernard Hogan-Howe's departure as commissioner of the Metropolitan police**. The Sunday Times understands that Theresa May is considering handing control of counterterrorism to the **National Crime Agency (NCA),** which she created as home secretary in 2013. According to a senior source familiar with her views on police reform, the change could come "within this parliament". The potential loss of about 2,000 Met officers and a significant chunk of its budget would represent a huge blow to Scotland Yard "The NCA job is going to be the premier job in policing. It is the British FBI and will get counterterrorism, probably sooner than some people think." A senior Home Office source said the move was not imminent, but was "likely to happen in this parliament".

MOD tries to halt book about undercover ops
Sunday Times (UK), John Mooney, 2016 10 02
London - The **Ministry of Defence has asked the Dublin-based publisher of a book by a former soldier about his involvement in clandestine spying operations in Northern Ireland to halt its sale and distribution.** The MoD has told **Merrion Press**, publisher of **Charlie One**, that it knows the identity of "**Seán Hartnett**", the pseudonym used by the author, who **gives details about classified surveillance operations involving undercover soldiers and MI5 in 2001.** It said Hartnett would be arrested should he enter the UK and would no longer receive his army pension. The MoD, through its solicitors, last week wrote to Merrion Press to say it was assessing the damage caused to Britain's national security by the book. It accused Hartnett, who works as a security consultant in Ireland, of breaching his special forces

confidentiality agreement, disclosing details of covert operations in which he participated. It also accused him of breaching **Britain's Official Secrets Act**.

Cyber crime unit opens amid surge in online attacks
Daily Telegraph, 2016 10 01
London - **Britain's first national centre for combating cyber criminals will open next week, amid rapid growth in the number of online attacks**. Terrorists, hackers and online gangs will be targeted by intelligence experts at the new National Cyber Security Centre in Victoria, central London. A team of around 700 people will help to advance the Government's war against cyber crime. The threat is growing, with 200 major incidents a month, double the rate last year. The centre will be led by Ciaran Martin, formerly the director general for cyber security at **GCHQ**. At a cyber security conference in Washington DC earlier this month, Mr Martin outlined plans to create a firewall that could protect government agencies and internet users against cyber attacks.

Drive to shake up UK's terror laws for benefit of victims is launched (Canada)
Belfast Telegraph, Rebecca Black, 2016 10 01
London - **London-based law firm McCue & Partners is behind the initiative, acting on behalf of Northern Ireland-based group Innocent Victims United**. The group said it was seeking to raise £25,000 to bring about **"much-needed and long-overdue change to the law to allow UK victims and survivors of terrorism to bring terrorists and their supporters to justice".** "Too often, the State fails, is unable or chooses not to do so," the campaigners said in a statement. "The laws of other countries provide their victims with such essential support. It's time the UK did too." The campaigners also claimed that the UK falls "far behind other Western countries, such as the **USA and Canada**, in providing adequate access to justice to UK citizens who are victims and survivors of terrorism".

National Cyber Security Centre to lead digital war from new HQ in the heart of London
London Evening Standard, staff reporters, 2016 09 30
London— **Britain's war against the soaring number of cyber attacks is to be led from a new HQ in the centre of London**, the Standard reveals today. **The National Cyber Security Centre**, close to Victoria station, will be tasked with bolstering security against the growing online threats from around the globe. It will be the front line in the UK's battle to protect itself from cyber attacks emanating from countries including China and Russia as well as from terrorists and criminal gangs. Some of Britain's best technological minds will break new ground in the bid to develop defences for the Government to block malware and phishing emails automatically. The HQ will be located in property giant Land Securities' ultra-modern Nova development — including offices, shops, restaurants and bars — off Victoria Street and close to Buckingham Palace. Specialist teams for the City, Whitehall, intelligence and security services, energy, telecoms, other parts of the critical national infrastructure and businesses will help them fight against and respond to general and more specific threats to their sectors. **NCSC chief executive Ciaran Martin, who moves from being GCHQ's director general of cyber security**, said: "Our role is helping to make the UK the safest place to live and do business online. So we'll tackle the major threats from hostile states and criminal gangs.

The danger was worth it, says IRA infiltrator
London Times, Sean O'Neill, 2016 09 30
Dublin - An **FBI spy who infiltrated the Real IRA said he felt vindicated now that a £1.6 million ruling against the alleged perpetrators of the Omagh bombing has been upheld by the European Court of Human Rights**. **David Rupert**, an American businessman who worked on behalf of the **FBI**, said that yesterday's ECHR decision showed that "the truth shall

overcome". He was reacting to the court's rejection of an attempt by Michael McKevitt and Liam Campbell, two convicted Real IRA members, to overturn the landmark civil ruling that found them and two others responsible for the Omagh bombing that killed 29 people in August 1998.

The spy who liked me: Britain's changing secret service
Financial Times, Sam Jones, 2016 09 29
London - **Behind the closed doors of British intelligence, the era of Smiley's People is giving way to a future of Smiley's Facebook friends. Digital disruption is sweeping through the world's second-oldest profession -- spying** -- and the UK is repurposing its intelligence services with a **£1.5bn annual top-up** for security available for the first time this year. For the **Secret Intelligence Service, or MI6, which supplies foreign intelligence**, this translates into its biggest ever recruitment drive, with as many as 1,000 new staff over the next four years, a 40 per cent rise. British security officials, in conversations with the Financial Times over the past few months, have painted a consistent picture of their trade: technology that empowered spooks for the past two decades is changing their business profoundly. Last week, **Alex Younger, the chief of MI6**, still known by the moniker "C" (with which, in green ink, he traditionally signs all his correspondence), spelt out the shift in a rare public speech with fellow spymasters in Washington. "The information revolution fundamentally changes our operating environment," said Mr Younger. "

Double agent's wife threatened suicide during WWII, previously top-secret files reveal
Toronto Star, Peter Edwards, 2016 09 28
Toronto - The **wife of one of Britain's top double agents turned on the gas outlets in their home and threatened to kill herself out of despair in the midst of World War II**. Her husband was Juan Pujol-Garcia, codenamed "Garbo," "Bovril" and "Immortal," according to newly-released **British MI5 intelligence** files, that were stamped "Secret" and "Most Secret." The previously-closed Security Service files say Pujol-Garcia wove Toronto, Ottawa and Montreal into a complex web of deception to trick the Nazis about plans for the massive D-Day invasion of Normandy, France on June 6, 1944. Other newly-released MI5 files deal with Soviet Intelligence agents and suspected agents from 1934 to 1959 and communists and suspected communists from 1920 to 1961.

Return to Table of Contents/ Retour à la table des matières

Australia / Australie

Data delays thwart counter-terrorism
Sydney Morning Herald, Rachel Olding, 2016 09 28
Sydney - **Counter-terrorism police fear crucial information may slip through the cracks in major investigations because a national case- management system has not been rolled out,** despite repeated requests for almost a decade. The number of terrorism investigations in Australia is rising, yet officers say some are being jeopardised because each state police force uses a different system for managing investigations. Fairfax Media understands that counter-terrorism police have picked up an increasing amount of communication between terror suspects in Sydney and Melbourne in recent months. Both cities remain the overwhelming focus of investigations.

Return to Table of Contents/ Retour à la table des matières

New Zealand / Nouvelle-Zélande

Dotcom's appeal against extradition to U.S. winds up in New Zealand, ruling likely weeks away
Reuters, Staff reporter, 2016 09 28
Wellington - Lawyers for German entrepreneur **Kim Dotcom**, wanted in the United States on copyright infringement and money-laundering charges over his file-sharing website Megaupload, argued on Wednesday there was not enough evidence to show he conspired to commit a crime. The Auckland court heard closing arguments in Dotcom's four-week appeal against a lower court's decision to extradite him to the U.S., the first New Zealand court proceedings to be broadcast live on the internet. Years of legal wrangling followed **Dotcom's arrest in the police raid in 2012 and it emerged that the Government Communications Security Bureau had illegally spied on him before the raid**. While the main arguments have now been heard, a few technical matters have yet to be argued in court. Lawyers said a decision was likely to be weeks away - and it was unlikely to be the final word.

Return to Table of Contents/ Retour à la table des matières

International

China / Chine

Inside China's Big Brother HQ
Mail on Sunday, George Knowles, 2016 10 01
Hangzhou, China— **Hikvision, a company controlled by the Chinese government, was recently revealed to be Britain's biggest supplier of CCTV equipment**, raising fears its internet-linked cameras could be hacked from Beijing at the touch of a button. Last week, undercover Mail on Sunday reporters posed as businessmen to infiltrate its headquarters in the 'surveillance city' of Hangzhou in eastern China, to investigate its activities. What they found will raise fresh cause for concern about a company whose growing influence in the UK has already been questioned by former MI6 officers and Security Ministers. Far from being the independently run business it claims to be in its customer-friendly marketing, **Hikvision is controlled by China's ruling Communist Party**. Hikvision is central to the government's Orwellian programme to spy on its 1.3 billion citizens, and is inextricably linked to the totalitarian crackdown on those considered 'enemies of the state'. More worryingly, Hikvision vice-president Pu Shiliang, 38, is also technical leader of a key laboratory at the **Ministry of Public Security**, the feared body that has been accused of the extrajudicial arrest and detention of thousands of lawyers, activists and perceived government opponents within China every year.

China cyber espionage continues
Washington Times, Bill Gertz, 2016 09 29
Washington - **U.S. Cyber Command recently reported within secret government channels that China is continuing aggressive cyber espionage against American companies**. An intelligence report disseminated earlier this month stated that one of China's biggest cyber spying operations involved the theft of 1.65 terabytes of sensitive proprietary data from a major U.S. software company, according to a defense official familiar with the report. The U.S. company was not identified by name. But the hacker group behind the data theft is part of the

Ministry of State Security, China's main police and intelligence service. The hacking operation by the MSS was carried out from at least October 2015 and contradicts the U.S.-China agreement on cyber espionage reached between President Obama and Chinese President Xi Jinping in September 2015.

Return to Table of Contents/ Retour à la table des matières

Russia / Russie

Russia's FSB Detains Ukrainian Spy Collecting Military Secrets
Sputnik, Staff report, 2016 10 03
Moscow - Russia's **Federal Security Service (FSB) detained a member of the Ukrainian Defense Ministry's chief intelligence directorate it accused of collecting state secrets on the Russian military,** the FSB said Monday. "**Roman Sushchenko**... purposefully collected state secret information on the activities of the Russian Armed forces and the National Guard troops, which could have harmed state defense capabilities if leaked abroad," the FSB said in a statement. It added that it launched a criminal case against Sushchenko on charges of espionage.

Russian Intelligence Says It Detained Ukrainian Spy Suspect
Associated Press, Staff report, 2016 10 03
Moscow - The **Russian intelligence agency FSB said on Monday it has arrested a Ukrainian journalist who is suspected of spying in** Russia. The FSB claimed in a statement that **Roman Sushchenko** is an officer with the Ukrainian military intelligence who has been collecting information about the Russian Armed Forces. The arrest, confirmed by a Moscow court on Monday, comes amid an almost complete breakdown in relations between the two neighbors, triggered by Russia's annexation of Crimea and its support for separatist rebels in eastern Ukraine.

Putin Has Finally Reincarnated the KGB
Foreign Policy, Andei Soldatose, 2016 10 02
Analysis: This past Sunday, as most of Russia focused its attention on parliamentary elections, the country's most popular daily, Kommersant, broke news of a story that, if true, could have consequences that last far beyond this latest round of Duma reshuffling. **Russian President Vladimir Putin,** according to Kommersant, **is planning a major overhaul of the country's security services**. The Russian daily reported that the idea of the reforms is to merge the Foreign Intelligence Service, or SVR, with the Federal Security Service, or FSB, which keeps an eye on domestic affairs. This **new supersized secret service will be given a new name: the Ministry of State Security**. If that sounds familiar, it should -- this was the name given to the most powerful and feared of Joseph Stalin's secret services, from 1943 to 1953. And if its combination of foreign espionage and domestic surveillance looks familiar, well, it should: In all but name, we are seeing a resurrection of the **Committee for State Security** - - otherwise known as the **KGB**. The **KGB, it should be remembered, was not a traditional security service in the Western sense -- that is, an agency charged with protecting the interests of a country and its citizens. Its primary task was protecting the regime**. Its activities included hunting down spies and dissidents and supervising media, sports, and even the church. It ran operations both inside and outside the country, but in both spheres the main task was always to

protect the interests of whoever currently resided in the Kremlin. With this new agency, we're seeing a return to form -- one that's been a long time in the making.

Russia steps up trolling attacks on the West, U.S. intel report finds
Yahoo News, Michael Isikoff, 2016 09 29
New York - A **new U.S. intelligence report says the Russian government is conducting a wide-ranging and "opportunistic" campaign to expand its political influence in Europe by deploying Internet "trolls and other cyber actors"** to challenge pro-Western journalists and spread pro- Kremlin messages in social media forums. Yahoo News obtained a **declassified summary** of the report, which also describes the role of two state-owned media outlets, RT and Sputnik, in what some experts say is an increasingly aggressive "information warfare" campaign. According to the report, the outlets promote Russia's political aims with programming targeted to "activist" audiences including "far-right and far-left elements of European society." It adds that the RT channel gives "disproportionate coverage and airtime to the European Parliament's more extreme factions." The **report, by the office of Director of National Intelligence James Clapper,** was originally requested by congressional intelligence committees late last year. The panels also asked for a separate report on Russia's use of political assassination. Classified versions of both documents were delivered by Clapper's office to Capitol Hill in July.

Russian hackers went after journalists investigating the downing of MH17
Washington Post, Ellen Nakashima, 2016 09 29
Washington - **Russian government hackers began targeting a British citizen journalist in February 2015,** eight months after he began posting evidence documenting alleged Russian government involvement in the shoot- down of a Malaysian jetliner over Ukraine. And then in February 2016, a group that researchers suspect is a propaganda mouthpiece of the Russian government - **CyberBerkut -** defaced the home page of Eliot Higgins's citizen journalism website, Bellingcat.com. That same month, CyberBerkut hacked the email, iCloud and social-media account of a Bellingcat researcher in Moscow, then posted online personal pictures, a passport scan, his girlfriend's name and other private details. Russia's information operations against Bellingcat are a taste of what may be in store for other media organizations whose reports anger the Kremlin, said a cyber-research firm that has extensively documented the effort. .

Were the Russians Behind the Massive Yahoo Email Hack?
NBC News, Chris Francescani, 2016 09 28
New York - The **hack of more than a half billion Yahoo email accounts was motivated by espionage, not profit, according to an independent cybersecurity firm report** released Wednesday, which contends that an **Eastern European state-sponsored actor** appears to have ordered the massive hack as part of a coordinated effort to infiltrate the email accounts of U.S. military, diplomatic and political figures. The findings by the cyber security firm **InfoArmor** are consistent with Yahoo officials' claim last week that a state-sponsored actor was behind one of the largest corporate breaches in U.S. history. Yet InfoArmor's version of events, if accurate, provides significant new details about how and why the company was hacked. Minor league hackers who were peddling. In an interview with NBC News prior to the release of his firm's findings, InfoArmor's chief intelligence officer Andrew Komarov described the Yahoo breach as part of a larger, ongoing campaign to break in to the email accounts of prominent officials from the U.S. and across the globe.

Return to Table of Contents/ Retour à la table des matières

Europe

L'affaire Squarcini embarrasse la Direction du renseignement intérieur
Le Monde, Simon Piel et Joan Tilouine, 2016 10 04
Paris— La **DGSI a été perquisitionnée, son directeur Patrick Calvar, et des agents ont été entendus.** M. **Calvar fait partie des personnes que M. Squarcini avait tenté de solliciter pour recueillir des informations confidentielles**. Les déflagrations de l'affaire Squarcini continuent de résonner dans les couloirs de la Direction générale de la sécurité intérieure (DGSI) à Levallois-Perret (Hauts-de-Seine). Plusieurs personnes en poste à la DGSI – dont deux policiers – ont été entendues, entre lundi26 et mercredi 28septembre, pour s'expliquer sur les contacts qu'ils avaient continué à entretenir avec leur ancien patron. L'un des deux policiers a été mis en examen pour «violation du secret professionnel», «collecte frauduleuse de données à caractère personnel», «détournement de la finalité d'un traitement de données à caractère personnel» et «compromission du secret de la défense nationale». Son contrôle judiciaire lui interdit jusqu'à nouvel ordre de travailler à la DGSI ainsi que dans tout service de renseignement. L'autre a, pour sa part, été placé sous le statut de témoin assisté pour avoir notamment effectué des traductions de revues de presse à destination de M. Squarcini. Le 27septembre, les locaux de la DGSI situés à Levallois avaient été perquisitionnés dans l'objectif de préciser les éléments que ces fonctionnaires avaient pu transmettre à M.Squarcini. Un acte d'enquête rarissime, compte tenu du fait que le siège des services de renseignement intérieur sont protégés par le secret-défense. **Trois assistantes de Patrick Calvar, l'actuel directeur de la DGSI, qui y travaillaient déjà sous l'ère Squarcini, ont été entendues la semaine dernière et leurs ordinateurs examinés par les enquêteurs de l'IGPN.**

Reforms underway mull a divided, better-controlled intelligence
Daily Sabah, Staff report, 2016 10 04
Istanbul - **Decades after its foundation, the National Intelligence Directorate (MIT), Turkey's highly discreet intelligence service, will undergo a major makeover**, that may or may not turn it into its American counterpart, the Central Intelligence Agency (CIA). The government's plans for a complete reformation of intelligence services will divide intelligence into two: external and internal. The MIT will focus on external intelligence while a new agency will be established to handle homeland intelligence. More importantly, new reforms call for a tighter monitoring on intelligence services' activity by the presidency in an effort to prevent a weakness in the intelligence as witnessed at the time of the July 15 coup attempt by the Gülenist junta. The MIT was criticized for an intelligence failure and being late to inform authorities about the putsch attempt afoot. Still, intelligence services will keep their liaison with the Prime Ministry that appoints MIT's directors. New reforms will be a part of statutory decrees regularly issued during the state of emergency following the coup attempt.

Turkey suspends 12,800 police, tightening clampdown after failed coup
Reuters, Staff report, 2016 10 04
Istanbul - **Hours after announcing a three-month extension of a state of emergency, Turkey suspended 12,801 police officers on Tuesday**, saying they had suspected links to U.S.-based cleric Fethullah Gulen, whom Ankara blames for orchestrating July's failed coup. In a statement, Turkey's national police headquarters said 2,523 of those suspended were police chiefs. The overall number represents more than 5 percent of Turkey's entire police force. They "have been assessed to have communications or links to the Gulenist Terror Organisation, identified as a **threat to national security**," the written police statement said. Turkey lists the

religious movement led by Gulen as an illegal terrorist network, though he has denied having any link to the uprising. State-run Anadolu Agency said 37 people working in the Interior Ministry's headquarters had also been removed from their posts. It was not clear if both measures were linked.

Reshuffles at Bulgaria's National Security Service
Sofia News Agency, Staff report, 2016 10 03
Sofia - A **reshuffle within the leadership of the National Security Service (NSO) enters into force on Monday**, the second one in two weeks. **Krasimir Stanchev is the second deputy head of the National Security Service** to be removed from office, the State Gazette's October 04 edition will say, according to information from BGNES wire service. Col Rosen Todorov will take over from Stanchev. The reasons for the reported reshuffle, if confirmed, are not immediately clear. In the summer, Col Yulian Haralampiev was replaced by Lt Col Emil Tonev, with NSO citing Col Haralampiev's lack of a minimum of 5-year experience on a managerial position.

Pourquoi Bernard Squarcini a été mis en examen
Le Monde, Simon Piel et Joan Tilouine, 2016 09 30
Paris - **L'avocat de l'ex-patron de la DCRI dénonce " l'hypocrisie " des accusations**. A l'issue de 48 heures de garde à vue dans les locaux de l'Inspection générale de la police nationale (IGPN), **l'ancien patron de la Direction centrale du renseignement intérieur (DCRI, aujourd'hui DGSI), Bernard Squarcini a été mis en examen mercredi 28 août par des magistrats du pôle financier pour de nombreux chefs parmi lesquels le trafic d'influence**, la violation du secret de l'enquête, la compromission ou encore l'entrave aux investigations. Cette décision a été assortie d'un contrôle judiciaire très strict qui interdit à M. Squarcini de paraître dans les locaux de la DGSI à Levallois-Perret (Hauts-de-Seine), d'entrer en contact avec les autres protagonistes de l'affaire mais aussi avec tout fonctionnaire de la direction centrale de la police judiciaire et des services de renseignement.

SBU chief, director of NATO Office of Security sign classified information treaty
Interfax (Ukraine), Staff report, 2016 09 29
Kyiv - An international treaty - Administrative Arrangements on Protection of Classified Information - between the Ukrainian government and NATO was signed as part of a visit of a NATO delegation headed by Director of the NATO Office of Security Todd Brown The press center of **Ukrainian Security Service (SBU)** reported on Wednesday that SBU Head Vasyl Hrytsak signed the document on behalf of the Ukrainian government. The **tool is aimed at specifying the procedure for mutual protection of the classified information set in the general agreement on security between Ukraine and NATO (1995**) and bringing the national mechanisms in line with the NATO standards.

5 pct of hacker attacks threaten Lithuania's natl security – chief
Baltic News Service, 2016 09 29
Vilnius— **Lithuania's state institutions are subjected to thousands of attempted cyber attacks on a daily basis,** including hundreds constituting a medium threat and at least 5 percent constituting a serious threat, says Ri**mtautas Cerniauskas, director of the National Cyber Security Center.** In the framework of Lithuania's first national cyber exercise Cyber Shield 2016, over 100 specialists from more than 40 of the country's institutions learned to respond to emerging cyber threats and coordinate their work in the face of cyber attacks. The week-long exercise involved over 30 scenarios, for instance, simulation of a power blackout, blocking of websites during elections, etc. The exercise was held in a virtual infrastructure to avoid hardware damage.In addition to specialists from the **National Cyber Security Center**, the

police, prosecutor's offices and the **State Security Department**, the exercise involved representatives of the Seimas, the government and the President's Office, the Communications Regulatory Authority, the Vilnius University and the Kaunas University of Technology, as well as other agencies and institutions.

Deux anciens grands flics en garde à vue
Le Figaro, Christophe Cornevin, 2016 09 28
Paris - **Bernard Squarcini et Christian Flaesch étaient entendus mardi par l'IGPN pour trafic d'influence.** Justice Une chape de plomb, plus lourde encore que celle pouvant couvrir une opération antiterroriste, pèse sur les gardes à vue entourant une trouble affaire de trafic d'influence présumé au coeur de laquelle se trouverait Bernard Squarcini. Depuis lundi, **l'ex-directeur central du renseignement intérieur, réputé proche de Nicolas Sarkozy et évincé de ses fonctions après l'arrivée des socialistes au pouvoir en 2012**, est aujourd'hui inquiété sur la base d'interceptions téléphoniques remontant, semble-t-il, à plus de trois ans.

Le renseignement géospatial français dans la guerre contre l'EI
Le Monde, Nathalie Guibert, 2016 09 28
Mossoul - Alors que la bataille de Mossoul se précise, la **France a renforcé ses capacités sur le terrain, notamment dans le renseignement.** Cliquer sur un bloc d'immeubles de Mossoul pour visualiser aussitôt tout ce qui s'y trouve en 3D, dévoiler les parties " aveugles " de la ville qui ne ressortent pas de l'observation humaine, ou encore simuler les capacités de nuisance d'une attaque sur les canalisations urbaines. Ces informations constituent une partie, discrète, du soutien militaire que la France apporte aux combattants irakiens en guerre avec l'organisation Etat islamique (EI). La décision d'accroître cette aide a été prise à Washington, lors de la réunion du 21 juillet des ministres de la défense les plus impliqués dans la coalition - anti-EI.

State Security Service to send petitions regarding the released secret recordings to respective countries
Prime News (Georgia), 2016 09 28
Tbilsi— The State Security Service will send petitions regarding the released secret recordings to the respective countries, - Nino Giorgobiani, spokesperson for the State Security Service, said at a briefing. "Petitions for legal assistance will be sent to all the countries that are in the interests of the investigation. The State Security Service will not allow any destabilization in the country, and in case of revelation of a crime, offenders will be strictly punished, "- Nino Giorgobiani said. The **Counterintelligence Department of the State Security Service** has launched an investigation into the released secret recordings.

Les réseaux Squarcini dans le viseur de la justice
Le Monde, Simon Piel et Joan Tilouine, 2016 09 28
Paris - Des **policiers auraient informé l'ex-patron du renseignement au profit de LVMH et du clan Sarkozy**. Certains de ses anciens collègues lui donnaient toujours du " chef " et continuaient de lui livrer des informations confidentielles, malgré sa reconversion dans le privé. Lundi 26 septembre, **Bernard Squarcini, ancien patron de la Direction centrale du renseignement intérieur (DCRI, aujourd'hui DGSI), a été placé en garde à vue dans les locaux de l'inspection générale de la police nationale (IGPN)** dans le cadre d'une information judiciaire ouverte notamment pour " violation du secret de l'instruction ", " entrave aux investigations ", " compromission ", " violation du secret professionnel " et " trafic d'influence ". Sa garde à vue se poursuivait mardi matin.

Military intelligence shared in targeted assassinations
NL Times, Janene Pieters, 2016 09 27
The Hague - The **Dutch military intelligence service MIVD shared information that could be used in so-called "targeted killings" by other countries**. While the service complied to the rules in this, the rules are insufficient to remove the risks of the MIVD inadvertently contributing to the unlawful use of force, the CTIVD concludes in a report published on Monday, ANP reports. The CTIVD is the committee responsible for overseeing and supervising the **Dutch intelligence services.** For this report, the committee looked at the MIVD's actions in the period 2013 to 2015. According to the report, the MIVD contributed to "targeting" in two military missions in which the Netherlands also participated.

National Intelligence agency MIT dismisses 87 FETÖ-linked personnel
Daily Sabah, Staff report, 2016 09 27
Istanbul - The **National Intelligence Agency (MIT) has dismissed 87 personnel for their links to the Fetullah Terrorist Group (FETÖ),** according to an intelligence agency source on Tuesday. 141 MIT personnel were suspended following the July 15 coup attempt and investigations into 100 of those suspended personnel have been completed. 87 out of them have been dismissed and 52 of them will face criminal complaints, the source said. The Turkish state has taken steps to dismiss anyone with suspected ties to FETÖ after the failed coup attempt on the night of July 15. MIT is one of the state institutions, alongside others, that the Gülenists have targeted for infiltration in order to carry out their intended plans in Turkey.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

General Security chief inaugurates new center in south Lebanon
Lebanon Daily Star, Staff Report, 2016 10 03
Beirut - **General Security head Maj. Gen. Abbas Ibrahim Saturday inaugurated a new agency center in the town of Shebaa** during a tour of south Lebanon. "This accomplishment is the best means to respond to the dangers imposed by the Israeli enemy and its ongoing threats against the Lebanese and the residents of the south in particular," Ibrahim said. He called the center a fulcrum in confronting "sabotage and criminal networks and in revealing enemy agents ... seeking to destabilize [the country] and spreading sedition." Ibrahim also praised the ongoing cooperation between the General Security and UNIFIL, which provided "the logistic aid necessary to establish the center." The high-ranking security official had also said Friday during a visit to a farmer's union rally in east Lebanon that the government was searching for a "serious" mediator to help secure the release of the nine servicemen held hostage by ISIS.

Iran's Top Security Official: West Lying About Its Role in Middle East's Security
Fars News Agency, 2016 10 03
Tehran— Secretary of Iran's **Supreme National Security Council** (SNSC) **Ali Shamkhani** dismissed as untrue the claims by the western countries that they are contributing a positive role in the security of the regional countries. "The claim about the West's contribution to the establishment of regional security is a big lie and its bloody and costly results can be seen in many countries in the region," Shamkhani said in a meeting **with Head of Iraqi National Intelligence Service Mustafa Kadhimi** in Tehran on Sunday. He said that the Iraqi army backed by popular forces has managed to make continued achievements in the fight against terrorism and the elimination of ISIL terrorists from many areas in the country.

Iranian spymasters 'running covert war' in Syria
Jerusalem Post, Staff Report, 2016 09 30
Jerusalem - **Iranian spymasters are commanding a large-scale clandestine war from Damascus in order to support Syrian President Bashar Assad**, The Daily Mail reported Thursday. The National Council of Resistance (NCRI) of Iran has claimed that Iranian Supreme Leader Ayatollah Ali Khamenei has spent billions to bolster its ally Assad in the last five years, including running operations from a five-floor building dubbed the "Glasshouse" near the airport in the country's capital.

Intelligence minister: Threats posed by terrorists under control
Islamic Republic News Agency, 2016 09 30
Tehran - **Threats by the enemies against the Islamic Republic are under control, Minister of Intelligence Mahmoud Alavi said** on Thursday. Iran has intelligence dominance over terrorists and the enemies have so far failed to conduct even a single successful terrorist operation inside the country, Alavi said during a meeting with the judiciary officials. He also said that nobody has the right to pressure judges and judiciary officials for issuing decrees against the regulations.

Notorious Aleppo intelligence chief moved from post
Now Lebanon, Albin Szakola, Amin Nasr, 2016 09 28
Beirut - The **powerful head of Syria's feared Air Force Intelligence in Aleppo has been moved from his post in an eyebrow raising** move, only days after Damascus started a massive bombardment campaign against the opposition-held half of the strife-stricken city. On Sunday, pro-regime outlets announced that **Major General Adib Salameh**, an officer notorious for his considerable influence and alleged corruption, was reassigned as the new deputy director of the **Air Force Intelligence Directorate** in Damascus. Meanwhile, General Iyad Mindo, the head of Air Force Intelligence at Damascus International Airport, was promoted to take up the posting in Aleppo, which Salameh held since 2012..

ISIL Appoints Saddam's Army General as 'New War Minister'
Fars News Agency, 2016 09 28
Tehran - A **senior commander of Iraqi popular forces revealed on Tuesday that ISIL has appointed a Saddam-era army commander as its 'new war minister'** to replace the terror group's notorious former war minister, Abu Omar al-Shishani, who was killed early in Summer. "ISIL leaders in a meeting held in the vicinity of Iraq's Anbar province selected former senior Iraq Army officer Yaseen al-Muadhidi, nom de guerre Abu Taha, as the terror group's new war minister," Senior commander in Iraq's Popular Mobilization Forces, locally known as Hashd al-Sha'abi, Colonel Nazem al-Chuqaifi said on Tuesday. **Abu Taha is among the most senior commanders and Emirs** within the hierarchy of the ISIL terrorist group, and has fought with the group, after pledging allegiance to the group some five years ago.

Return to Table of Contents/ Retour à la table des matières

Asia / Asie

Presidential office dismisses claim over Park's retirement residence
Yonhap News Agency, 2016 10 04
Seoul— The **presidential office Cheong Wa Dae on Tuesday dismissed an opposition politician's claim that President Park Geun-hye's close aide has directed the state intelligence agency to prepare a new home for her retirement**. Calling the claim "totally

groundless," presidential spokesman Jung Youn-kuk told reporters that Park plans to return to her old house in Samseong-dong, southern Seoul after her term ends in February 2018. During a parliamentary audit, Rep. Park Jie-won, the interim leader of the minor opposition People's Party, raised the claim that Lee Jae-man, the president's secretary for general affairs, has instructed the National Intelligence Service (NIS) to prepare a home for her after she leaves her presidential post.

Indian intelligence hired fake crowd to back Brahamdagh
The International News, 2016 10 04
Karachi - **Baloch separatist leader Brahamdagh Bugti is playing in the hands of Indian intelligence Research and Analysis Wing (RAW),** evidence gathered by Geo News showed on Tuesday. The **Indian intelligence agency was behind the recent protests held against Pakistan in Geneva**, which Brahamdagh Bugti led to push his agenda of vilifying Pakistan. The Indian media used the Bugti-led protest to hoodwink the people of India in an effort to divert attention from the atrocities being carried out by Indian army in held Kashmir. Shahzeb Khandaza, senior journalist and host of Pakistan's most popular show, produced evidence that Indian intelligence brought "paid demonstrators" from a refugee camp to the protests led by Bugti and Mehran Murri. He said usually the refugees are paid 100-150 Francs to take part in protests called Silent Solidarity Protests. Geo News research shows the demonstrators chose to remain silent in these protests as they could not speak foreign languages.

Pak spy balloons, pigeons, boat captured
The International News, 2016 10 03
Islamabad - A **frightened India on Sunday claimed to have got hold of suspected balloons with sentences written in Urdu** on them in the Gurdaspur area, media reports said. After the flop drama of a **pigeon's** custody, India has come up with the balloons case and claimed to have "detained them" with a message for Modi.According to the Indian media, sentences giving warning to India and taking revenge of surgical strikes were written on them. As revealed, the message read: "Modi, do not consider us the same people as we were during 1971. Now each and every child is ready to fight against India." Earlier, the Indian police detained another pigeon that flew into a village near the heavily-militarised border with **Pakistan on suspicion of being a 'spy'.** The **state intelligence and army officers inspected the pigeon** which might have flown across border from Pakistan and landed in Punjab's Hoshiarpur district with some words in Urdu inscribed on its wings.

Embassy mum on CIA plot's 'kill Rody'
Manila Standard, 2016 10 01
Manila— The **US Embassy in Manila refused to comment on President Rodrigo Duterte's remarks in Vietnam that he had received reports that the US Central Intelligence Agency wanted him dead**, saying his staff should clarify his statement. "We [US Embassy] would want to refer you to President Duterte for clarification on his statement," US embassy press attache Molly Koscina said in a text message. Before Filipinos living and working in Hanoi, Duterte said that the CIA was planning to kill him. "That's the situation. They said, the CIA is planning to kill me. Susmaryosep, ginoo," Duterte said.

N. Korea combines 2 units managing leader's coffers into one: Seoul
Yonhap News Agency, 2016 09 29
Seoul— **North Korea is presumed to have combined the ruling party's two units handling its leader Kim Jong-un's governing funds into one**, a Seoul government official said Thursday. North Korea is projected to have kept intact Office 39 of the Workers' Party of Korea (WPK) as the special unit managing state coffers while eliminating Office 38, according to an

official at Seoul's unification ministry. Office 38 is known to raise money within the country to run North Korean leader Kim Jong-un's private coffers, while Office 39 is believed to manage hard currency earned from overseas. **Seoul said North Korea's three key security-related ministries are presumed to be controlled by a newly created state apparatus named the State Affairs Commission (SAC)**, but more information is needed for confirmation. The three ministries are the **Ministry of State Security, North Korea's intelligence agency**, the Ministry of the People's Armed Forces, the North's defense ministry, and the Ministry of People's Security, which is the North's police agency.

RAW tasked to carry out covert strikes against Pakistan
The International News, Ansar Abbasi, 2016 09 29
Islamabad - **Pakistan's intelligence establishment has got the information that RAW has been tasked by the Modi government to execute covert strikes against Pakistan** that includes terrorist activity, targeting of ISI or MI offices and assassination of Hafiz Saeed and Masood Azhar. According to a senior security official source, after the Indian military command advised Modi against any surgical strike or going for war with Pakistan, the option of covert strike against Pakistan has been approved. "RAW has been tasked to plan and execute a covert strike which should speak by itself being an Indian response to Uri," the source said, adding that RAW has been asked to select as target intelligence establishment of Pakistan. Besides this, it is said that RAW has been asked to speed up execution of its plans to assassinate Hafiz Saeed and Masood Azhar.

Return to Table of Contents/ Retour à la table des matières

Africa / Afrique

Somalia: Grande explosion in Kismayo
Garowe Online, 2016 10 04
Kismayo-- **Somalia's National Intelligence and Security Agency (NISA) base was targeted in a grenade attack on Tuesday**, in Kismayo city, regional capital of Jubaland, Garowe Online reports. Unidentified armed men thought to be Al Shabaab militants have tossed grenade bomb at the base located at Guul Wade neighborhood in Kismayo, according to an eyewitness.

Somalia: NISA chief fires over 1000 Intelligence personnel
Garowe Online, Staff report, 2016 10 03
Mogadishu - **Somalia's Intelligence Agency chief has fired 1,500 intelligence staff on Sunday, in a new shakeup of the Intelligence agency following intensified attacks by Al Shabaab group** in the capital of Mogadishu, Garowe Online reports. **Somali National Intelligence and Security Agency (NISA) chief General Abdulahi Gafow** said that the officers were sacked over incompetence to perform their duties, and will carry out major reforms to the agency to bring more competent officers to counter insurgency in the Somali capital of Mogadishu. Caretaker President Hasan Shaikh Mahmoud also has officially replaced Abdi Hakim Fareey with Mohamed Hasan Farah as the new head of NISA in Banadir region, through a presidential decree, yesterday.

Lutte antiterroriste dans le Sahel Le Canada appuie la France au Mali
Liberté (Algérie), Lyès Menacer, 2016 10 02
L'armée canadienne compte venir en aide aux forces françaises qui opèrent dans le Sahel dans le cadre de l'opération Barkhane, a révélé le journal spécialisé canadien

45eNord. "Les Forces armées canadiennes travaillent actuellement sur des plans pour assurer la continuité du transport aérien, **soutien stratégique aux efforts antiterroristes français dans la région du Sahel**", lit-on sur le site de ce journal qui reprend des extraits d'un courriel du ministère canadien de la Défense. "Comme ce fut le cas avec la récente contribution des FAC en 2015, les avions de transport aérien seront probablement utilisés pour le transport de troupes et de matériel français", a ajouté la même source, soulignant toutefois que "cette fois, l'appui serait différent, puisque l'Opération Barkhane sert également de support à l'opération des Nations unies au Mali et que le Canada envisage très sérieusement d'y prendre part, dans le cadre de son retour aux opérations de soutien de la paix".

Return to Table of Contents/ Retour à la table des matières

Americas / Amériques

Former Peru spy chief given another jail sentence for 1993 forced disappearances
The Guardian (London), Dan Collyns, 2016 09 29
Lima - **Peru's former spy chief Vladimiro Montesinos has been sentenced to 22 years in jail** for the forced disappearance of two students and a university professor, whose bodies were burned in the basement of the country's intelligence agency. The students, Kenneth Anzualdo and Martin Roca, and professor Justiniano Najarro were tortured, interrogated then executed in 1993, the court found. Montesinos, 71, who is already serving multiple sentences for human rights crimes, corruption and arms and drugs trafficking, is widely regarded to have been the éminence grise to the former president Alberto Fujimori, who is himself serving a 25-year sentence for corruption and authorising death squad killings. Nicolas Hermoza, the jailed former head of the Peruvian army, was also sentenced at the hearing.

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

05-10-2016 to/au 11-10-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

'Follow us,' spy agency tweet urges
Ottawa Citizen, Jon Willing, 2016 10 11
Ottawa - **Canada's spy agency developed a new external communications plan and kicked around ideas for its first tweet before stepping out of the cyber-shadows, on Twitter**, in July. Internal documents obtained by the Citizen through access to information legislation show how the **Canadian Security Intelligence Service spitballed some options for the agency's first tweet, on July 13, before settling on, "Yes, we're on Twitter. Now it's your turn to follow us."** It notched more than 1,000 retweets and 1,400 likes. The agency had four options for cheeky tweets ready to roll, according to a Twitter game plan. The three that were left on the cutting room floor were: So, we're on Twitter. #WhatWe-DoWednesday may be a challenge for us. (redacted) Yes (redacted) (redacted) we're (redacted) on (redacted) (redacted) Twitter. #LearningCurve ¦¦ In honour of Twitter launching 10 years ago this month, we suddenly decided to join. #LateTo- TheParty There was some talk in emails about potentially crowdsourcing recommendations for the first tweet from all CSIS staff. One staffer served up 13 suggestions, including "Terrorists shaken, spies stirred." Names of CSIS staffare redacted in the documents. As reconnaissance, staffchecked out the first tweets **by the Communications Security Establishment, Central Intelligence Agency in the United States and Government Communications Headquarters in the United Kingdom**. The agency higher-ups approved a list of the initial 16 Twitter accounts to follow, which included the Federal Bureau of Investigation, CIA, Canadian Border Services Agency, RCMP and Privy Council clerk Michael Wernick, plus other national and international agencies. CSIS started thinking about exposing more of itself to the public earlier this year. A 16-page social media strategy dated April 2016 set the foundation for the agency's baby steps into the cyber-spotlight. As one might expect, CSIS noted that establishing "complex passwords" was key for its social media accounts. While posting stuffin error was identified as a risk, the social media strategy recommends "multiple sets of eyes" reviewing any content before it goes live. As well, the agency says it will need a "comprehensive exit strategy," with a heads-up to the clerk of the **Privy Council**, if it decides to close a social media account.

CSIS, Bill C-51 and Canada's growing metadata collection mess
CBC.CA, Steven Zhou, 2016 10 11
Opinion: **Much has been made over whether the Canadian Security Intelligence Service, Canada's spy** agency, should be armed with broader powers to "disrupt" what it perceives as terrorist plots. A report tabled this month by the **Security Intelligence Review Committee**, which watches over CSIS's work, notes that while the spy agency hasn't abused its new powers of disruption, its bulk data collection program needs to be scaled back. It's easy to think of CSIS and other spy agencies as shadowy organizations that carry out James Bond-like "missions" involving cool gadgets and high-tech weaponry, but the Snowden leaks, among other revelations, have shown the public that metadata collection (online communications, phone logs and other electronic exchanges that can be intercepted in enormous amounts) now constitutes the state's primary instrument of control. **Privacy Commissioner Daniel Therrien** recently called upon legislators (the Liberals in particular) to amend certain aspects of Canada's national security laws in order to address the issue of metadata collection. In particular, Therrien referred to the Communications Security Establishment, which seems to get a lot less public scrutiny

than CSIS. (Note: Steven Zhou is a Toronto writer who has experience in human rights advocacy. He has worked for Human Rights Watch, OXFAM Canada and other NGOs.)

RCMP boss admits his force 'failed' women
Toronto Star, Tonda MacCharles, 2016 10 07
Toronto - The **RCMP will settle two massive class-action harassment lawsuits for up to 1,000 female Mounties with a $100-million fund and new promises to change a workplace it now admits was toxic for them**. The landmark move comes with a historic admission: The RCMP is a workplace marked by systemic gender-based discrimination, bullying and sexual harassment. It is the first settlement of a systemic workplace harassment claim in Canada, according to the two law firms that negotiated the deal. Janet Merlo, 53, one of the lead plaintiffs, called it "a turning point. I have total faith this is the beginning of a new era. Hopefully a better era." RCMP Commissioner *Bob Paulson* personally made an emotional apology, his voice cracking, to Merlo and Linda Davidson, the two who filed the class actions, and to the hundreds of women he said they "courageously" represented. "To all the women who have been impacted by the force's failure to have protected your experience at work, and on behalf of every leader, supervisor or manager, every commissioner: I stand humbly before you today and solemnly offer our sincere apology," Paulson said.

What led up to the RCMP apology
National Post, Douglas Quan and Ian Macleod, 2016 10 07
Analysis: The **issue dogged Bob Paulson from the day he was appointed RCMP commissioner in 2011: how to stamp out pervasive allegations of harassment and discrimination against women in the force**. Despite taking several steps - developing a "Gender and Respect" action plan, inviting the RCMP civilian watchdog to investigate how the force handled workplace harassment, setting new hiring and promotion targets and revising the force's harassment policy - it seemed like it was never enough. In July 2013, several of his senior advisers suggested bolder action: a public apology. They presented him with a briefing document titled "Regimental Apology: Advice to the Commissioner." But after talking it over with senior staff, Paulson shelved the idea. He felt the timing wasn't right. There was still the matter of a proposed class-action lawsuit that was drawing hundreds of women. He wanted the apology to be paired with a resolution on compensation. **"It was about being in the right place, the right mindset," said Angela Workman-Stark, a former chief superintendent** who was involved in the discussions.

Espionage bill will allow PM to muzzle watchdog, report says
Globe and Mail, Colin Freeze, 2016 10 06
Toronto - **Canada's new spy-accountability legislation will create a parliamentary watchdog that prime ministers can keep on a short leash, or even muzzle, a report on the bill by the Library of Parliament** says. The Liberal government has said the national-security legislation will create an independent committee of MPs that will have regular briefings from government spy agencies on their activities. However, a report on Bill C-22 suggests the national security and intelligence committee of parliamentarians could end up "in effect, accountable to the Prime Minster alone." The report, done by the nonpartisan Library of Parliament and released this week, is a synopsis of the bill for parliamentarians. Such reports are among the information services the staff of the library provide to MPs and senators. The Library of Parliament's report points out that the bill would allow prime minsters and cabinet to shape, block or censor the committee's work. This hits a decidedly different tone from an essay published this week by **Public Safety Minister Ralph Goodale, who said Bill C-22 creates a committee that "will set its own agenda and report when it sees fit."** Every democracy has to determine how far legislators should be able to go to act as a check on government spies,

who typically work under secret orders from presidents and prime ministers. Canada gives its elected politicians less information about and fewer review powers over the security agencies than most governments do. And, unlike its closest allies, Canada has not cleared any parliamentarians to hear state secrets. Under C-22, that would change. The prime minister would pick nine lawmakers, mostly MPs but up to two senators, who would receive regular briefings on the activities of national security agencies such as the **RCMP, the Canadian Security Intelligence Service and the Communications Security Establishment**.

Members of dormant national security roundtable seeking answers
CBC News, Alison Crawford, 2016 10 06
Ottawa—A **group of Canadians who advise the federal government on national security issues are in the dark about the future of a 16-member roundtable they were appointed to**. Members of the **Cross-Cultural Roundtable on Security** are supposed to meet in-camera at least twice a year, yet the group hasn't met since October 2014. The roundtable was set up in 2005 to act as a sounding board for cabinet ministers and other high-ranking federal executives on how security matters and government policies affect different ethnic communities. Over the years, it has covered topics such as countering violent extremism, migration and cyber-security. Tories turfed anti- radicalization specialist, but can't prove they investigated him Federal study disputes claim diaspora communities breed extremists Federal security officials meet local Somali-Canadians "I feel I'm in limbo," said Farzana Hassan, a newspaper columnist and past-president of the Canadian Muslim Congress who was appointed to the roundtable in June 2015. "It seemed like a very good fit and I jumped on the idea and I accepted the appointment, but I have not heard anything," she told CBC News. This past spring, Hassan and several other members contacted by CBC received a letter informing them that the government is re-thinking the roundtable's activities and composition. Myrna Lashley, a psychologist, was appointed to the roundtable in 2005 and has been the group's chairperson since 2007. But after receiving the letter in March, Lashley suspects her involvement has come to an end. "Effectively when you get that letter, you have been told 'thank you,'" Lashley said. In the meantime, Lashley is concerned the federal government is not communicating as effectively on national security issues with Canada's ethnically diverse communities, such as Syrian refugees. In the past, Lashley says the group met with and advised ministers of public safety and justice as well as senior executives from the **RCMP, CSIS and Canada Border Services Agency** on all sorts of issues that could or would affect an array of cultural groups.

China tries to block visits of Canadian diplomats to Tibet, says Dion
Canadian Press, Mike Blanchfield, 2016 10 06
Ottawa - **China has for years tried to block Canadian diplomats from Tibet,** banning some of them from visiting aid projects once funded by Canadian taxpayers, says Foreign Affairs Minister Stephane Dion. While China has never denied a request by a high-level diplomat to visit Tibet, Dion says, it has put up roadblocks, including delays in approving travel requests and shadowing Canadians while there. Dion describes the problems in a written response to questions from New Democrat MP Randall Garrison that was recently tabled in the House of Commons.

National security review must look beyond terrorism, expert tells MPs
Canadian Press, Jim Bronskill, 2016 10 05
Ottawa - An intelligence expert says a federal review of national security shouldn't be fixated solely on terrorism. **Wesley Wark, who teaches at the University of Ottawa, says Canadians need to have a discussion about other dangers, including cyberthreats and problems that could arise from climate change.** He told the Commons public safety committee that terrorism is just one of a number of security threats _ and it may not be the most serious one

society faces. Wark was among the first witnesses as the committee kicked off hearings that will help shape the Liberal government's security policy. The government also recently opened an online consultation soliciting feedback on issues ranging from sharing information and preventing attacks to **conducting surveillance and ensuring intelligence agencies** are accountable. In last year's election campaign, the Liberals promised to repeal "problematic elements" of omnibus security legislation, known as **Bill C-51,** ushered in by the previous Conservative government. The bill gave the Canadian Security Intelligence Service explicit powers to disrupt terrorist threats, not just gather information about them. The legislation also created a new offence of promoting the commission of terrorist offences and broadened the government's no-fly list powers. In addition, it expanded the sharing of federally held information about activity that "undermines the security of Canada."

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

FBI Hacked Computers in Australia as Part of Global Child Porn Sting
Motherboard (Vice Magazine), Joseph Cox, 2016 10 10
New York - In early 2015, **the FBI hacked thousands of computers across the world, based on a single, arguably illegal, warrant.** Now, Motherboard has learned that as part of the same operation, the FBI also hacked computers in Australia, highlighting how law enforcement agencies are increasingly using malware to remotely search computers outside of their jurisdiction. The case, codenamed Operation Pacifier, revolves around the FBI's investigation into one of the largest ever dark web child pornography sites, called Playpen. When the FBI seized the site in 2015, instead of shutting it down, the agency briefly ran Playpen from a government server in order to deploy a network investigative technique (NIT)--the agency's term for a piece of malware--in an attempt to identify its visitors. The agency's malware used a Tor Browser exploit, and then grabbed a suspected Playpen user's IP address, MAC address, and other technical information.

Spy fraud
Vice Magazine, Jason Leopold, 2016 10 09
New York - **When contractors and employees who work for America's most powerful intelligence agencies get bored at work, they sometimes kill time by viewing pornography on their classified government computers**, browsing online dating services, engaging in "sex chats" with minors, and playing games on **Facebook. And they charge U.S. taxpayers millions of dollars for it. Between 2013 and 2015, the Intelligence Community's Inspector General,** the watchdog entity overseeing 16 federal intelligence agencies, investigated dozens of instances of employee misconduct and crimes based on referrals it received from intelligence agencies. **Many of them centered on widespread contracting fraud involving individuals who worked on highly classified intelligence programs for the NSA, the CIA, and the Office of Director of National Intelligence (ODNI)** on behalf of well-known contractors such as IBM, Booz Allen Hamilton, Boeing, and General Dynamics. That's according to hundreds of pages of top-secret internal watchdog reports that were declassified and released to VICE News in response to a Freedom of Information Act lawsuit.

How U.S. Torture Left Legacy of Damaged Minds (Canada)
New York Times, Matt Apuzzo & Sheri Fink, 2016 10 08

Analysis: **Before the United States permitted a terrifying way of interrogating prisoners, government lawyers and intelligence officials assured themselves of one crucial outcome**. They knew that the methods inflicted on terrorism suspects would be painful, shocking and far beyond what the country had ever accepted. But none of it, they concluded, would cause long lasting psychological harm. Fifteen years later, it is clear they were wrong. Today in Slovakia, Hussein al-Marfadi describes permanent headaches and disturbed sleep, plagued by memories of dogs inside a blackened jail. In Kazakhstan, Lutfi bin Ali is haunted by nightmares of suffocating at the bottom of a well. In Libya, the radio from a passing car spurs rage in Majid Mokhtar Sasy al-Maghrebi, reminding him of the C.I.A. prison where earsplitting music was just one assault to his senses. And then there is the despair of men who say they are no longer themselves… In several cases, their mental status has complicated the nation's long effort to bring them to justice. **Omar Khadr,** a Canadian citizen, had been wounded and captured in a firefight at age 15 at a suspected terrorist compound in Afghanistan, where he said he had been sent to translate for foreign fighters by his father, a Qaeda member. Years later, he would plead guilty to war crimes, including throwing a grenade that killed an Army medic.

U.S. Says Russia Directed Hacks to Influence Elections
New York Times, David E. Sanger & Charlie Savage, 2016 10 08
Washington - The **Obama administration on Friday formally accused the Russian government of stealing and disclosing emails from the Democratic National Committee and a range of other institutions and prominent individuals,** immediately raising the issue of whether President Obama would seek sanctions or other retaliation. In a **statement from the director of national intelligence, James Clapper Jr., and the Department of Homeland Security, the government said the leaked emails that have appeared on a variety of websites "are intended to interfere with the U.S. election process."** The emails were posted on the well-known WikiLeaks site and two newer sites, DCLeaks.com and Guccifer 2.0, identified as being associated with Russian intelligence. "We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities," the statement said. It did **not name President Vladimir V. Putin of Russia**, but that appeared to be the intention. The statement from Mr. Clapper and the Department of Homeland Security, which is primarily responsible for defending the country against sophisticated cyberattacks, said the intelligence agencies were less certain who was responsible for "scanning and probing" online election rolls in states around the country. It said that those "in most cases originated from servers operated by a Russian company," but stopped short of alleging the Russian government was responsible for those probes.

Russia's Senior-Most officials' Ordered DNC Hack
The Daily Beast, Shane Harris and Nancy Youssel, 2016 10 08
Washington - **The Obama administration has concluded that "Russia's senior-most officials" ordered hackers to break into the computer networks of American political organizations in order "to interfere with the U.S. election process," intelligence and security agencies said** in a joint statement Friday. The statement was the administration's first public attribution of the hacks against the Democratic National Committee and a second political institution to the Russian government. Privately, officials had said for the past few months that all signs pointed to an operation being directed by Moscow intended to meddle with the November election. That evidence mounted as law enforcement and intelligence agencies sifted through technical details about the hack and eventually reached a consensus that Russia was to blame, a senior administration official told The Daily Beast.

3 Arrested in Alleged Bid to Export US Technology to Russia
Reuters, Staff report, 2016 10 07
Washington - A **U.S. citizen and two Russian nationals were arrested Thursday on charges relating to the alleged illegal export of sensitive military technology from the United States to Russia,** the Justice Department said. The department said **Alexey Barysheff** of Brooklyn, New York, a naturalized U.S. citizen, was arrested for illegally exporting controlled technology. Russian nationals Dmitrii Aleksandrovich Karpenko and Alexey Krutilin were simultaneously arrested on charges of conspiring with Barysheff, it said. All three were scheduled to appear in court Thursday afternoon. In its complaint, the government alleged the defendants had engaged in a conspiracy to obtain microelectronics from manufacturers and suppliers in the United States and export them to Russia while evading government controls on high-tech exports.

Accused Contractor Was on Hacking Team
Wall Street Journal, Damian Paletta, Scott Calvert, 2016 10 07
Washington - **Harold "Hal" Martin, the former National Security Agency contractor charged this week with stealing government secrets, spent parts of the past decade on a government hacking team**, sought funding for research into post-traumatic stress disorder, and tried to rally internet users to wage digital warfare against computer "commandos." Investigators are still trying to determine why Mr. Martin, a former employee of consulting firm **Booz Allen Hamilton** who worked on projects at the NSA and the Pentagon, took classified documents containing computer-spying tools to his home in Glen Burnie, Md. But as the probe continues, more details of his background are coming into focus. A former academic mentor of Mr. Martin described him as focused, and burdened by a sense that his insights weren't appreciated.

After latest NSA breach, does agency do enough to protect classified data?
Associated Press, Staff report, 2016 10 07
Washington - The **arrest of a National Security Agency contractor accused of stealing classified information represents the second known case of a government contractor being publicly accused of removing secret data from the intelligence agency since 2013**. The latest arrest came despite efforts to reform security after the Edward Snowden disclosures, especially in regard to insider threats. **Harold Thomas Martin III**, 51, of Glen Burnie, Maryland, was arrested by the FBI in August, after federal prosecutors say he illegally removed highly classified information and stored the material in his home and car. A defense attorney said Martin did not intend to betray his country. "One key thing we don't have visibility into now is how he was caught, because that would provide some insight into whether the reforms that were put in post-Snowden were effective or not, or their relative efficacy," said Rajesh De, who was the NSA's general counsel when the Snowden story broke and remained there until last year. Snowden's 2013 theft of documents that were leaked to journalists revealed the NSA's bulk collection of millions of Americans' phone records.

Another Security Breach Shines a Light on Booz Allen's Ubiquitous Spy Business
New York Times, Matthew Rosenberg, 2016 10 07
Washington - In the six weeks since federal agents raided a suburban Maryland home and arrested **Harold T. Martin III** on suspicion of stealing classified information from the National Security Agency, **another organization has quietly prepared to face the fallout: Booz Allen Hamilton**, Mr. Martin's employer. Booz Allen, a consulting firm that earns billions of dollars by working for American intelligence agencies, has been called the world's most profitable spy organization. News this week of Mr. Martin's arrest in August could renew scrutiny of the firm's operations and, more broadly, the lucrative contracting business that American intelligence now

relies on to run its vast, global surveillance operations. Mr. Martin's arrest is the second time in three years that a Booz Allen contractor has been **accused of stealing potentially damaging material from the N.S.A**. The company also employed Edward J. Snowden, who spirited out a cache of documents that, in 2013, exposed the extent of American surveillance programs in the United States and around the world. Tens of thousands of contractors are believed to work for American intelligence agencies (the exact number is not known). They do everything from helping secure the military against cyberattacks and plan intelligence operations, to training spies and running war games for NATO generals.

Arrest of NSA contractor highlights growing concern over insider threats
Washington Post, Christian Davenport, 2016 10 07
Washington - The **arrest of a National Security Agency contractor charged with stealing highly classified material is the latest example of a trend that officials say can be every bit as dangerous as an outside hacker: the insider threat**. The federal government has been increasingly concerned about the ability of its own employees and contractors to use their positions to walk away with troves of sensitive information. And it has tried to implement new safeguards to not only better secure important data but also monitor the people with access to it. Fears over insider threats intensified after the breach by former Army Pfc. Chelsea Manning and Edward Snowden, an NSA contractor working for Booz Allen Hamilton. But with the revelation that **Harold Thomas Martin III** was arrested in August and charged with theft of government property and unauthorized removal and retention of classified materials, there will be even greater scrutiny of how the nation protects its secrets, officials said.

N.S.A. Suspect Is a Hoarder. But a Leaker? Investigators Aren't Sure.
New York Times, Scott Shane, David E. Sanger, 2016 10 07
Washington - **On a half-dozen occasions in the last three years, top-secret information has leaked from the National Security Agency and appeared on the web.** Government analysts concluded with alarm that the documents, including intercepted communications from Europe and Japan and the computer code for the N.S.A.'s hacking tools, had not come from the huge collection taken by **Edward J. Snowden**. That meant there was at least one more leaker still at large, and when F.B.I. agents found in August that a former agency contractor had been taking home top-secret material, they thought they might have the culprit. Now they are not so sure. **Harold T. Martin III,** the contractor arrested by the F.B.I. on Aug. 27, brazenly violated basic security rules, taking home a staggering quantity of highly classified material. He had been doing this undetected, agency officials were chagrined to learn, since the late 1990s. But, officials say, they have not been able to definitively connect Mr. Martin, 51, a Navy veteran, to the leaked documents.

NSA Director Denies Mass Scanning of Yahoo Emails
Boston Herald, Jordan Graham, 2016 10 07
Boston - **Top U.S. intelligence officials denied a blockbuster Reuters report claiming Yahoo built special software to scan emails to hundreds of millions of accounts**, while a subsequent New York Times report claims the snooping was limited to suspected members of a terrorist organization. "That would be illegal. We don't do that, and no court would ever grant us the authority to do that. We have to make a specific case. And what the court grants is specific authority for a specific period of time for a specific purpose," said **Adm. Michael Rogers**, director of the **National Security Agency**, speaking at the Cyber Security Summit at Massachusetts Institute of Technology Oct. 5. "We have a legal framework in this nation that enables the government ... ?for specific reasons, under specific conditions, to make a case before a judge in which we're able to show a judge we have reason to believe that there is threat here to the United States associated with specific individuals and a judge grants,

simplistically, authority for a specific purpose for a specific period of time to access data." On Tuesday, Reuters reported Yahoo had built custom software for the U.S. government that scanned incoming emails to millions of accounts. "I've read this real quickly and I thought, well, this is a little speculative," Rogers said. In a statement, Yahoo called the story "misleading."

N.S.A. Contractor Arrested in Possible New Theft of Secrets
New York Times, Multiple reporters, 2016 10 05
Washington - The F**.B.I. secretly arrested a National Security Agency contractor in recent weeks and is investigating whether he stole and disclosed highly classified computer code developed to hack into the networks of foreign governments**, according to several senior law enforcement and intelligence officials. The theft raises the embarrassing prospect that for the second time in three years, an insider has managed to steal highly damaging secret information from the N.S.A. In 2013, **Edward J. Snowden**, who was also a contractor for the agency, took a vast trove of documents that were later passed to journalists, **exposing N.S.A. surveillance programs in the United States and abroad**. The contractor was identified as **Harold T. Martin III,** 51, of Glen Burnie, Md., according to a criminal complaint filed in late August. He was charged with theft of government property, and unauthorized removal or retention of classified documents. During an F.B.I. raid of his house, agents seized documents and digital information stored on electronic devices. A **large percentage of the materials found in his house and car contained highly classified information**. At the time, F.B.I. agents interviewed Mr. Martin, and he initially denied having taken the documents and digital files. The agency later said he had stated that he knew he was not authorized to have the materials. According to the complaint, he told the agency that "he knew what he had done was wrong and that he should not have done it because he knew it was unauthorized."

NSA Thief Worked With Elite Hacker Squad
The Daily Beast, Multiple reporters, 2016 10 06
Washington - **The retired Navy officer arrested for allegedly removing highly classified information from the National Security Agency worked with the organization's elite computer hackers,** who specialize in using computer code to penetrate the systems of foreign nations, according to a former colleague and the man's online resume. **Harold Thomas Martin, III,** who goes by Hal, was also enrolled in a PhD program at the University of Maryland Baltimore County. The university has a partnership with the NSA, in which the agency helps develop curriculum for the school and agency employees can take classes there. Martin worked with **NSA's Tailored Access Operations unit,** sources with knowledge of his background told The Daily Beast. In his LinkedIn resume, Martin says he worked as a "cyber engineering advisor" supporting "various cyber related initiatives" in the Defense Department and intelligence community. Allen was employed by NSA contractor Booz Allen Hamilton. Former intelligence officials, who said they aren't familiar with Martin's case, suggested he may have brought the material home to use as research for his PhD studies.

Obama Admin Hiding Secret Hostage Docs Signed With Iranian Intel Officials
Washington Free Beacon, Adam Kredo, 2016 10 06
Washington - **Key documents relating to the Obama administration's secret negotiations with Iran, including a $1.7 billion cash payment, are being stored at a highly secure site on Capitol Hill,** preventing the public and many in Congress from accessing them, according to multiple sources who described the situation to the Washington Free Beacon. The documents are not technically classified but are being kept in a "secure reading space" where the majority of congressional officials cannot access them. Those cleared are forced to relinquish their cellular devices and are barred from taking notes, undermining the ability of staffers to brief their lawmakers on the contents, according to the sources. Sources further disclosed that joint U.S.-

Iranian signatures across the three documents add up to a package deal between Washington and **Iran's Intelligence Ministry**, the country's internal spy agency. Sources familiar with a closed-door January briefing by senior Obama administration officials told the Free Beacon they were informed the United States negotiated with "the Iranian intelligence apparatus."

Revealed: The FBI's Secret Methods for Recruiting Informants at the Border
The Intercept, Cora Currier, 2016 10 06
Washington - Think about arriving at the airport from a foreign country. You are tired from a long flight, anxious about your baggage, and thinking about meeting your family in the arrivals area. You may not have seen them in years. Perhaps it is your first time in the United States. Perhaps you do not speak English well. Perhaps you plan to ask for asylum. Perhaps you are coming from a country where interactions with people in uniform generally involve bribery, intimidation, or worse. The **FBI and U.S. Customs and Border Protection work closely together to turn these vulnerabilities into opportunities for gathering intelligence**, according to government documents obtained by The Intercept. **CBP assists** the FBI in its efforts to target travelers entering the country as potential informants, feeding the bureau passenger lists and pulling people aside for lengthy interrogations in order to gather intelligence from them on the FBI's behalf, the documents show. In one briefing, CBP bills itself as the "GO TO agency in the Law Enforcement world when it comes to identifying individuals of either source or lead potential."

Top CIA officers to face questions about brutal interrogations in civil suit
Washington Post, Greg Miller, 2016 10 06
Washington - **Two former high-ranking CIA officials will be compelled to answer questions under oath about the agency's brutal interrogations of terrorism suspects**, a federal judge ruled Tuesday as part of a lawsuit brought against former CIA contractors by the American Civil Liberties Union. The ruling would require **Jose Rodriguez, who was the head of the CIA's Counterterrorism Center** after the Sept. 11, 2001, attacks on the United States, and **John Rizzo, the agency's former acting general counse**l, to submit to depositions about a program that used methods widely condemned as torture. "This ruling is a critical step towards accountability, and it charts a way forward for torture victims to get their day in court," ACLU attorney Dror Ladin said in a statement released by the organization after the ruling in federal court in Spokane, Wash.

NSA has lost some terrorists because of encryption, its top lawyer says
CNBC, Harriet Taylor, 2016 10 05
Cambridge - The **NSA has lost some terrorists because of their adoption of strong encryption, but the agency is supportive of the use of the technology**, it's top lawyer said Wednesday. **Glenn Gerstell**, general counsel of the National Security Agency, made the comments at the Cambridge Cyber Summit at MIT in Cambridge, Massachusetts. "We are big supporters of encryption," said Gerstell. "Encryption is more of a law enforcement issue." He said the NSA sees ISIS terrorists using end-to-end encryption, and that has prevented the agency from finding out the key information about those bad actors.

The Aspen Institute's Walter Isaacson Interviews Admiral Michael S. Rogers from the Cambridge Cyber Summit Today
CNBC website, Walter Isaacson, 2016 10 05
WALTER ISAACSON: Thank you. Thank you very much, Michael, for being with us today. The latest of these is Yahoo, in which supposedly a lot was just read because they were ordered to do so. I just got a statement from them, an email, saying, no, no it wasn't really that way. We did not open up all of the emails. It was a much narrower complying with orders. Talk to us about the type of things you need to do and have industry cooperate with you, why that's legal and

where you think we have to draw the line. **ADMIRAL ROGERS: So clearly we have a legal framework in this nation that enables the government under specific -- for specific reasons, under specific conditions, to make a case before a judge in which we're able to show a judge we have reason to believe that there is threat here to the United States associated with specific individuals and a judge grants, simplistically, authority for a specific purpose for a specific period of time to access data.** And the court order is then given to the private sector to execute. This is done -- phone records, bank records, this is a long- standing mechanism in our nation for how does the government access information using a lawful mechanism to do that. Cyber and intelligence, in this aspect, is no different then. WALTER ISAACSON: Let me make sure I heard you correctly. That means you couldn't get one that would just blanket look at all emails. ADMIRAL ROGERS: No. I was going to say, that would be illegal. We don't do that, and no court would ever grant us the authority to do that. We have to make a specific case. And what the court grants is specific authority for a specific period of time for a specific purpose. It's not a blanket, A, just everything. WALTER ISAACSON: So we shouldn't believe the stories that we read? ADMIRAL ROGERS: I've read this real quickly and I thought, well, this is a little speculative.

Homeland Security Deputy Secretary stepping down
Federal News Radio, David Thorton, 2016 10 06
Washington - **Department of Homeland Security Deputy Secretary Alejandro Mayorkas announced that he is stepping down effective Oct. 28**. Mayorkas announced his departure and thanked the department in a staff email sent out Oct. 5 and obtained by Federal News Radio. "I began my government service as a federal prosecutor, a position I held for nearly twelve years, and I have been a member of our department for nearly seven years," he said. "I have cherished every moment of public service. Thank you for making it so."

Yahoo secretly scanned customer emails for U.S. intelligence - sources
Reuters, Joseph Menn, 2016 10 04
San Francisco - **Yahoo Inc last year secretly built a custom software program to search all of its customers' incoming emails for specific information provided by U.S. intelligence officials,** according to people familiar with the matter. The company complied with a classified U.S. government directive, scanning hundreds of millions of Yahoo Mail accounts **at the behest of the National Security Agency or FBI,** said two former employees and a third person apprised of the events. Some surveillance experts said this represents the first case to surface of a U.S. Internet company agreeing to a spy agency's demand by searching all arriving messages, as opposed to examining stored messages or scanning a small number of accounts in real time. It is not known what information intelligence officials were looking for, only that they wanted Yahoo to search for a set of characters.

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

Police use snooping devices on phones
London Times, Fiona Hamilton, 2016 10 11
London - A **string of police forces have secretly purchased surveillance technology that enables large amounts of phone data to be collected from passers-by**, it has emerged. At least seven forces in England and Wales are now thought to be using IMSI Catchers that can collect and identify call and message data from mobile phones within a given area. They mimic

mobile-phone towers and act as a "dummy", sending out signals that trick devices into automatically trying to connect to them. Police find the Catchers useful to track suspects and uncover their phone activity, but they can capture information from other mobiles within a radius of up to five miles. It is believed that there is no automatic deletion of the gathered material from police systems, meaning that forces could be harvesting information about tens of thousands of members of the public.

Pour se protéger contre l'espionnage russe, le gouvernement britannique bannit l'Apple Watch
FranceTv Info (site web), Journaliste maison, 2016 10 11
Londres - **Pour se protéger contre l'espionnage russe, le gouvernement britannique bannit l'Apple Watch des ministères** En Grande Bretagne, la montre connectées d'Apple est désormais interdites lors des réunions ministérielles. Les services de sécurité pensent que la Russie pourrait y placer un mouchard. La montre connectée d'Apple n'est pas la bienvenue au sein du gouvernement britannique. Le gadget est désormais banni des ministères. Motif ? Un risque d'espionnage. Des hackers pourraient se servir de ces montres pour écouter les conversations de leurs propriétaires.

Apple Watches banned from Cabinet after ministers warned devices could be vulnerable to hacking
London Daily Telegraph, Peter Dominiczak, 2016 10 09
London - **Ministers have been barred from wearing Apple Watches during Cabinet meetings amid concerns that they could be hacked by Russian spies**, The Telegraph has learned. Under David Cameron, several cabinet ministers wore the smart watches, including Michael Gove, the former Justice Secretary. However, under Theresa May ministers have been barred from wearing them amid concerns that they could be used by hackers as listening devices. Mobile phones have already been barred from the Cabinet because of similar concerns. One source said: "The Russians are trying to hack everything."

Female spy spills MI6 secrets including details over agency's 'Q'
The Express (UK), Zoie O'Brien, 2016 10 05
London - **Thousands of listeners tuned in to hear the agent discuss what life is like for a real James Bond.** The agent given the name "**Emma**" has her vice distorted as she chatted to Radio 2 host Chris Evans on Tuesday morning. "Emma" revealed similarities in her life to the 007 films - like calling her bosses by just one letter. "Everyone has massive misconceptions they think it's all cars with spike things coming out the side and motorbikes with parachutes on. It's nothing like that. We have lots of gadgetry, lots of people who are really creative, really technical and have a fantastic time thinking about things and inventing things. It's not what people think."

Muslims see Prevent programme as spying scheme, watchdog admits
The Independent (UK), Joseph Watts, 2016 10 07
London - The **UK's terror law watchdog has said Muslim communities see the Government's anti-extremism strategy as a "spying programme"** and called for it to be overhauled. **David Anderson** QC claimed many people believe the programme targeted the "practice of Islam" as opposed to the spread of radical beliefs. He urged ministers to conduct an independent review of the scheme, which is designed to help officials spot individuals who are becoming radicalised. Mr Anderson said: "There is a strong feeling in Muslim communities that I visit, that Prevent is, if not a spying programme, at least a programme that is targeted on them. In some cases, it is even felt it is targeted not just at Islamist terrorism or extremism, but at the practise of Islam. People who pray or who wear the veil, for example, are sometimes felt to be

under suspicion." He added: "Now, I'm sure those fears are exaggerated, and they are certainly not what the programme is supposed to be about, but the fact is that they are very real. So it is frustrating for me to see a programme whose ideals are so obviously good, falling down on the delivery to the point where it is not trusted in the community where it principally applies."

Return to Table of Contents/ Retour à la table des matières

Australia / Australie

Australians want tougher terror measures

Australian Associated Press, Staff Writer, 2016 10 11

Canberra - A m**ajority of Australians want the government to do more to prevent terrorist attacks on home soil a**nd are happy to give up some personal freedoms to help the cause, new research shows. But many are concerned that Muslims are being singled out for increased surveillance and monitoring. The Australian National University poll found 71 per cent were worried about the rise of Islamist extremism in Australia while nearly as many felt Muslims shouldn't be subject to additional scrutiny based on their religion. "People are obviously concerned whether it's the faith of Islam that gives rise to these things," co-author Katja Theodorakis told reporters on Monday. "That's something that warrants further study because that could have political ramifications and divisions - and it's not good for social cohesion in a multicultural society."

Anti-terror plan for domestic thugs

The Australian, Amos Aikman, 2016 10 07

Canberra - The **Northern Territory's top cop wants to deploy "counter-terrorism-like" tactics against violent and alcoholic thugs who repeatedly bash their families**, warning that recidivists pose a danger to society at large and tougher measures are needed to control them. While no details have been announced, The Australian understands the proposals would see police apply to courts for "prohibition orders" targeting the nastiest offenders when they leave jail. A person subject to such an order would have to report to police regularly and keep away from certain individuals and areas -- similar to the rules applied to some sex criminals -- and could be sent to prison for up to a further five years if they did not comply. Consideration is also being given to seeking wider legislative reform that would allow police to apply for a prohibitive order against a person not convicted of any crimes, where there is evidence doing so would significantly improve community safety.

Return to Table of Contents/ Retour à la table des matières

New Zealand / Nouvelle-Zélande

Spark seeks details on US email scans

New Zealand Herald, Nicholas Jones, 2016 10 06

Wellington - **Kiwi telco Spark is seeking clarification from Yahoo as to whether any of its customers had email searched at the behest of United States intelligence agencies**. According to an investigation by Reuters, Yahoo last year used a software program to search its customers' incoming email for specific information provided by US intelligence agencies. That happened after the Yahoo complied with a classified US government demand, it was reported.

Spark is seeking more information, including whether Spark's Xtra Mail customers could have been affected. Yahoo hosts more than 800,000 accounts on behalf of Spark. "At this time we are still seeking clarification from Yahoo if any Spark Xtra email customers are involved," a spokeswoman told the Herald. **Privacy Commissioner John Edwards** said Spark was right to be making its own inquiries. "I would be concerned if these kinds of arrangements were occurring without a clear legal authority. But we haven't seen enough in the Reuters report to know the basis of it."

Return to Table of Contents/ Retour à la table des matières

International

China / Chine

China says anti-terrorism cooperation should follow int'l law
Xinhua News Agency, 2016 10 11
Beijing - **China on Monday said international anti-terrorism cooperation should follow international law** and basic norms and principles of international relations. "No domestic law shall be above international law," Foreign Ministry spokesperson **Geng Shuang** said at a daily press briefing in response to a question concerning the Justice Against Sponsors of Terrorism Act (JASTA) recently passed by the U.S. Congress. China maintains that international anti-terrorism cooperation should allow the United Nations the leading role, accord with the purposes and principles of the Charter of the United Nations, and follow international law and basic norms of international relations, including the doctrine of sovereignty equality, he said.

Half of Chinese Favorable Toward U.S., but Many See a Threat, a Survey Finds
New York Times, Edward Wong, 2016 10 06
Beijing - With tensions between the United States and China on the rise over issues such as the South China Sea and **cyberespionage**, one might think the citizens of the two nations have an increasingly hostile view of the other. Yet, **Chinese have a more favorable view of the United States than they did a year ago, according to the results of a global survey released by the Pew Research Center on Wednesday.** They hold that perspective even as many cite the United States as a major threat to China, Pew said. The report also said that although three-quarters of Chinese say their country is playing a larger role in the world than it did a decade ago, most want their government to focus on domestic issues rather than helping other nations. And more than three-quarters say their way of life needs to be protected from foreign influence -- a 13 percentage-point increase from 2002.

Return to Table of Contents/ Retour à la table des matières

Russia / Russie

Foreign Intelligence Service to preserve continuity, follow rich traditions of Soviet and Russian agents - new chief
Interfax News Agency, 2016 10 06

Moscow—The **new director of Russia's Foreign Intelligence Service (SVR), Sergei Naryshkin, has pledged to preserve continuity within the organization and attain its goals**. Naryshkin said this to reporters after being introduced to the staff by Russian President Vladimir Putin at the SVR headquarters. "The Foreign Intelligence Service is one of the best prepared and efficient agencies in the world," Naryshkin said. "I think that in its work, it is necessary to preserve continuity and follow the rich traditions formulated by many generations of Soviet and Russian intelligence officers, and I intend to ensure this continuity," the new SVR director said, adding that herein lies the guarantee "of successful resolution of those very serious and large-scale problems that face the Service's personnel."

Naryshkin worked well in intelligence, politics, 'goes home' – Putin
Interfax News Agency, 2016 10 05
Moscow—Russian President **Vladimir Putin has visited the Moscow headquarters of the Russian Foreign Intelligence Service to introduce Sergei Naryshkin to employees as its new head**. The former State Duma speaker took the position of Foreign Intelligence Service director on Wednesday. "Dear colleagues, I am officially introducing Sergei Yevgenyevich Naryshkin as the new Service director," the president told the service staff."As you know, he worked well in the intelligence service, when he was with it, and in politics. In this sense, Sergei Yevgenyevich is coming home," Putin said.

Putin: Russia's Foreign Intelligence Service Must Be Proactive, Innovative
Sputnik, Staff report, 2016 10 05
Moscow - The **Russian Foreign Intelligence Service (SVR) should be proactive by taking innovative steps and identify key tendencies of development of the international situation, Russian President Vladimir Putin said** Wednesday. "Today the situation in the world makes special demands to the quality and effectiveness of the SVR work. It is necessary to be proactive, use innovative, unconventional decisions," Putin said. He also stressed the importance of identifying and analyzing "the whole spectrum of external threats, identifying key strategic trends in the development of the international situation, contributing to the strengthening of economic, technological and military potential of Russia. " "Of course the safety of our citizens should be under special control, especially in regions such as the Middle East, Africa, as well as in certain Central Asian countries," Putin said at a ceremony formally appointing Sergei Naryshkin to lead the SVR.

Russia denies drugging US diplomats
CNN.com, Jamie Crawford, 2016 10 05
Washington - A **top Russian official strongly denied Wednesday a report that Moscow may have been behind the alleged drugging of two US diplomats in St. Petersburg** and suggested instead that the pair may simply have been drunk. "We are outraged," Russian **Deputy Foreign Minister Sergey Ryabkov** said in a statement posted on the Russian Foreign Ministry website, adding the claim may have been the work of the US State Department seeking "revenge" for the collapse of talks between the two counties to address the situation in Syria. Russia's denial came after a report two days ago by **Radio Free Europe/Radio Liberty** that the diplomats -- a man and a woman who were not senior officials -- allegedly had their drinks spiked with a date- rape drug while attending a United Nations convention on corruption last November. The report, attributed to anonymous sources, said the State Department quietly protested the incident to Russian officials. The story also said one of the diplomats had been treated at a "Western medical clinic" - which Russia said was not true.

Two U.S. Diplomats Drugged In St. Petersburg Last Year, Deepening Washington's Concern
Radio Free Europe, Mike Eckel, 2016 10 03
Washington - **Two U.S. officials traveling with diplomatic passports were drugged while attending a conference in Russia last year**, and one of them was hospitalized, in what officials have concluded was part of a wider, escalating pattern of harassment of U.S. diplomats by Russia. The incident at a hotel bar during a UN anticorruption conference in St. Petersburg in November 2015 caused concern in the **U.S. State Department**, which quietly protested to Moscow, according to a U.S. government official with direct knowledge of what occurred. But it wasn't until a dramatic event in June, when an accredited U.S. diplomat was tackled outside the U.S. Embassy in Moscow, that officials in Washington reexamined the November drugging and concluded they were part of a definite pattern. According to the U.S. government official, and another former official also knowledgeable about the case, the drugged diplomats were part of a delegation of Americans attending the Conference of the States Parties to the United Nations Convention against Corruption, held on November 2-6 in St. Petersburg.

Is Vladimir Putin Poisoning U.S. Diplomats?
The Daily Beast, Anna Nemtsova, 2016 10 05
Moscow - A **sensational report about drugged U.S. diplomats published by the U.S. government funded Radio Free Europe/Radio Liberty on Monday has met with a certain irony, and even skepticism among veteran correspondents here**. According to the report, last year two mid-level U.S. officials visiting St. Petersburg for a conference were drugged in the bar of an upscale hotel, which was not named. The effect of the poison was so dramatic that one of the visitors was hospitalized, a U.S. government official told RFE/RL. When the victim was taken to an independent clinic, the power went out so no samples could be taken. All this was part of pattern of harassment, the article noted, that included creepy poltergeist- like incidents where American diplomats would open the doors of their apartments to discover faucets inexplicably turned on, or a cigarette left burning, or human excrement on the floor. Way back in 2013, when relations between Moscow and Washington were relatively civil, the State Department inspector general complained that U.S. employees in Russia were facing "intensified pressure by **the Russian security services** at a level not seen since the days of the Cold War." But, then, Washington generally kept quiet. That the story is coming out now is just one more sign that relations are no longer civil at all. And this week the Cold War vituperation between Moscow and Washington sounded especially bad.

Lawyer files appeal against arrest of Sushchenko charged with espionage in Russia
Interfax (Ukraine), Staff report, 2016 10 05
Moscow - A **lawyer has challenged the arrest of Ukrainian citizen Roman Sushchenko, who is under arrest in Russia on espionage charges**, the press service of Moscow's Lefortovsky District Court told Interfax. "We have received an appeal from a lawyer against the court resolution on the preventive measure against Sushchenko in the form of custody. The lawyer requests [the court] to cancel its resolution and select a softer preventive measure against his client," Yekaterina Krasnova, spokesperson for the court, said. **Russia's Federal Security Service (FSB)** reported on October 3 that "Ukrainian military intelligence career officer Col. Sushchenko had been detained in Moscow when gathering intelligence."

Ukrainian journalist detained in Russia, accused of espionage
Kyiv Post, Yuliana Romanyshyn, 2016 10 05
Kyiv - **Ukrainian journalist Roman Sushchenko was placed in detention for two months by Lefortovo District Court in Moscow on Oct. 3** after being arrested by Russia's Federal Security Service on charges of spying. Sushchenko worked as a foreign correspondent in Paris,

France, for Ukrainian online news agency Ukrinform. He was in Moscow in personal business, Ukrinform said. Ukrinform rejected the charges against their employee, and said the FSB violated the law while arresting him. According to Ukrinform, the federal security agents officially informed neither his employer nor his wife of his arrest, although his relatives in Moscow were aware he had been detained.

Return to Table of Contents/ Retour à la table des matières

Europe

Danish security agency files charges against former boss
The Local (Denmark), 2016 10 11
Copenhagen—The **Danish Security and Intelligence Service (PET) reported its former director Jakob Scharf to the police on Tuesday for violating a confidentially agreement**. Scharf is the subject of journalist **Morten Skjoldager's new book 'Seven Years for PET'**, the release of which the intelligence service blocked through an injunction last week. On Monday, it was revealed that Scharf had signed an agreement with PET stating that he would seek the agency's prior approval before participating in a book project or any other activity that could entail the dissemination of sensitive information. Copenhagen City Court blocked the book without PET even having read it. The injunction was filed solely based upon publicity material distributed by publisher People's Press. **PET's attempt to block the book's release was met by defiance in some quarters.** Politiken newspaper published the book in its entirety as a special section in its Sunday edition and some booksellers sold copies of the book despite the injunction. Broadcaster Radio 24syv also covered the contents of the book. PET formally rescinded the ban request, but said on Tuesday that it has now filed police charges against Scharf.

German spy chief says Syrian suspect targeted Berlin airports
Reuters, Staff report, 2016 10 11
Berlin - The **head of Germany's domestic intelligence agency (BfV) said a Syrian suspect arrested on Monday was building a bomb and probably planned to attack one of the airports in Berlin. Hans-Georg Maassen** told public broadcaster ARD that intelligence leads had suggested in early September that militant group Islamic State (IS) was planning an attack on Germany's transport infrastructure. Spies managed to track down and identify the suspect in the eastern state of Saxony last Thursday and started a round-the-clock observation, Maassen said. "We found out that he then bought hot glue in a discount shop on the following day. And then we immediately put all measures into place to start a raid because we assumed this can basically be the last missing chemical for him to build a bomb."

Faut-il limiter la loi sur le renseignement ?
La Provence, Journaliste maison, 2016 10 11
Paris - La **loi sur le renseignement permet-elle de surveiller toutes les communications sans fil "sans cadre contraignant" au nom de la sécurité?** C'est ce qu'affirment trois associations, qui attaquent aujourd'hui au Conseil constitutionnel un article de la loi votée en juin 2015. Cette loi avait été adoptée six mois après les attentats djihadistes contre l'hebdomadaire satirique Charlie Hebdo et contre le magasin Hyper Cacher. Ce n'est pas la première fois que la Quadrature du Net, le fournisseur d'accès French Data et la Fédération des fournisseurs d'accès à internet (FFDN) dénoncent des "définitions tellement vagues de la défense des intérêts nationaux que tout peut y correspondre". Le Conseil constitutionnel a déjà validé à deux reprises cet été des dispositions contestées, portant sur la surveillance des

données de connexion des usagers d'internet (loi de programmation militaire) ainsi que la majeure partie de la loi renseignement, dont le volet sur les "interceptions administratives".

SBU arrests Russian spy in Rivne
Interfax (Ukraine), Staff report, 2016 10 10
Kyiv - A **spokesperson for the Ukrainian Security Service (SBU) said that a Russian intelligence agent has been held in the town of Rivne**. "The spy, a Ukrainian citizen who permanently resides in Russia, was to recruit a senior officer from the headquarters of the Ground Force of the Ukrainian Armed Forces," the SBU spokesperson said in a statement on Sunday. "In exchange for passing documents classified as 'secret' and 'top secret' concerning the military training, armament, mobilization deployment and military cooperation between the Ukrainian Armed Forces and foreign partners, the GRU [Russian military intelligence] agent was to offer to a Ukrainian officer and his family Russian citizenship and money.

Pourquoi l'affaire Squarcini inquiète la DGSI (et le sommet de l'Etat)
Marianne2 (site web), Frédéric Ploquin, 2016 10 10
Paris - **L'enquête que mènent deux juges d'instruction parisiens, Serge Tournaire et Aude Buresi, autour de Bernard Squarcini est une bombe à retardement. Notamment pour son successeur, Patrick Calvar.- Sipa « Pourquoi les fonctionnaires de la DGSI continuent-ils à vous appeler 'chef' » ?** demande un enquêteur de la police des polices à Bernard Squarcini, placé en garde-à-vue pour 48 heures, le 28 septembre dernier. « Ils m'ont toujours appelé chef », réplique l'ancien espion préféré de Nicolas Sarkzoy, désormais à la tête de la société privée de conseil en sécurité Kyrnos (le nom que les Grecs anciens donnaient à la Corse). L'enquête que mènent deux juges d'instruction parisiens, Serge Tournaire et Aude Buresi, autour de Bernard Squarcini est une bombe à retardement. Ce n'est pas tant l'ancien président de la République qu'elle fait trembler, mais les actuels dirigeants de la **Direction générale de la sécurité intérieure (DGSI)**, fer de lance de la lutte contre le terrorisme. A commencer par son patron, Patrick Calvar, un homme qui a toujours pris soin de ne s'affilier à aucune écurie politique.

Affaire Squarcini: le directeur de la DGSI Patrick Calvar bientôt réentendu?
L'Express, Journaliste maison, 2016 10 10
Paris - **D'après Marianne, l'actuel patron de la DGSI risquerait d'être poursuivi pour "complicité de compromission du secret défense" dans le cadre de l'enquête qui vise son prédécesseur Bernard Squarcini.** L'affaire Squarcini serait "une bombe à retardement", pas tant pour Nicolas Sarkozy que pour **Patrick Calvar**, l'actuel directeur de la DGSI, selon les informations de Marianne . Ce dernier, qui a déjà été entendu comme simple témoin dans la plus grande discrétion le 29 septembre, serait sous la "menace de poursuites pour complicité de compromission du secret défense", écrit l'hebdomadaire ce lundi matin.

Danish paper to defy court ban and publish book on ex-spy chief
The Peninsula (Denmark), 2016 10 09
Copenhagen: A **Danish newspaper said Sunday it will defy a court ban and publish excerpts of a book about the country's former intelligence chief to protest censorship**. "This ban directly attacks the fundamental liberties on which our open society and free press depends," said Christian Jensen, editor-in-chief of Politiken, the country's paper of record. The **Danish Security and Intelligence Service (PET)** had obtained a provisional injunction Friday from the Copenhagen district court against the publication of the book, fearing it could contain secrets. The book, called "Seven Years for PET -- **Jakob Scharf's Time" is based partly on interviews with the former spy chief and was due to go on sale from October 17** and be serialised in Politiken on Monday. "The summary of the book on the site of (publisher) People's

Press gives the impression that the book might contain confidential information, the disclosure of which might endanger lives or hamper the PET's capacity to prevent crimes... like terrorism," said the agency. Jensen said that "if the PET, without concrete evidence, can exert control on books, or media articles, then this suggests we have effectively accepted an intelligence agency as an authority on publication, which would hamper the freedom of the press. There is another word for that: censorship".

Ukraine says catches Russian military intelligence spy red-handed
Reuters, 2016 11 09
Kiev—**Ukraine's State Security Service (SBU) said on Sunday it had caught red-handed a Ukrainian working as a spy for Russia's military intelligence agency**, just days after a Ukrainian journalist was arrested on espionage charges in Russia. The unnamed suspect had come to SBU's attention after he offered a senior Ukrainian military official Russian citizenship and money in exchange for top secret documents on Ukraine's military capabilities and work with foreign partners, it said. "He was caught by SBU officers red-handed while receiving a flash drive containing misinformation that he believed to be secret documents of a military nature," a SBU statement said. There was no immediate comment from Russian authorities.

France to invest $47 mln in Sahel counter-terror training
Reuters, 2016 10 08
Paris - **France plans to invest 42 million euros ($47 million) to help countries of Africa's Sahel region prepare to face extremists attacks** similar to those that killed dozens in Paris in 2015, an interior ministry official said on Friday. The Sahel, a politically fragile region whose remote desert spaces host a medley of extremists groups, is seen as vulnerable to further attacks after strikes on soft targets in Burkina Faso and Ivory Coast earlier this year. Nearby Senegal, a Western security partner with a long history of stability, has so far been spared. "In future we will train all the countries of the G5 Sahel and Senegal with 42 million Euros in financing, including 24 million Euros for equipment," said a spokeswoman for Interior Minister **Bernard Cazeneuve** during his visit to Dakar on Friday. G5 Sahel is a regional security organization composed of Chad, Niger, Burkina Faso, Mali and Mauritania. The investment period is 2017-2022, the spokeswoman added.

Lutte contre le terrorisme : l'état des lieux de Georges Fenech
La Dépêche du Midi, Romain Gruffaz, 2016 10 07
Aveyron, France - Geo**rges Fenech, député Les Républicains du Rhône, a été invité par son homologue aveyronnais Yves Censi à animer, hier soir, une conférence à propos des moyens mis en oeuvre par l'État pour lutter contre le terrorisme**. « Il faut aller au contact des gens, les rencontrer et répondre à leurs questions », a souligné l'ancien juge d'instruction, qui a présidé la commission d'enquête sur les attentats de Paris, à l'issue de laquelle un rapport pointant les erreurs commises, et contenant quarante propositions pour tenter d'y remédier, a été rendu. « La réorganisation du renseignement a été l'un des points centraux, a-t-il expliqué. Le problème est que l'on n'a pas tiré toutes les conséquences de ce qui a été présenté, par les responsables de **la DGSI et de la DGSE** eux- mêmes, comme "un échec de leurs services". En ce qui nous concerne, nous sommes pour la création d'une agence nationale antiterroriste, sur le modèle du **National Counterterrorism Center américain**, dont la coordination se ferait au niveau du chef de l'État et non pas du ministre de l'Intérieur, qui n'a pas autorité sur ses homologues. Il faut également accroître la coopération à l'échelle européenne, même si cela nécessite de céder un peu de sa souveraineté.

La Suisse plus restrictive
Le Temps (Suisse), Sylvia Revello, 2016 10 06

Berne - Expert en droit des médias et des nouvelles technologies, Nicolas Capt analyse l'affaire Yahoo! du point de vue juridique suisse Peut- on envisager un accord similaire à celui de Yahoo! entre les autorités et des fournisseurs suisses? Au-delà du caractère illégal, cette situation me paraît peu probable. Le **cadre helvétique est bien plus restrictif, y compris avec la nouvelle loi sur le renseignement,** qui pose de nombreux garde-fous. De la part des autorités pénales comme du **Service de renseignement de la Confédération (SRC),** l'observation des données privées reste limitée et surtout ciblée. La vraie différence réside dans une certaine opacité de la surveillance du SRC qui officie, par principe, hors de toute procédure pénale. La **NSA** avait-elle vraiment besoin que Yahoo! lui fournisse ses données, connaissant sa puissance de frappe? Il n'est pas absolument certain que la NSA soit capable de procéder seule à une surveillance aussi large.

German intelligence faces new cover-up claims in neo-Nazi case
Daily Sabah, Staff report, 2016 10 06
Istanbul - **Germany's intelligence services are once again subject to allegations of a cover-up with regards to the neo-Nazi National Socialist Underground (NSU)** gang that is implicated in the racist murders of Turks in the country. Lawyers for the family of Mehmet Kubasik, killed by the NSU in 2006, filed a criminal complaint against Lothar Lingen, a senior official in the Federal Office for the Protection of the Constitution (BFV), Germany's domestic intelligence agency. Lingen, who was in charge of the BFV's division monitoring the far-right scene, is accused of destroying documents that could have shed light on the NSU's murders. Speaking to Anadolu Agency after filing the complaint against Lingen, Carsten Ilius, lawyer for the family of Kubasik, said new revelations on the case added to suspicions that the BFV destroyed paperwork that might be related to the NSU in 2011.. He said Lingen's statements during the legal process concerning the NSU showed intelligence officials were concerned about facing an inquiry if it was revealed that the **BFV** did not act though it knew about the neo-Nazi gang thanks to its informants in the far-right scene.

Les renseignements n'ont pas vu venir le 22 mars
La Libre, 2016 10 06
Bruxelles— **Nous avons fait tout ce que nous devions faire" : le patron du service de renseignements militaires (SGRS) l'a dit sans ciller**. Son service ne disposait d'aucune information qui aurait permis d'éviter les attentats de Paris et de Bruxelles. Et pourtant, a dit le général **Eddy Testelmans** au cours de son audition devant les députés de la commission d'enquête sur les attentats du 22mars, ils collaboraient avec une vingtaine de services de renseignements étrangers. Interrogé sur le pourquoi, il a indiqué qu'il n'avait pas "d'explication mathématique". Mais il voit bien l'un ou l'autre facteur : tout d'abord la complexité de ces dossiers de "Foreign Terrorist Fighters". Ceux-ci peuvent circuler sans entraves dans l'espace Schengen et même en Turquie. Il est dès lors très difficile de suivre leurs traces, surtout, a-t-il expliqué, s'ils ont reçu une formation. Le **SGRS** ne travaillait à l'époque que sur une vingtaine de djihadistes partis en Syrie qui étaient alors considérés comme prioritaires.

Lutte contre le terrorisme - Le patron de la Sûreté de l'Etat demande le doublement de ses effectifs
Agence Belga, 2016 10 05
Bruxelles— **L'administrateur de la Sûreté de l'Etat, Jaak Raes, a demandé mercredi le doublement à terme de ses effectifs.** Le **service civil de renseignement** dispose actuellement de 571 personnes pour un budget de 45 millions d'euros. "On ne peut presser éternellement le citron", a-t-il fait remarquer devant la commission d'enquête sur les attentats du 22 mars. Le patron de la Sûreté a comparé la situation de son service avec les pays proches et semblables à la Belgique. Au Pays-Bas, l'AIVD dispose de 1.500 agents pour un budget de 200

millions d'euros. En Suède, le **SAEPO** dispose de 1.100 agents pour un budget de 123 millions d'euros. Au Danemark, le **PET** dispose de 780 agents pour un budget de 75 millions d'euros. La Sûreté, comme le **Service Général du Renseignement et de la Sécurité (SGRS - militaire),** dit également éprouver des difficultés de recrutement dans le circuit traditionnel du Selor. La procédure complique la recherche de profils inhabituels, disposant de compétences particulières, et débouche trop souvent sur des profils "standard". M. Raes a plaidé en faveur d'un statut particulier pour les agents de la Sûreté, du SGRS et de l'Organe de Coordination et d'Analyse de la Menace (OCAM), qui permettrait notamment de faire face à des besoins temporaires.

Turkey detains 55 military, intelligence personnel over attempted coup – media
Reuters, 2016 10 05
Ankara—**Turkey detained 55 military and intelligence agency personnel on Wednesday** over suspected links with U.S.-based cleric **Fethullah Gulen** and his network, accused by Ankara of orchestrating a failed coup in July, media reports said. In the latest of a stream of raids targeting those suspected of ties to the putsch, police carried out operations in 31 provinces after prosecutors issued detention warrants for a total of 101 suspects, state-run Anadolu Agency reported.

26 detained over Gülen links in army, intelligence in coup attempt probe
Hurriyet Daily News, Staff report, 2016 10 05
Ankara - **Police detained a total of 26 suspects on Oct. 5 in an operation targeting the members of the Gülen movemen**t, which has been blamed for the July 15 coup, in Turkey's army and intelligence services. The Ankara Public Prosecutor's Office issued detention warrants for 101 suspects, the organization's alleged imams in the Turkish Armed Forces (TSK) and the **National Intelligence Organization (MIT),** during the operation that was conducted in 31 provinces. "Imam," which traditionally refers to a religious public worker, is a term used by the Gülenist organization to mark local leadership.

Les fonctionnaires face à la radicalisation
Midi Libre, Lola Cros, 2016 10 05
Non identifié - **Plus de 130 agents du département ont suivi une formation sur le phénomène et les moyens de l'affronter**. Parce qu'ils sont en première ligne face au public, parce qu'ils représentent l'État et ne sont ainsi « pas des citoyens comme les autres » , plus de **130 agents territoriaux du département étaient invités, jeudi, à suivre une formation sur le thème : « La radicalisation : quels enjeux pour les collectivités locales, quelles pistes d'action ?** » Une formation proposée nationalement par le **Centre de la fonction publique territoriale (CNFPT**) et relayée par ses antennes locales. « Choisir la radicalisation comme thème de formation, ou plutôt de sensibilisation, est une décision politique de notre établissement , explique Gérard Chaubet, chargé de mission au CNFPT. Elle ne découle pas d'une demande explicite des agents, mais le nombre exceptionnel d'inscriptions prouve que c'est une vraie préoccupation pour les fonctionnaires.

Georgian security services blamed for attack on MP
UK Times, Tom Parfitt, 2016 10 05
Moscow— A **leader of Georgia's main opposition party has accused the country's security services of being behind an apparent assassination attempt on one of its MPs days before parliamentary elections. Givi Targamadze**, an MP with the United National Movement, and his driver escaped injury when their car blew up in the capital Tbilisi, injuring five passers-by. Giorgi Bokeria, one of the leaders of the UNM, blamed state security agents acting on behalf of the governing Georgian Dream party. David Usupashvili, the parliamentary

speaker, suggested that the attack was a Russian plot to undermine Georgia before the elections on Saturday. Mr Bokeria said: “There are no illusions in Moscow that a pro-Russian force will be victorious in these elections, so if it has a chance to destabilise Georgia then it won’t turn it down.” He claimed “everyone” knew that Mr Targamadze had a “political stand-off” with the **State Security Service** and its boss, Ioseb Gogashvili. “All of us have a reason to suspect them,” he said.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Mossad and IDF both conclude Ron Arad died in captivity

Jerusalem Post, Zack Pyzer, 2016 10 11

Jerusalem - 30 years after Israeli navigator Lt.-Col. Ron Arad ejected from his Mirage plane over Lebanon, Channel 2 reported on Monday that two new intelligence reports have been compiled in an attempt to uncover the enduring mystery of his fate. Having been officially listed as missing in action since the incident 1986, few if any had realistic hopes that the airman was still alive. The reports confirmed the fears, indicating that Arad had indeed died in captivity, and earlier than previously estimated by the authorities. Both of the reports, compiled separately by the **IDF's Military Intelligence Directorate (AMAN) and Mossad,** included a comprehensive examination of new intelligence, in addition to previously obtained information throughout the years. Arad's family were kept informed throughout the process. Arad and his pilot evacuated their plane due to a technical malfunction during a mission to hit terror targets in the Lebanese city of Sidon as part of the First Lebanon War.

Bahrain security chief vows zero tolerance towards Ashura abuses

Gulf News, Habib Toumi, 2016 10 05

Manama - **Bahrain's Public Security has warned a zero-tolerance policy would be applied towards those who "misuse the religious occasion of Ashura to engage in criminal activity".** Ashura is the anniversary of the death of Imam Hussain, the grandson of Prophet Mohammad (PBUH), and the occasion is publicly commemorated by Shiites through emotional marches, rallies and speeches. Ashura commemorations will peak on the tenth of Muharram (October 12), and Public Security chief Tariq Al Hassan said that the police were coordinating with those in charge of the rituals to prevent the exploitation of the occasion and to ensure the safety of all participants.

Return to Table of Contents/ Retour à la table des matières

Asia / Asie

Spymaster Stanikzai calls for shifting military tactics

Pajhwok Afghan News, Khwaja Basir Ahmad Fitri, 2016 10 11

Kabul - The spymaster on Monday said Afghanistan has been a victim of war over foreign interests and due to its strategic location, asking the security forces to change their tactics. National Directorate of Security (NDS) chief Masoom Stanikzai called for a tactical shift while briefing the Wolesi Jirga, lower house of parliament, on the current security situation. Defence MinisterLt. Col. Abdullah Khan Habibi and Interior MinisterTaj Mohammad Jahidalso informed lawmakers on steps being taken to stabilize the security environment. “The current war here is

not a war of Afghans,; outsidersare interfering and supporting militants in Afghanistan," Stanikzai alleged, saying the conflict was driven by the interests of foreign countries. "Afghanistan is a victim of its strategic location; we should change our tactics," Stanikzai believed, stressing the need for unity. He asked the people yo support their security forces.

Pak ISI Director General likely to be replaced soon
Asian News International, 2016 10 08
Karachi - **Pakistan media has reported that Lt. General Rizwan Akhtar, the Director General of the Inter-Services Intelligence Directorate (ISI) is likely to be replaced within the next few weeks**. Lt. General Akhtar was appointed as the head of ISI in September 2014 and took office in November 2014. Quoting official sources, the Nation states that a security official privy to the development, confirmed the impending change of command and said that preparations were underway for the changes. However, he may be leaving the position earlier than the typical three-year tenure of a ISI DG. The report further states that the corps commander of Karachi, Lt General Naveed Mukhtar, is most likely to replace him.

Myanmar prepared for anti-terrorism attack: official
Xinhua News Agency, Staff reporter, 2016 10 07
Nay Pyi Taw - **Myanmar is prepared for possible anti-terrorism attack in the country, Deputy Minister of Home Affairs Maj-Gen Aung Soe told the parliament**, official media reported Friday. The readiness includes surveillance of suspected terrorists and specially-trained anti-terrorist combatants. Collaborating with local, regional and international organizations in fight against terrorism, Aung Soe said the government has been working to respond speedily to destructive elements by carrying tasks which include organizing operation missions, **deploying specially- trained anti-terrorism combat groups in Nay Pyi Taw, Yangon and Mandalay**, and guarding of dignitaries under a special security program. Besides, exchange and collection of terrorist attack information and linking with INTERPOL, ASEANAPOL, neighboring countries and allied organizations and other sources are to be carried out.

PM vows to bolster anti-terrorism capabilities
Yonhap News Agency, Staff reporter, 2016 10 06
Seoul - **Prime Minister Hwang Kyo-ahn said Thursday the country will focus its efforts to improve its anti-terrorism capabilities amid rising threats from extremist groups** around the globe. "International terrorists' groups, including the Islamic State of Iraq and the Levant (ISIL), have been conducting indiscriminate attacks on various locations like stadiums and streets to claim more lives," Hwang said.

Return to Table of Contents/ Retour à la table des matières

Africa / Afrique

Senate blocks move to summon SSS boss over raids on judges
The Premium Times, 2016 10 11
Abuja— The **Senate has stood down a proposal to invite the Director General of the State Security Service, Lawan Daura, over the ongoing clampdown on suspected corrupt judges**. In a motion brought as matter of urgent national importance by Joshua Lidani (PDP-Gombe), the Senate was asked to look into the action of the SSS which led to arrest of seven judges in the early hours of Saturday. One of the resolutions canvassed by Mr. Lidani was that

the Senate should invite Mr. Daura to explain why his agency carried out the action the way it did without deference to the constitutional responsibility of the National Judicial Council. When Mr. Saraki called for vote to uphold Mr. Lidani's prayer, Senators yelled "ayes" and later "nay" in somewhat equal proportion.

Nigerians object as judges detained, suspected of corruption
Associated Press, 2016 10 10
Abuja— **Nigeria's chief justice on Monday criticized the arrest of several senior judges in weekend sting operations that intelligence services said were part of a crackdown on corruption.** Officials announced that more than $800,000 had been seized in raids targeting judges from the country's high courts. The State Security Service said it had been monitoring the judges' "expensive and luxurious lifestyle" amid complaints they had accepted bribes. It did not specify how many judges were in custody. "It is indeed very saddening and deeply regrettable," Chief Justice Mahmud Mohammed said in brief comments to reporters Monday. He said an emergency meeting of the National Judicial Council would take place Tuesday to investigate the incident.

Spy agency acts against 'drug envoy'
The Sunday Times (South Africa), 2016 10 09
Johannesburgh— The **State Security Agency has revoked the security clearance of South African high commissioner to Singapore Hazel Francis Ngubeni**. The Sunday Times **exposed Ngubeni as a convicted drug trafficker** who had served time in a US prison. Ngubeni returned to South Africa on Monday and is facing an internal probe, which might end in her possible recall. She failed to declare her 1999 drug-trafficking conviction for smuggling cocaine into the US while working as a cabin crew member for SAA. Arthur Fraser, the director-general and accounting officer of the SSA, wrote to International Relations Minister Maite Nkoana-Mashabane on Friday informing her about the agency's decision to revoke Ngubeni's clearance.

Les «agents de la France» et les jeux de pouvoirs
El Watan, 2016 10 06
Alger— Après un silence qui aura duré plusieurs semaines, voire des mois, voilà que **Amar Saadani, secrétaire général du FLN, tire à boulets rouges sur ses détracteurs**. Il commence par **l'ancien patron du défunt Département du renseignement et de la sécurité (DRS), le général Toufik,** son ancien parrain. Celui auquel il doit sa promotion au sein du parti jusqu'à devenir président de l'APN et finir secrétaire général du vieux parti, est présenté comme «la tête des agents de la France» et, mieux encore, comme rédacteur de la lettre des 14 anciens cadres de l'ALN, demandant son départ de la direction du FLN.

Head of Central African Republic armed forces assassinated
Associated Press, Staff report, 2016 10 05
Bangui - The **head of Central African Republic's armed forces has been shot dead and his teenage son injured in an attack in the capital, Bangui**, a family member said. Marcel Mombeka was shot twice in his car in the PK5 neighborhood, said his sister Kevine Mombeka. The mostly Muslim enclave was visited by Pope Francis last year in an effort to urge calm in a country shaken by deadly violence between Christians and Muslims. "Shots rang out, creating panic among the population. I fled like everyone else," Kevine Mombeka said. "A young man then stopped me to say my older brother had been killed by Muslims." Marcel Mombaka's 14-year-old son, who was in the car, was shot and was being treated at a hospital, she said. She had been in the car as well but got out before the attack. The minister of public security, Jean Serge Bokassa, denounced what he called acts to destabilise the nation, warning "they will not

go unpunished". The United Nations peacekeeping mission condemned the attack, saying it would assist with investigations.

Return to Table of Contents/ Retour à la table des matières

Americas / Amériques

Report Finds Loose Laws on Data and Surveillance In Latin America

The Intercept, Cora Currier, 2016 10 10

Washington - The **laws in many Latin American countries haven't kept pace with the increasing power of surveillance technology, creating the potential for serious abuses**, according to a new report from a privacy watchdog. Despite recent revelations of widespread use of spyware capable of infiltrating phones and computers by many governments in the region-- including in some instances, against political opposition and journalists-- not a single Latin American country surveyed in the report has specific laws on the use of such invasive technology. Many countries, including Brazil, Colombia, Chile and Mexico, require companies to log detailed data on their customers and give law enforcement access to the information on demand. Colombia has a ban on encryption, and El Salvador requires communications providers to decrypt traffic at the government's demand. The report, written by researchers for the San Francisco-based Electronic Frontier Foundation, looked at surveillance laws in 12 countries in Central and South America. It opens with a stark reminder of what is at stake: A history of the collaboration among military dictatorships in Argentina, Chile, Paraguay, Bolivia, Uruguay and Brazil in the 1970s and 80s known as "Operation Condor." Files discovered later documented torture, disappearances, imprisonment and executions, enabled through a regime of informants and surveillance. **Many intelligence agencies in the region were formed under these military dictatorships,** and even after transitioning to democratic rule, most Latin American countries maintained strong executive branch powers "without well-placed controls or public oversight mechanisms." Given the power vested in many presidents in the region, the report says, "intelligence agencies in Latin America have been powerful tools in presidential politics, specially used to spy on dissident groups, opposition politicians or independent journalists."

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

12-10-2016 to/au 18-10-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Renewed Bill C-51 questions: Balancing national security with civil liberty
Globe and Mail Online, Kent Roach and Craig Forcese, 2016 10 18
Op-ed: The **police are presently intercepting private communications in search of speech that they think may promote "terrorism offences in general." That is the conclusion to be drawn from last week's government report on wiretaps authorized under Canada's criminal law**. To be sure, the report cites only two wiretaps seeking evidence of this new speech crime, introduced by **Bill C-51**. This may be because C-51 only came into force half way through 2015. But since the new speech crime is breathtaking in its scope, normalizing investigations of it would draw police into surveillance of an even broader range of speech. Such practices raise clear free speech and privacy concerns. There is also still the unanswered question about how the new speech crime will dovetail (or not) with the government's promised new program to counter violent extremism. An essential ingredient of any such program is speaking to those with extremist views, if only to dissuade. But if voicing views in the wrong place is a crime, those practising counter-extremism must worry that their efforts will become a stalking horse for a police investigation. And so the dilemmas raised by C- 51 remain: new powers with definite civil liberties costs incurred for doubtful security gains. **This is a recurring issue. CSIS has employed its new so-called threat-reduction powers about 24 times**, but we have no detail about what it has actually done.. **And while the Green Paper helpfully raises the issues of accountability neglected during the C-51 debates, its consideration of accountability gaps** – the need to fix the lack of expert, specialized review for most of Canada's security and intelligence sector – is perfunctory. It can also be criticized for a glaring omission: discussing revamped oversight for Canada's signals intelligence service, the **Communications Security Establishment**. Note: Kent Roach and Craig Forcese are professors of law at the University of Toronto and the University of Ottawa, respectively, and authors of False Security: The Radicalization of Canadian Anti-terrorism.

The mystery of the listening devices at DND's Nortel Campus
Ottawa Citizen Online, David Pugliese, 2016 10 18
Column: My colleague Jim Bagnall and I recently wrote a feature on **the move by the Department of National Defence to the former Nortel campus** in west end Ottawa. More than 8,000 military and civilian staff will make the move. **One of the issues that emerged when we were researching and writing the article had to do with the mystery of listening/spy devices that were planted at the Nortel Campus.** So what happened? Were listening devices found at the Nortel Campus or not? The Department of National Defence keeps changing its story on that issue. In 2013 the Citizen reported that workers preparing the former Nortel complex as the new home for the DND had discovered electronic eavesdropping devices. It shouldn't have come as a big surprise. The year before it had been revealed that Nortel was the target of industrial espionage for almost a decade, with the main culprits thought to be based in China. An internal security study by Nortel suggested that hackers had also been able to download research and development studies and business plans as far back as 2000. The hackers also placed spyware into some employee computers. **Michel Juneau-Katsuya, a former senior officer with the Canadian Security Intelligence Service, said the spy agency also determined that Nortel had been targeted.** "We knew it was well penetrated," he told the Citizen at the time. "When I was the Chief of Asia-Pacific we warned Nortel." But after the Citizen article was published, Julie Di Mambro, spokeswoman for then Conservative Defence Minister Rob Nicholson, noted in a statement that, "security officials have assured us that they

have not discovered any bugs or listening devices." Government documents, however, obtained by the Citizen through the Access to Information law, showed that the year before concerns had already been raised about security at the former Nortel campus.

Better to pass Bill C-22 now - and modify it later
Globe and Mail online, Reid Morden, 2016 10 13
Op-ed: On Oct. 7, The Globe and Mail weighed into the debate on **Bill C-22**, which proposes to establish a parliamentary committee on security and intelligence. Its editorial, citing a recent report by the Library of Parliament, points out some of the weaknesses of the bill and counsels, in a lukewarm fashion, patience and common sense. On Sept. 12, The Globe also published a **column by Ron Atkey, Craig Forcese and Kent Roach** on this important and controversial issue of accountability and oversight of Canada's security agencies. All three are eminent voices in the relatively new and evolving area of security law. The authors deal briefly but starkly with some of the controversial provisions in Bill C-51, passed by the previous government but focus mainly on what they perceive as the shortcomings of the proposed legislation of the current government as embodied in its Bill C-22. **There is much to agree with in their expressed views.** The authors draw critical attention to one of C-51's most egregious provisions, which permits the **Canadian Security Intelligence Service** to act in violation of the Charter of Rights and Freedoms. Check. They note the gaps in Canada's oversight system, especially the silos and stovepipes that inhibit a truly seamless oversight throughout our security agencies. Check. They judge that a parliamentary oversight body will be best suited to the examination systemic questions of whether Canada's security agencies are acting efficiently and effectively. Check. They are clear that no parliamentary oversight body can hope to function effectively without relying on expert review and complaints bodies to scrutinize the day to day operations of the security agencies. Check. Back to C-22: I do not sense any general resistance to the concept of parliamentary oversight by the security agencies. The **managements of organizations such as CSIS, the RCMP and the Communications Security Establishment have moved beyond that and today are primarily concerned with finding a model that will accommodate Parliament while not impairing their ability to carry out their responsibilities**. Finding the appropriate degree of intrusiveness is, in part, the nub of the problem. Note: Reid Morden is a former director of the Canadian Security Intelligence Service and a former deputy minister of foreign affairs.

RCMP block harassment claim
Ottawa Citizen, Andrew Seymour, 2016 10 13
Ottawa - It was a **dream come** true for **Caroline O'Farrell** to pull on the red serge and climb atop the majestic horses of the RCMP's Musical Ride. At 25 years old, the young Mountie couldn't believe she was going to be paid to ride in front of adoring crowds on the 100th anniversary of the RCMP's training depot in Regina, the Calgary Stampede and the Musical Ride's first performance in the Northwest Territories. Her face appeared on promotional posters for the RCMP's iconic travelling equestrian show. But the **dream quickly became a nightmare for O'Farrell, who alleges she was subjected to humiliating and demeaning hazing**, bullying and sexual abuse at the hands of her male colleagues in 1986 and 1987 as one of the first female members of the Ride. The abuse reached such heights that at one point her co-workers allegedly launched a suicide pool and took bets on when she would kill herself. Following last week's historic apology to all female members of the RCMP for decades of abuse and harassment and the announcement of a **$100-million settlement to right the wrongs suffered by women within the ranks of Canada's national police force**, O'Farrell is questioning why the RCMP and Canada's attorney general have blocked her own attempts to seek damages. O'Farrell launched a multimillion-dollar lawsuit in 2013, but after three years of motions by the government seeking to end her civil action, she feels revictimized.

Spy culture hasn't come home to roost
National Post, John Ivison, 2016 10 12
Column: **Remember how the Conservative antiterror legislation was going to usher in a new era of omnipresent government surveillance? Well, it hasn't happened** - at least not according to the scraps of information that are publicly available. The latest figures made available were on electronic surveillance, released by the **Department of Public Safety**. As part of the anti-terror bill, it became a crime to "knowingly" advocate or promote the commission of a terrorism offence. Critics claimed there would be a rash of wiretap authorizations, as police sought to crack down on speech crimes. But the **numbers for 2015 suggest there were precisely two cases where the authorities were given authorization to listen in on people suspected of promoting terrorism.** We don't know how many prosecutions resulted from the authorizations but it's a good bet there were none. For one thing, prosecutors would be aware that they would be guaranteed to face a constitutional challenge - many of the critics of Bill C-51 suggest that the definition of "the commission of terrorism offences in general" was too broad, and therefore unconstitutional. For another, the maximum penalty on conviction was five years in jail, hardly worth the effort for busy prosecutors. The speech-crime provision was not the only part of C-51 that constitutional scholars believed would never pass muster if challenged. **CSIS, Canada's spy agency, was given wide-ranging powers to disrupt suspected terrorist plots, rather than just gathering information about them.** The new law gave CSIS the power to ask judges to approve warrants, even if its preventive measures breached rights or freedoms otherwise protected by law. When he was before a Senate committee last March, CSIS chief **Michel Coulombe** said the agency had used the disruption powers nearly two dozen times but had not sought judicial approval in any of the cases.

Former CBSA boss lays out grievances at tribunal
Toronto Star, Alicja Siekierska, 2016 10 12
Toronto - The **former director of Canada's busiest immigration centre began testifying Tuesday as he pursues grievances against his former employer, the Canada Border Services Agency (CBSA). Reg Williams** was the director of immigration enforcement at the CBSA's Greater Toronto enforcement centre, the largest in the country, from 2004 until his retirement in May 2012. Williams said he retired after the CBSA abruptly reassigned him from his post in April 2012 because of an investigation into him at the time. Williams filed two grievances against the CBSA that are currently before the Public Service Labour Relations and Employment Board.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

Agencies Split on Classifying Clinton Emails
New York Times, Eric Lichtblau, Steven Lee Myers, 2016 10 18
Washington - **Documents released Monday in the Hillary Clinton email investigation show intense disagreement last year between the State Department and the F.B.I. over whether some of Mrs. Clinton's emails should be considered classified**, including a discussion of a possible "quid pro quo" to settle one dispute. The new batch of documents indicated that in one particular case, a senior State Department official, Patrick F. Kennedy, pressed the F.B.I. to agree that one of Mrs. Clinton's emails on the 2012 Benghazi attack would be unclassified -- and not classified as the bureau wanted. What remained unclear from the documents was

whether it was Mr. Kennedy or an F.B.I. official who purportedly offered the "quid pro quo": marking the email unclassified in exchange for the State Department's approving the posting of more F.B.I. agents to Iraq.

Official: you can still trust the NSA
FCW.com, Sean D. Carbery, 2016 10 18
Washington - It might not be as momentous as knocking down the Berlin Wall, but **tearing down the barriers between Signals Intelligence and Information Assurance inside the National Security Agency is revolutionary, an NSA official in the thick of those efforts contends**. The NSA is six weeks into "NSA21," which the agency calls the most substantial organizational reform in its 60-year history. Announced earlier this year, NSA21's primary change is flattening the organization and moving it from a mission-based construct to a functional model. **Curtis Dukes had been until recently the deputy director of NSA's Information Assurance directorate**. Now, he's deputy national manager of national security systems in charge of the IA portfolio of the new operations directorate. NSA's reputation in the information assurance business took a hit from leaks by former contractor Edward Snowden that included confirmation that an NSA-approved cryptographic algorithm was deliberately compromised. Still, Dukes said that there has been trust in the past, and that should continue under the new system.

Retired general pleads guilty to lying to the FBI in leak probe
Washington Post, Spencer S. Hsu, Ellen Nakashima, 2016 10 18
Washington - A **retired four-star Marine Corps general who served as the nation's second-ranking military officer pleaded guilty Monday to a federal felony charge of lying to the FBI** in a probe of a leak of classified information about a covert U.S.-Israeli cyberattack on Iran's nuclear program. **James E. "Hoss" Cartwright**, who served as deputy chairman of the Joint Chiefs of Staff before he retired in 2011, entered his plea before U.S. District Judge Richard J. Leon of Washington hours after the charge was announced by the office of U.S. Attorney Rod Rosenstein of Maryland. A senior Obama administration official in June 2013 acknowledged that Cartwright was the target of a Justice Department investigation into a leak to New York Times reporter David E. Sanger of details about a highly classified operation to hobble Iran's uranium-enrichment capability through cybersabotage - an effort not acknowledged by Israel or the United States. In court documents, **Cartwright admitted to falsely telling FBI investigators he did not provide or confirm classified information to Sanger for a June 2012 newspaper article and his book, "Confront and Conceal."**

Secret Law Is Bad Law
New York Times, Elizabeth Goitein, 2016 10 18
Op-ed - The Central Intelligence Agency's torture of detainees, and the National Security Agency's **warrantless wiretapping of Americans' international communications, were two of the most controversial programs our government implemented after Sept. 11. Both are now widely considered to have been illegal**, even though both were authorized by official legal analyses that were withheld from the public -- a phenomenon known as "secret law." The notion of secret law is as counterintuitive as it is unsettling. When most of us think of law, we think of statutes passed by Congress, and we take for granted that they are public. Statutes, however, are only one kind of law. When the secret surveillance panel known as the **Foreign Intelligence Surveillance Court, or FISA** court, construed the Patriot Act to allow bulk collection of Americans' phone records, that interpretation became part of the statute's meaning. When President Obama issued procedures and standards for using lethal force against suspected terrorists overseas, agency officials were bound to follow them. In the realm of national security, where Congress tends to tread lightly, other sources of law predominate -- and

a new study by the Brennan Center shows that they are frequently withheld from the public. Intelligence agencies routinely issue rules and regulations without publishing them in the Federal Register, exploiting what are intended to be narrow exceptions to the publication requirement. Most presidential directives addressing national security policy are not made public. Note: **Elizabeth Goitein co-directs the Brennan Center for Justice's Liberty and National Security Program and is author of the center's report "The New Era of Secret Law."**

Senate intel chair caught between Russian hacking and Donald Trump
Foreign Policy, Molly O'Toole, 2016 10 18
Hamlet, N.C. - When **Richard Burr**, the **Senate Intelligence Committee chairman**, is home in North Carolina, he's never more than a 90- minute drive from a secure phone line on which he can discuss secretive security issues facing the United States. But the tie that binds Burr to Washington is tripping him up in his tough re-election race this year. The senior senator is not only torn between Republican officials who want him constantly on the campaign trail and the very duties he's fighting to keep, but also Donald Trump, the GOP presidential nominee. Burr has maintained his support for Trump even as the increasingly erratic real-estate-magnate-turned-politician threatens down-ballot Republicans. **Burr has been careful to the point of reluctant to discuss the alleged Russian hacking -- a case of potential state espionage that falls squarely into his committee's oversight.** "I have yet to see anything that would lead me to believe that's the case," Burr told FP on Oct. 3, when asked whether he believes Russia has been interfering explicitly to benefit Trump. He called his congressional colleagues' warnings "probably incorrect," adding, "They give the impression there's one cyber-problem in the world: Russia and the elections, and that's a huge understatement." He said he couldn't speak to the DNC hack because the Obama administration hadn't yet declassified its findings.

Etats-Unis Relents de guerre froide dans le cyberespace
Le Monde, Martin Untersigner, 2016 10 17
Washington - **L'administration Obama vient d'incriminer officiellement la Russie dans la cyberattaque** qui avait ciblé, en juin, le Parti démocrate. Une accusation qui a encore envenimé les relations russo- américaines La Russie tente " d'interférer avec le processus électoral américain " . Vendredi 7 octobre, après maintes tergiversations, l'administration Obama a officiellement confirmé, par la voix de son directeur du **renseignement national (DNI) et de celle du département de la sécurité intérieure (DHS),** l'implication de Moscou dans l'attaque informatique visant le Parti démocrate. Cette accusation, au parfum de guerre froide et à un mois de l'élection présidentielle américaine, marque un tournant. Depuis des semaines, la Russie est suspectée d'orchestrer une série de piratages visant les Etats-Unis. Mais c'est la première fois que le gouvernement de Barack Obama incrimine directement Moscou dans " la récente compromission de courriels de citoyens et d'institutions américains, y compris d'organisations politiques " .

Slow implementation of insider threat programs not the cause of latest incident
Federal News Radio, Jason Miller, 2016 10 17
Washington - **Agencies continue to struggle to establish insider threat programs**. Many missed the deadline to hit initial operating capability in December 2015, and many still will miss the December 2016 deadline to hit full operational capability. The most recent data from the Obama administration on the Performance.gov portal doesn't provide specifics on how many or which agencies, but the **National Insider Threat Task Force (NITTF)** says a combination of "organizational culture, legal questions and resource identification" are among the obstacles preventing agencies from meeting the White House goal. The Coast Guard is one of the few agencies that met the full operational capability goal around insider threats. All of these delays

and challenges with creating an insider threat program would seemingly point to yet another reason why **Harold Thomas Martin III**, 51, of Glen Burnie, Maryland, allegedly was successful in taking classified materials from the National Security Agency over a two-year period. Experts, however, say the insider threat program is neither the problem nor the answer. Instead, experts say, reducing the risk of federal employees or contractors becoming threats goes back to security clearances. "To effectively counter the inside threat, we have to take advantage of the technology and implement the processes that continuously evaluate the behavior of employees to flag suspicious activities," said Larry Hanauer, vice president of policy for the **Intelligence National Security Alliance (INSA).**

Donald Trump stuns experts by refusing to accept intelligence on Russia
The Independent, Shehab Khan, 2016 10 16
Washington— A **former senior US national security official has said Donald Trump's refusal to accept information from intelligence professionals about Russia "defies logic".** US intelligence agencies claim Russia stole files from Democratic National Committee (DNC) computers in an attempt to influence the presidential election. Mr Trump received a classified briefing on the subject, where he was told intelligence officials were "confident" Moscow was responsible for the hack – something he has seemingly ignored. During the first presidential debate, Mr Trump asked if Russia was involved in the attack and in the second debate he questioned if there had been a hacking. "I don't think anybody knows it was Russia that broke into the DNC," he said in the first debate. "I mean, it could be Russia, but it could also be China. It could also be lots of other people. It also could be somebody sitting on their bed that weighs 400 pounds, okay?"**John MacLaughlin**, the **former acting CIA director**, said Mr Trump was using the information for his own benefit. "[Trump] is playing politics. He's trying to diminish the impression people have that [a Russian hack of the DNC] somehow helps his cause," Mr MacLaughlin said, according to Chicago Tribune.

CIA Prepping for Possible Cyber Strike Against Russia
NBC News, staff reporters, 2016 10 14
Washington— The **Obama administration is contemplating an unprecedented cyber covert action against Russia in retaliation for alleged Russian interference in the American presidential election,** U.S. intelligence officials told NBC News. Current and former officials with direct knowledge of the situation say the CIA has been asked to deliver options to the White House for a wide-ranging "clandestine" cyber operation designed to harass and "embarrass" the Kremlin leadership. The sources did not elaborate on the exact measures the CIA was considering, but said the agency had already begun opening cyber doors, selecting targets and making other preparations for an operation. Former intelligence officers told NBC News that the agency had gathered reams of documents that could expose unsavory tactics by Russian President Vladimir Putin. **Retired Admiral James Stavridis told NBC News' Cynthia McFadden that the U.S. should attack Russia's ability to censor its internal internet traffic and expose the financial dealings of Putin and his associates.** Two former CIA officers who worked on Russia told NBC News that there is a long history of the White House asking the CIA to come up with options for covert action against Russia, including cyber options — only to abandon the idea. "We've always hesitated to use a lot of stuff we've had, but that's a political decision," one former officer said. "If someone has decided, `We've had enough of the Russians,' there is a lot we can do. Step one is to remind them that two can play at this game and we have a lot of stuff. Step two, if you are looking to mess with their networks, we can do that, but then the issue becomes, they can do worse things to us in other places."

C.I.A. Director talks ISIL, next president and Augusta University's role in Cyber Security education
WJBF TV (Augusta Ga.), Stefany Bornman, 2016 10 14
Augusta, Ga. - The Director of the Central Intelligence Agency spoke at Augusta University's Cyber Summit. **John Brennan discussed ISIL, the upcoming change of presidential administration and Augusta University's role in educating the next generation of cyber warriors**. The C.I.A. Director says the future president has to hit the ground running on day one. The digital world is uncharted territory and presents daunting challenges for both the president and Central Intelligence Agency. "I must say ISIL is exceptionally sophisticated," he said. "Right now we are fighting against ISIL's External Operations efforts, that we've seen such horrific consequences, in places like Paris or Brussels."

FBI, DOJ roiled by Comey, Lynch decision to let Clinton slide by on emails, says insider
Fox News, Malia Zimmerman, Adam Housley, 2016 10 12
Washington - The **decision to let Hillary Clinton off the hook for mishandling classified information has roiled the FBI and Department of Justice, with one person closely involved in the year-long probe telling FoxNews.com that career agents and attorneys on the case unanimously believed the Democratic presidential nominee should have been charged**. The source, who spoke to FoxNews.com on the condition of anonymity, said FBI Director James Comey's dramatic July 5 announcement that he would not recommend to the Attorney General's office that the former secretary of state be charged left members of the investigative team dismayed and disgusted. More than 100 FBI agents and analysts worked around the clock with six attorneys from the **DOJ's National Security Division, Counter Espionage Section,** to investigate the case. "No trial level attorney agreed, no agent working the case agreed, with the decision not to prosecute -- it was a top-down decision," said the source, whose identity and role in the case has been verified by FoxNews.com.

NSA contractor thought to have taken classified material the old- fashioned way
Washington Post, Ellen Nakashima, Matt Zapotosky, 2016 10 12
Washington - **Harold T. Martin III is accused of stealing mounds of classified information from the government for at least a decade**, and investigators also believe some of the information was taken the old- fashioned way -- by walking out of the workplace with printed-out papers he had hidden, according to U.S. officials. The case against Martin, which was unsealed last week, raises new questions about whether the **National Security Agency** and other agencies are doing enough to detect and prevent their sensitive data from leaving the secure confines of government offices. While investigators believe much of Martin's material was removed before stringent controls were imposed in the wake of 2013 disclosures linked to former NSA contractor **Edward Snowden**, some feel the system still failed. When investigators searched Martin's home, they seized several terabytes of data, which Martin stored on dozens of computers and other devices, and thousands of pages of documents, according to the officials, who spoke on the condition of anonymity to discuss an open case. Investigators are still exploring whether he was connected in any way to the online leak of some of the NSA's most powerful hacking tools in August. "Someone was able to walk out the front door with a whole bunch of stuff from NSA," said one congressional aide. "That's not supposed to happen."

Russia May Be Hacking Us More, But China Is Hacking Us Much Less
NBC News, Ken Dilanian, 2016 10 12
New York - In a rare bit of good cyber security news, **Chinese hacking thefts of American corporate secrets have plummeted in the 13 months since China signed an agreement with the Obama administration to curb economic espionage,** U.S. officials and outside experts say. Analysts say the success may hold lessons for how the U.S. should deal with

Russia, which at the same time has stepped up a different sort of hacking campaign that officials says is aimed at undermining confidence in the American election. The change in China's behavior "has been the biggest success we've had in this arena in 30 years," said Dmitri Alperovitch, co-founder of Crowdstrike, a cyber security firm that tracks computer network intrusions. "And it wasn't anything we did in cyber space -- it was the threat of sanctions and the impact on their economy." Alperovitch said his firm has observed a 90 percent drop in commercial hacking against U.S. firms attributable to Chinese government actors. **U.S, intelligence agencies** also have reported a sharp falloff, according to officials briefed on the matter.

Security fears over FBI contracting out highly sensitive surveillance documents
The Guardian (London), Spencer Ackerman, 2016 10 12
New York - The **FBI has contracted out with a private firm to handle, distribute and monitor highly sensitive surveillance documents**, in an arrangement veteran FBI agents consider a potential privacy and counterintelligence risk. Since 2015, the FBI has entrusted a national- security professional services contractor, Aveshka, to prepare, organize, courier and disseminate surveillance materials, including documentation leading to court orders under the **Foreign Intelligence Surveillance Act (Fisa),** the legal wellspring of domestic national-security surveillance. Neither the company nor its employees have been accused of any wrongdoing, but national security has come under renewed scrutiny in the wake of the arrest last week of a Booz Allen Hamilton employee on suspicion of stealing **National Security Agency** computer code. FBI veterans and other surveillance experts consider the bureau to be effectively inserting a private firm as a middleman in surveillance, which they consider an inherent and seemingly unnecessary security vulnerability.

Democrats Say WikiLeaks Is a Russian Front; U.S. Intelligence Isn't So Sure
The Daily Beast, Nancy A. Youssef, Shane Harris, 2016 10 12
Washington - The **Hillary Clinton campaign and the Democratic National Committee are publicly accusing WikiLeaks of being a front for the Russian government** and an ally in efforts to help elect Donald Trump, but **U.S. intelligence officials aren't so sure.** On Monday, Clinton's spokesman called WikiLeaks "a propaganda arm" of the Kremlin and accused the site's founder, Julian Assange, of "colluding with [the] Russian government to help Trump" by leaking embarrassing emails taken from the Democratic National Committee and from the account of Clinton campaign chair **John Podesta**. "**Our Intelligence Community** has made it clear that the Russian government is responsible for the cyberattacks aimed at interfering with our election, and that WikiLeaks is part of that effort," **Donna Brazile** said in a statement. But four U**.S. military and intelligence officials** told The Daily Beast that the relationship between Russia and WikiLeaks is not so clear cut. Undoubtedly, the group has benefited from the work of Russian hackers, who passed purloined emails to WikiLeaks. But does that mean that WikiLeaks is taking orders from Vladimir Putin and doing his bidding? "For Russia, WikiLeaks is more like a useful idiot because they [the Russians] are too cowardly and dumb to be in on the master plan," one U.S. intelligence official told The Daily Beast, describing the website as essentially giving cover to Russian hackers.

U.S. Military Operations Are Biggest Motivation for Homegrown Terrorists, FBI Study Finds
The Intercept, Murtaza Hussain, Cora Currier, 2016 10 11
Washington - A **secret FBI study found that anger over U.S. military operations abroad was the most commonly cited motivation for individuals involved in cases of "homegrown" terrorism**. The report also identified no coherent pattern to "radicalization," concluding that it remained near impossible to predict future violent acts. The study, reviewed

by The Intercept, was conducted in 2012 by a unit in the **FBI's counterterrorism division** and surveyed intelligence analysts and FBI special agents across the United States who were responsible for nearly 200 cases, both open and closed, involving "homegrown violent extremists." The survey responses reinforced the FBI's conclusion that such individuals "frequently believe the U.S. military is committing atrocities in Muslim countries, thereby justifying their violent aspirations."

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

Boney M singer's brother who ran a mosque and had military-grade explosives and ammunition at his home 'had spurned MI5's advances'
Daily Mail (UK), Paddy Dinham, 2016 10 18
London - A **Boney M singer's brother who was found with half a pound of military-grade plastic explosives at his home near Wembley Stadium had spurned the advances of MI5**, he has told a court. Khalid Rashad, a Muslim convert and mosque director whose garage was also found to contain ammunition, was approached by the Security Service but refused to become a 'secret agent.' 'I don't think they were too happy with it,' he told the Old Bailey. 'I know many young men who frequented the centre and told me they had been approached and asked to spy within the organisation.'

The Snoopers' Charter 'should terrify us all' says former MP
International Business Times (UK), Jason Murdock, 2016 10 18
London - A **former MP who previously sat on the Home Affairs Select Committee has spoken out against the incoming Investigatory Powers Bill - called the Snoopers' Charter** by critics - which he brands a deeply intrusive piece of surveillance legislation "that should terrify all of us." **Dr Julian Huppert**, a lecturer at the University of Cambridge and former Liberal Democrat politician, claimed the bill has avoided any real public debate or scrutiny and slammed its proposals as a "real threat" to technology firms operating in the UK. "Some of the powers in the Bill are deeply intrusive, and with very little possible justification. All of us want to be safe, and protected from terrorists and the like - but the evidence that these powers are all needed is thin indeed. However, the cost to all of our privacy is huge," he wrote on OpenDemocracy. The **Investigatory Powers Bill (IPBill)** contains a number of proposals aimed at bulking up surveillance powers open to the **UK intelligence agencies MI5 and GCHQ,** while allegedly increasing the oversight regime available to the politicians at Whitehall.

UK security agencies unlawfully collected data for 17 years, court rules
The Guardian (London), Alan Travis, 2016 10 17
London - **British security agencies have secretly and unlawfully collected massive volumes of confidential personal data, including financial information, on citizens for more than a decade**, top judges have ruled. The investigatory powers tribunal, which is the only court that hears complaints against **MI5, MI6 and GCHQ**, said the security services operated secret regimes to collect vast amounts of personal communications data, tracking individual phone and web use and large datasets of confidential personal information, without adequate safeguards or supervision for more than 10 years. The ruling said the regime governing the collection of bulk communications data (BCD) - the who, where, when and what of personal phone and web communications - failed to comply with article 8 protecting the right

to privacy of the European convention of human rights (ECHR) between 1998, when it started, and 4 November 2015, when it was made public. It said the holding of bulk personal datasets (BPD) - which might include medical and tax records, individual biographical details, commercial and financial activities, communications and travel data - also failed to comply with article 8 for the decade it was in operation until its public avowal in March 2015.

GCHQ branded as "barbaric" by Oscar-winning director Oliver Stone at Cheltenham Literature Festival
Cheltenham Echo, Phil Norris, 2016 10 17
Cheltenham - Oscar-winning director **Oliver Stone launched an extraordinary attack on GCHQ while appearing at the Cheltenham Literature Festival** tonight. The JFK, Platoon and Wall Street director was speaking in the Town Hall to promote a book, The Oliver Stone Experience, about his many award-winning movies. And after a bit of joking along the lines of **'GCHQ is listening'** from host Mark Lawson, Stone said: "GCHQ is one of the most barbaric agencies around, very cold, very smart. "And likely to arrest anybody at any time, on any thing on any cause. So hello!" There was laughter at the time, but Stone was later questioned about his use of the word "barbaric" from the floor during the question and answer section. When challenged, Stone appeared to not understand and asked in what context he had described GCHQ as barbaric.

Chinese link as smart meters spook GCHQ
Sunday Times (UK), Jon Ungoed-Thomas, 2016 10 16
London - **Chinese electronic companies are manufacturing smart meters to install in millions of Britain's homes despite warnings by the intelligence agency GCHQ** that the technology poses a potential threat to national security. Two of China's biggest electronics companies -- one controlled by the Beijing government -- are providing some of the meters and software for the £11bn programme to install the technology in almost every home in the UK by 2020. One has already signed a deal with one of the "big six" energy companies and the other has been on an official list for trials. The vetting of the Chinese manufacturers is set to be among the first tasks of the **National Cyber Security Centre** (NCSC), which opened in London earlier this month. Nigel Inkster, a former director of operations and intelligence at MI6, said it was important the role of any Chinese firm was subject to a proper risk assessment. "A Chinese corporation is always going to have to do what the state tells it when the crunch comes, although these corporations really do want to be proper international corporations and operate on this basis," he said. Experts have expressed concern that the meters -- which communicate wirelessly with energy companies -- feature a switch that can be used to remotely turn off power, potentially blacking out homes and risking dangerous electricity surges at power stations.

'We don't do it for medals or glory': MI5 agent who helped foil Arndale bomb plot on risking life every day to protect us
The Mirror UK, 2016 10 15
London - A **former MI5 agent who helped foil a plot to blow up Manchester's Arndale Centre has revealed how he was paid just £30,000-a-year over a decade of risking his life to save ours**. "I realise now it's not a lot of money. It was never about the money for us. It's just about dealing with it," **Tom Marcus** matter-of-factly told the M.E.N. during a revealing interview about the ups and downs of life as a secret agent. Considered too bolshy while in the Army, his boss 'volunteered' him for MI5 where he started on £26,500-a-year, rising to a touch over £30,000 by the time he left ten years later after being struck down by Post Traumatic Stress Disorder (PTSD). The former officer spoke frankly about his remarkable life as an MI5 agent during an enthralling hour-long interview with the M.E.N. at a secret Manchester location. Tom,

from the north, spoke candidly about what it was like to risk his life on a daily basis, although he took care not to avoid incidents not covered in his book **'Soldier Spy'**, each line of which was okayed by the secret services prior to publication last week. The book covers how he helped the security services foil the 2009 Al Qaeda plot to blow up Manchester's Arndale Centre and how he stopped another outrage when terrorists planned to kill 60 London schoolkids by detonating a pipe-bomb. Tom revealed he worked an average 80 or 90 hours each week, and sometimes 18 in a day, during more than a decade with MI5.

Man who rejected MI5 convicted of terror charge after semi-secret trial
The Guardian (London), Owen Bowcott, 2016 10 13
London - A **Somali-born man who spurned MI5 efforts to recruit him as an informant has been found guilty - following a partially secret trial - of preparing to join Islamic State fighters in Syria.** Anas Abdalla was discovered hiding behind canisters in the back of a lorry in Dover as he tried to smuggle himself out of the UK in April 2015. He claimed he was escaping from years of harassment by anti-terrorism officers. His final movements had been closely tracked by an undercover "law enforcement" agent. It is the fourth time the former computer technology student, who holds British citizenship, has been put on trial for the same terrorist offence at the Old Bailey on London. He was convicted after the prosecution shifted from its previous position of neither confirming nor denying (NCND) Abdalla's allegations of "oppressive treatment" by the security service. In order to contest details of Abdalla's dealings with MI5, evidence was given in secret by counter-terrorism officers.

UK to have rapid armed police unit to respond to terror attacks
Financial Times, Helen Warrell, 2016 10 12
London - **Downing Street is planning to establish the UK's first national armed police unit for rapid deployment in the event of a Paris- style terror attack**. The proposal, currently under review by police chiefs, would combine firearms officers from the British Transport Police, the Civil Nuclear Constabulary and the Ministry of Defence Police to create a 4,000- strong armed force under one central command. The **new unit, known as the Armed Infrastructure Constabulary, is expected to be a highly-mobile team** with unified systems and communications. Its brief would be to protect national infrastructure as well as responding quickly to marauding attacks such as the recent terror incidents in Paris, Nice and Munich. To broaden its reach, the force would seek strong links with European partners at the Channel tunnel and ports around the country.

World faces cold-war-era threat levels, says former MI6 chief
The Guardian (London), Patrick Wintour, 2016 10 12
London - The **world faces cold-war-era threat levels, Sir John Sawers, the former head of MI6, has said**, due to the west vacating the stage in Syria and failing to recognise that the growth of Russian military power over the past 15 years required the development of a new strategic relationship with Moscow. "We are moving into an era that is as dangerous, if not more dangerous, as the cold war because we do not have that focus on a strategic relationship between Moscow and Washington," Sawers told the BBC on Wednesday. He said the west needed to recognise that the balance of power had changed in the world because of an increase in Russian military power, and its willingness to use that power. "We are not treating Russia and China as major powers that can cause us a great deal of damage," he said.

Return to Table of Contents/ Retour à la table des matières

Australia / Australie

Cabinet has 'never' disclosed sensitive material on WhatsApp
Sydney Morning Herald, James Massola, 2016 10 18
Sydney -**Attorney-General George Brandis says confidential material has "never, ever" been communicated by cabinet ministers on WhatsApp** - but he won't be releasing the proof. And testy officials from the Department of Prime Minister and Cabinet dismissed security experts' concerns about the use of WhatsApp, insisting that the security clearances given to ministers and their staff were sufficient to protect sensitive information. Those officials said that to the best of their knowledge, **Defence's cyber security agency, the Australian Signals Directorate, had not approved the use of WhatsApp for classified or sensitive communications**. Fairfax Media reported last week that cabinet ministers, MPs, ministerial chiefs of staff and media advisers are using WhatsApp to hold confidential discussions about government business. That prompted Labor's legal affairs spokesman, Mark Dreyfus, to warn the arrangement was a "national security risk". But Senator Brandis told a Senate hearing yesterday that using the app did not pose a security threat. "I can assure you, having communicated with the Prime Minister and other cabinet colleagues on WhatsApp, there has never been an occasion, ever, in which the material on WhatsApp has been other than extremely routine, of an extremely routine nature," he said.

Terror laws to be tested in court
Australian Associated Press, Belinda Merhab, 2016 10 17
Canberra--**Pauline Hanson wants laws stripping dual-national terrorists of their citizenship to go further, calling for their families to be deported as well**. A dual-national terrorist is set to become the first to be stripped of citizenship after the controversial laws cleared federal parliament last year but an immediate High Court challenge is expected, News Corp Australia reported on Monday. The One Nation leader says the immediate family of anyone stripped of their citizenship should be deported as well. "It has to be a real deterrent to get these people out of the country," she told the Seven Network.

Labor queries Brandis over intel committee
Australian Associated Press, Paul Osborne, 2016 10 15
Canberra - **Labor has accused the attorney-general of misleading the parliament's intelligence and security committee over controversial 2015 laws stripping terror suspects of Australian citizenship**. Shadow attorney- general Mark Dreyfus said Attorney-General George Brandis had told the committee he had received advice from Solicitor-General Justin Gleeson that the laws would survive a High Court challenge. But Mr Gleeson told a Senate committee on Friday he had only provided advice on an earlier draft of the laws and not the final bill introduced to parliament by Immigration Minister Peter Dutton in June last year. "My concern in relation to the citizenship bill was that I had provided a lengthy advice in respect to that proposal in 2014 and apparently ... in the first half of 2015 a substantial change was made to that proposal," Mr Gleeson said.

ASIO boss fears wave of attacks too big to stop
The Australian, Brendan Nicholson, 2016 10 14
Canberra - The **scale of the terrorist threat faced by Australia is such that ASIO cannot guarantee it will uncover and prevent attacks, the key counter-terrorism agency has warned. ASIO director-general Duncan Lewis has warned** in his annual report that he fears his staff will be singled out for terrorist attacks. "It is an unfortunate reality that the changes to the security environment have resulted in an increased threat to the personal safety of ASIO

staff," he said. "My officers are operating in an environment that puts their personal safety at risk from spontaneous or opportunistic attack using readily acquired weapons and relatively simple tactics. "In today's environment, regardless of resourcing and expertise, we cannot provide complete assurance that all terrorist attacks or high harm espionage activities affecting Australia and Australians will be identified and prevented." Mr Lewis said the principal threat came from a small number of individuals in Australia who remained committed to anti-Western, violent and extremist Sunni Islamist ideology.

PM's 'favourite thing': WhatsApp chat raises security fears
Sydney Morning Herald, James Massola, 2016 10 13
Sydney - **Prime Minister Malcolm Turnbull and his most senior cabinet ministers are using a third-party messaging application to conduct confidential discussions**, prompting cyber security experts to warn the innovation could actually pose a security risk. The use of WhatsApp is not limited to senior ministers; private chat "groups" exist for government chiefs of staff, ministerial media advisers, the frontline economic team, and a defence-focused "broadcast group" used by Defence Industry Minister Christopher Pyne to communicate with MPs and staff. Fairfax Media has spoken with four cyber security experts who have each flagged potential security issues with the widespread use of WhatsApp by the Turnbull government - particularly at a cabinet level - in place of secure, government email servers from platforms approved by the **Australian Signals Directorate (ASD),** Australia's cyber intelligence agency. Craig Searle, the founder of security consultancy firm Hivint, pointed out WhatsApp was not an approved platform on the ASD list of Evaluated Products or Certified Cloud Services, whereas Apple's iOS operating system and Blackberry's operating system were.

The bungling spies like us
Adelaide Advertiser, Peter Jean, 2016 10 13
Unknown placeline - **Spy agency ASIO tapped the wrong phone by mistake, illegally hacked a computer and had to pay for professional carpet cleaning in a home its agents raided**. And its sister intelligence agency the **Australian Secret Intelligence Service** passed information about Australians to a "foreign liaison" without applying privacy rules. A series of stuff-ups by **Australia's intelligence organisations** have been made public in Inspector-General of Intelligence and Security's Margaret Stone's annual report. Most were reported to Ms Stone's office by the agencies themselves after they realised they had made mistakes. The report reveals ASIO tapped the wrong phone because it had an "incorrect number" and a telco mistakenly sent the agency wrongly intercepted SMS messages. An "administrative "oversight" also led to a computer being accessed without a warrant from the Attorney-General. And a woman whose home was raided **by ASIO agents** executing a search warrant complained to the Inspector-General that the property had been left in a "disordered state" at the end of the search.

Aust authorities warn on cyber security
Australian Associated Press, Roje Adaimy, 2016 10 12
Canberra - The **Australian government warns the prospect of terrorists launching a significant cyber attack on one of its secure networks is real and serious**. A new report by the **Australian Cyber Security Centre** ranks the current threat level as low, with terrorist groups more likely to embarrass governments and exploit the internet for propaganda purposes. But it predicts that within three years, they could have the ability to compromise a secure network with "disruptive and destructive effect". "Of course they're developing their wherewithal when it comes to this area and they're looking to see 'ok, can we use cyber as an offensive weapon?'," Dan Tehan, the minister assisting the prime minister for cyber security, said. "The

real danger is if they're able to recruit and get the right people, then they will be able to use cyber as an offensive weapon and that's what we've got to be aware of."

Bureau of Meteorology hacked by foreign spies in massive malware attack, report shows
ABC (Australia), Andrew Greene, 2016 10 12
Canberra - A **foreign power managed to install malicious software - - known as malware -- on the Australian Bureau of Meteorology's computer system** to steal sensitive documents and compromise other government networks, an official cyber security report has revealed. The **2016 Australian Cyber Security Centre Threat report**, to be released today, provides new details on , which also breached sensitive systems across the Federal Government. It is not known what the motivation for the attack was, but experts have suggested it could be commercial, strategic or both. The bureau is considered a critical national resource, and another state would place a high value on its intellectual property and scientific research. According to the **Australian Cyber Security Centre (ACSC)** report, the **Australian Signals Directorate (ASD)** last year detected suspicious activity from two computers on the bureau's network. "On investigation, ASD identified the presence of particular Remote Access Tool (RAT) malware popular with state-sponsored cyber adversaries, amongst other malware associated with cybercrime," the report stated.

Foreign spies hacked Australian agency, report says
Agence France-Presse, Staff reporter, 2016 10 12
Sydney - **Foreign spies installed malicious software on an Australian government agency's computer system, stealing an unknown number of documents,** an official report revealed Wednesday, stopping short of naming the country involved. The security breach on the Bureau of Meteorology's system, which has connections to the defence department, was detected in 2015 and initial media reports linked it to China. China has previously been accused of hacking websites run by the US government and by private firms. In 2013 Chinese hackers were accused of stealing the top- secret blueprints of Australia's new intelligence agency headquarters. The government's **Australian Cyber Security Centre** report released Wednesday attributed "the primary compromise to a foreign intelligence service" but did not name any country as responsible. "We don't narrow it down to specific countries, and we do that deliberately," said **Dan Tehan, who assists Prime Minister Malcolm Turnbull on cyber security.**

Threat of cyber terror closes in
The Australian, Cameron Stewart, 2016 10 12
Sydney - Terrorists could be able to break into secure Australian government networks to wreak significant disruption or destruction within three years, according to a major government report on cyber security. The wide-ranging report identifies foreign powers as the most serious and rising threat to the security of government networks, which suffered 1095 serious cyber assaults from all sources, including foreign espionage, in the 18 months to June 30 this year. The 2016 Threat Report -- to be released today by the government's peak cyber agency, the Australian Cyber Security Centre -- highlights the growing prevalence and threat of cyber assaults across government, business and society. It warns that the danger of a single major cyber attack on the government has increased after a recent series of brazen attacks against other countries and major organisations. The report comes as Russia and China step up their cyber assaults and espionage against the West, such as Russia's recent hacking of the US Democratic National Committee and the World Anti-Doping Association. "Behaviour by a number of countries is demonstrating a willingness to use disruptive and destructive cyber operations to seriously impede or embarrass organisations and governments -- equating to foreign interference or coercion," it says. "The employment of the tactic in such a brazen manner against high-profile

entities has almost certainly lowered the threshold of adversaries seeking to conduct such acts." The report says the cyber threat to Australia from terrorists is currently limited to the ability to hack websites, social media and personal information, but this will change as they develop more sophisticated cyber-terror capabilities.

Return to Table of Contents/ Retour à la table des matières

New Zealand / Nouvelle-Zélande

Foreign spies hack NZ phones, laptops

New Zealand Herald, Matt Nippert, 2016 10 15
Wellington - **New Zealand government officials travelling abroad had their mobile phones and laptops containing classified information hacked by foreign agents** after their hotel room safe was broken into, government **cyber security officials** have revealed. According to an account of the incident prepared by the Government that does not name either the department involved nor the foreign power believed responsible, the incident occurred when two trade negotiators attended an overseas conference. Precautionary efforts by the pair to delete sensitive materials from their devices prior to departure proved ineffective in protecting classified information. A cloned copy of hard drives allowed foreign agents to "recover not only deleted protectively marked documents, but also intellectual property and sensitive information pertaining to trade negotiations", according to the account. Following their return to New Zealand, malware designed to log all electronic activity was also found to have been installed on the devices. **Paul Ash, director of the national cyber policy office at the Department of Prime Minister and Cabinet**, said the incident showed New Zealand's geographic isolation was no firewall.

Public hearings are starting today on the new law to govern New Zealand's two spy agencies.

Radio New Zealand News, Staff reporter, 2016 10 13
Wellington - **Parliament's Foreign Affairs, Defence and Trade committee will hear submissions on the legislation establishing a fresh set of rules for the Government Communications Security Bureau and the Security Intelligence Service**. The legislation removes the restriction on the **GCSB** intercepting New Zealanders' communications. But that would have to be signed off by the Attorney General, the Commissioner of Warrants, and could only be for the purposes of 'national security', as defined in the bill. The legislation creates a two tier system for all of the agencies' activities, and requires them to follow the same warranting and compliance regime. (Full report)

Return to Table of Contents/ Retour à la table des matières

International

China / Chine

Ban on spreading extremism among children in line with law: experts

Global Times, Yang Sheng, 2016 10 13

Beijing - A **new regulation, which encourages people to call the police if they find parents or guardians organizing, luring or forcing their children into religious activities** is in accordance with the country's law on religious freedom, experts said on Wednesday. The regulation, released by the **Xinjiang Uyghur Autonomous Region** on Wednesday and to be effective on November 1, says that parents and guardians should neither promote extremist beliefs in children, nor force them to wear extremist clothing and symbols. "Any group or individuals have the right to stop such behavior and report them to the public security authorities," Article 9 reads. The regulation also bans any form of religious activities in schools. Article 16 stipulates that schools must guide students away from separatism, terrorism and extremism, to create a healthy environment that "respects science, refuses ignorance and opposes superstition." Xi Wuyi, an expert on Marxism and religious studies at the **Chinese Academy of Social Sciences,** told the Global Times that this regulation conforms to the Constitution which protects the freedom of religion, because separation of education and religion is a key principle of China's education and religious activities.

Return to Table of Contents/ Retour à la table des matières

Russia / Russie

Putin confidant denies plans for new KGB in interview

DPA News Agency, 2016 10 18

Moscow— The **KGB secret service is not being revived in Russia, former Kremlin chief of staff Sergey Ivanov said** in an interview published Tuesday. Ivanov, a close confidant of Russian President **Vladimir Putin,** said reports that a new ministry of state security was being set up along the lines of the much-feared Soviet-era body were false. Different bodies would continue to work separately on investigations, counter-espionage and security, Ivanov told Komsomolskaya Pravda daily. "I don't see any sense in having a super ministry," said Ivanov, who in August switched portfolios to transport and the environment after working for four years as chief of staff of the presidential administration.

Kremlin Has No Plans to Create More Security Agencies

Sputnik News Service, 2016 10 17

Moscow—Media reported in September that the government planned to **create a State Security Ministry based on the Federal Security Service (FSB)**, the main security agency. The new ministry would reportedly take over inquiries into high-profile criminal cases and act as an internal oversight body. "It is a one-hundred-percent fake! There is no state security ministry under consideration and never will be, I assure you," Ivanov told the Russian Komsomolskaya Pravda online newspaper. **"There are enough security agencies." According to reports, an alleged reshuffle of security and law enforcement agencies was to be completed by the time of the next presidential elections in March 2018**. It would also merge the service protecting the president and high-level state officials with the intelligence agency, which Ivanov said did not have any sense.

Putin to Kremlin journalists: US is watching you

Associated Press, 2016 10 16

Moscow - **Russian President Vladimir Putin has told journalists in the Russian press corps that they are possibly being watched by American intelligence agencies**. Putin made the comments Sunday in Benaulim, India, where he was attending the summit of the BRICS group of emerging economies. Putin told journalists covering his visit that ``the United

States listens to everything and looks at everything. All of you are objects of exploitation for the special services."

Russian Spycraft: How the Kremlin Hacked Its Way Into a Crisis
Moscow Times, Vladimir Frolov, 2016 10 11
Column - Last Friday the U**.S. Intelligence Community (USIC) publicly named the Russian government for directing "the recent compromises of emails from U.S. persons and institutions, including from U.S. political organizations."** It claimed that the disclosures of hacked emails "on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are intended to interfere with the U.S. election process", while "only Russia's most senior officials could have authorized these activities." President Vladimir Putin in a recent interview to Bloomberg denied that Russia on a state level had anything to do with the email hacks, but his claim that "the important thing is the content that was given to the public, and not the search for who did it" suggested more than a cursory knowledge of the matter. His further claim that the Russian government did not possess the kind of sophisticated sense of U.S. domestic politics to pull off such a tricky game sounded lame. The **Russian Foreign Ministry** maintains a granular understanding of the intricate details of U.S. presidential and party politics. The Russian Embassy in Washington keeps about a dozen diplomats on the beat. It is not, as some claim, that the Russians suddenly discovered the DNC last year. While the publicly available evidence linking Russian intelligence to the hacks is inconclusive and may even suggest a false flag operation to entangle Moscow in a brawl with Washington, **the U.S. Intelligence Community** had a high degree of confidence in Russian involvement even in July and the fact that they publicly named Russian intelligence as perpetrators suggests that they have definitive proof.

Return to Table of Contents/ Retour à la table des matières

Europe

Les espions, au service du pays
L'Est Républicain, 2016 10 17
Paris—**James Bond, OSS 117, Kim Philby, George Blake, Jeanne Bohec… Qu'ils soient de fiction ou bien réels, les agents secrets renvoient souvent une image de surhomme**. «Un espion est un homme ou une femme qui travaille dans un service, pour un pays et ses intérêts, sa population», explique Emmanuel Ranvoisy, l'un des commissaires de l'exposition **«Guerres secrètes», au Musée de l'armée, à Paris**, qui retrace l'histoire de l'espionnage pendant les grands conflits du Second Empire jusqu'à la guerre froide. Le travail des agents se révèle primordial durant les guerres ouvertes (Première et Seconde guerres mondiales), mais aussi pendant les guerres fermées (guerre froide). «L'action des espions est un moyen vital pour assurer la sûreté du système de défense et l'expression de la stratégie d'un pays et la souveraineté de l'État», précise Emmanuel Ranvoisy. «Les agents travaillent au plus proche du pouvoir, de la haute administration.

François Hollande révèle avoir ordonné l'exécution d'au moins quatre terroristes par la DGSE, tout en dévoilant des conversations qui mettent le Grec Tsipras en difficulté
L'Opinion, Jean-Dominique Merchet, 2016 10 17
Paris— Soixante-dix pages du livre «Un président ne devrait pas dire ça» de Gérard Davet et Fabrice Lhomme (Stock) sont consacrées à la diplomatie et au renseignement. Elles aussi contiennent quelques bombes à retardement...**Avec François Hollande, pas besoin de WikiLeaks ! Il raconte lui-même, avec une légèreté confondante, ce qui en principe devait**

rester secret... Sur l'international, la lecture du livre de Gérard Davet et Fabrice Lhomme contient son lot de révélations, principalement dans deux domaines : l'action des services secrets français et la crise grecque. « J'en ai décidé quatre au moins », répond le chef de l'État alors que les deux journalistes l'interrogent, le 9 octobre 2015, sur le nombre d'opérations « Homo », c'est-à-dire d'assassinats ciblés confiés au **Service Action de la DGSE**. « D'autres présidents en ont fait davantage » ajoute-t-il, comme pour se justifier. Un mois plus tard, il semble revenir sur ces propos, estimant que tout cela est « totalement fantasmé ». Mais, l'année précédente, le 7 mars 2014, n'avait-il pas montré aux journalistes une liste de dix-sept responsables terroristes à « neutraliser » ? Toutes ses informations sont évidemment couvertes par le secret de la défense nationale et leur divulgation relève du Code pénal. N'importe quel fonctionnaire ou militaire qui livrerait de telles informations s'attirerait de sérieux problèmes. À l'Élysée, on est visiblement au-dessus de cela. Toujours dans le domaine du renseignement, le chef de l'État indique qu'il souhaitait « écarter » le patron de la DGSE, Erard Corbin de Mangoux, nommé par Nicolas Sarkozy, parce qu'il « retenait des informations », mais que la guerre du Mali a retardé cette décision. **Revenant sur l'échec, en 2013, de la libération de Denis Allex, un agent de la DGSE retenu en otage en Somalie**, le président de la République confirme les récits qui avaient alors filtré. Le chef de l'État fournit des informations sur l'identité de Denis Allex, jusqu'alors soigneusement préservée par la DGSE.

A Terrorist, Three Heroes and a Bumbling Judiciary
Spiegel Online, 2016 10 14
Berlin—**Jaber al-Bakr was allegedly planning a terrorist attack in Berlin**. But then he was captured, tied up and turned into the police by three Syrian refugees. SPIEGEL spoke with the trio and with al-Bakr's brother to learn more about the case -- one which ended with al-Bakr's suicide and questions about the German judiciary. At the end of each week, Hans-Georg Maassen, the president of **Germany's Federal Office for the Protection of the Constitution (BfV), receives several rolls of paper from his staff.** They look not unlike rolls of wallpaper -- and are full of tables with information about the domestic intelligence agency's current investigations. Changes from the previous week are color-coded to make it easier to see how operations are progressing. The multitude of colorful blotches indicates how seriously the agency takes signs of possible terror attacks in Germany. Last week, a case depicted on Maassen's tables suddenly triggered extreme concern. A tip received from American intelligence agencies led German officials to Jaber al-Bakr, a Syrian citizen born on Jan. 10, 1994 in Saasaa, a town near Damascus. He was thought to be living at Usti nad Labem Street 97 in Chemnitz, though that wasn't his officially registered place of residence. And there were indications that he was planning a bomb attack on an airport in Berlin, perhaps in just a few days.

Sur la piste du magot des services secrets
Le Parisien, Éric Pelletier, 2016 10 13
Paris—Á la Piscine, **le siège des services secrets français (DGSE), on attend avec un brin d'appréhension le 18 octobre, date à laquelle tombera la décision du tribunal de commerce de Paris.** Rien à voir avec une affaire d'otages ou un risque d'attentat. **Au cœur du litige : de (très) gros sous, en l'occurrence le reliquat du patrimoine amassé à l'étranger par des générations d'espions français.** Une cagnotte destinée à « assurer la continuité de l'Etat » en cas de coup dur. Les agents récupèreront-ils leur mise de départ, estimée à plus de 25 M€, ou vont-ils tout perdre ? Quitte ou double. C'est l'enjeu de cette procédure qui ferait passer un roman de John Le Carré pour une bluette. Pour se garantir en cas d'invasion du territoire, que l'ennemi soit prussien, allemand ou soviétique, les gouvernements successifs ont confié au service de renseignement extérieur la gestion d'un trésor de guerre à l'étranger. En

1995, pour faire fructifier ces sommes, la **DGSE** place une partie de cet argent dans plusieurs sociétés, notamment au Luxembourg.

Denmark unveils new anti-radicalization measures
The Local (Denmark), Staff report, 2016 10 12
Copenhagen - The **Danish government on Tuesday presented a list of measures to combat radicalization,** including a "corps of digital voices of reason" to challenge extremist views on the internet. Part of the new plan was for the **Danish Security and Intelligence Service (PET)** to form a "national alliance against online radicalization" including authorities and people from civil society, to which the new "voices of reason" project would be linked. "A civil society-driven corps of digital voices of reason will be established," the Ministry of Justice said in a presentation of the anti- radicalization plans. The group would "systematically be present in social media and engage critically in relevant forums, take part in dialogue and challenge extremist views," it said. A **new unit would also be formed within PET to identify and remove extremist material from the internet.**

Scandinavian Security Forces Step Up Surveillance
Sputnik News Service, 2016 10 14
Helsinki—A **Finnish working group has proposed amendments to the Constitution in order to drastically widen the scope of Finland's Security Intelligence Service (Supo)**. Accordingly, Supo's intelligence-gathering power is to be expanded both domestically and abroad. At present, Supo is already authorized to track people, tap phones and monitor other communications on suspicions of terrorism, espionage and treason. According to the suggestions by the civilian working group, Supo should be granted the right to conduct intelligence without requiring any suspicion of crime. Accordingly, Supo will be allowed to secretly intervene in citizens' post and communications to obtain information about clandestine military activities or anything that "seriously threatens public safety." According to Finnish daily Helsingin Sanomat, the proposal marks a departure from Supo's traditional role of revealing, preventing and investigating crime to the proactive collecting of intelligence about potential national security risks.

La menace "prise au sérieux" par le Renseignement
Valeurs Actuelles, Louis de Raguenel, 2016 10 13
Paris - « Nous sommes au bord de la guerre civile. » Mais qu'a bien voulu dire **Patrick Calvar, le patron de la DGSI, lors de son audition à huis clos le 24 mai dernier par la commission d'enquête parlementaire sur les attentats du 13 novembre ?** Ce n'est pas la première fois que ce Breton, qui n'a jamais accordé d'interviews depuis sa nomination à la tête du Renseignement intérieur, tient des propos qui détonnent. Déjà le 10 mai 2016, devant la commission de la défense nationale et des forces armées, sa parole heurte. Attendu pour disserter sur la lutte contre le terrorisme islamique, il retourne son auditoire et prévient : « L'Europe est en grand danger. » Explication : « Les extrémismes montent partout et nous sommes [...] en train de déplacer des ressources pour nous intéresser à l'ultradroite qui n'attend que la confrontation. » Sans langue de bois, il conclut : « Vous vous rappeliez que je tenais toujours un langage direct; eh bien, cette confrontation, je pense qu'elle va avoir lieu. » Les députés qui écoutent le patron du Renseignement intérieur sont stupéfaits. Quand ? Qui ? Où ? Pas le temps de respirer. Avec sang-froid, Calvar donne le coup de grâce : « Encore un ou deux attentats et elle adviendra. »

Les secrets bien gardés des espions dévoilés dans une exposition à Paris
Agence France-Presse, Journaliste maison, 2016 10 12
Paris - Du parapluie bulgare empoisonné à la célèbre machine à chiffrer allemande Enigma, **400 objets et documents d'archives, rassemblés pour la première fois lors d'une**

exposition à Paris dessinent à petites touches l'univers très secret de l'espionnage mondial. "C'était une gageure, (...) donner un visage à ce qui normalement n'en a pas", a dit le ministre de la Défense Jean-Yves Le Drian en inaugurant l'exposition **"Guerres secrètes"** qui s'ouvre mercredi au **musée de l'Armée des Invalides**. Dans un décor aussi sombre que le sujet, une galerie de photos légendées rappelle d'entrée le destin d'espions de légende: l'officier-écrivain britannique Thomas Edward Lawrence, dit "Lawrence d'Arabie", dont le sabre et le poignard au fourreau doré sont exposés; Vladimir Vetrov alias "Farewell", taupe du **KGB** qui a livré au début des années 80 une liste d'espions soviétiques en Europe et aux Etats-Unis ; la Britannique Violette Szabo, exécutée à 24 ans par les nazis à Ravensbrück.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Morocco tipped off Israeli intelligence, 'helped Israel win Six Day War'
Times of Israel, Sue Surkes, 2016 10 18
Jerusalem - **Israel largely has Morocco to thank for its victory over its Arab enemies in the 1967 Six Day War, according to revelations by a former Israeli military intelligence chief**. In 1965, King Hassan II passed recordings to Israel of a key meeting between Arab leaders held to discuss whether they were prepared for war against Israel. That meeting not only revealed that Arab ranks were split -- heated arguments broke out, for example, between Egypt's president Gamal Abdel-Nasser and Jordan's king Hussein -- but that the Arab nations were ill prepared for war, **Maj. Gen. Shlomo Gazit** told the Yedioth Ahronoth newspaper over the weekend. On the basis of these recordings, as well as other intelligence information gathered in the years leading up to the war, Israel launched a preemptive strike on the morning of June 5, 1967, bombing Egyptian airfields and destroying nearly every Egyptian fighter plane.

Syria intelligence chief in Cairo for security talks
Now Lebanon, Albin Szakola, 2016 10 18
Beirut - A **top Syrian intelligence official has discussed security coordination with his Egyptian counterpart amid** warming ties between the two countries. Syria's state news agency reported Monday that Syrian National Security Bureau chief Ali Mamlouk "made an official visit to Cairo," where he met with General Khaled Fawzy, the head of Egypt's General Intelligence Directorate, as well as other "senior security officials." "The two sides agreed to coordinate political stances," SANA claimed, adding that they also decided to "strengthen coordination in the fight against terrorism."

The Yom Kippur War Came as a Surprise to the Egyptians as Well, Documents Show
Haaretz, Amir Oren, 2016 10 13
Jerusalem - **"We had a report in the CIA in late May 1973** that said, 'Egypt and Syria will start **war against Israel** on the 6th of October,'" **CIA Deputy Director Gen. Vernon Walters** said in a lecture to the U.S. Army Security Agency Training Center and School a year and a half after the Yom Kippur War. "We duly reported this," Walters continued. "But one of my experiences with the intelligence business has been that the analysts generally shrink from telling you something really unpleasant, and even after we try to fit every piece of intelligence in to show that it wasn't going to happen on the 6th of October.

Return to Table of Contents/ Retour à la table des matières

Asia / Asie

Pakistani agents making calls to executives at oil installations to extract key details
The Economic Times, Sanjeev Choudhary, 2016 10 18
New Delhi—Indian oil installations are on Pakistan's radar. The **Intelligence Bureau has advised the oil ministry to step up safety and information shield at important energy installations after it intercepted a conversation in which a Pakistani spy was heard extracting information from an oil industry executive**.Since the September 18 terror attack in Uri and the retaliatory surgical strikes by the Indian Army on terror camps across the Line of Control in Pakistan-occupied Kashmir, there have been fears of an escalation of conflict on both sides of the border prompting defence forces and intelligence agencies to be on high alert. IB recently intercepted a conversation in which a Pakistani operative, posing as an officer of India's external intelligence agency, **the Research & Analysis Wing**, engaged on phone an executive managing a sensitive hydrocarbon pipeline in Rajasthan and sought finer details about the facility, sources with direct knowledge of the matter said.

Create National Counter-Terrorism Centre to fight terror: Experts
Times of India, Bharti Jain, 2016 10 17
New Delhi - As the Modi government mulls **revisiting UPA's proposal for a National Counter-Terrorism Centre (NCTC) to track and fight terror,** experts feel the idea may be stillborn without a constitutional amendment to separate common 'law and order' duties from intra-state, transnational offences like terrorism and cyber crime, and bringing the latter under the Union or concurrent list. Chief ministers, who have been opposing NCTC, saying its powers to arrest and search suspects anywhere in the country would encroach upon their turf.

Supreme Court ruling over KakaoTalk wiretapping sparks controversy
Korea Herald, Sohn Ji-young, 2016 10 17
Seoul - The **South Korean Supreme Court's latest ruling over the legality of wiretapping the country's dominant mobile messenger KakaoTalk** for investigative purposes is igniting controversy between the prosecution and related stakeholders. Last Thursday, the Supreme Court of Korea ruled that conversations taken from KakaoTalk severs cannot be recognized as **wiretapped evidence**, as they were not seized in real time as mandated by the legal definition of "wiretapping." The ruling over what constitutes as "wiretapped evidence" came as the court was reviewing various evidence alleging that a leftist civic group violated the National Security Law. Up to now, Kakao has been handing over personal conversation records saved on its servers during selected time periods as requested by the prosecution.

Two held for 'spying' for Pakistan: ISI agent honey trapped one accused
The Indian Express, 2016 10 14
New Delhi—A day after two **Bhuj residents were arrested for allegedly spying for Pakistani intelligence agency ISI, officials of the Gujarat Anti-Terrorism Squad (ATS)** on Thursday said they suspect "one accused was honey trapped by a 17-year-old ISI agent and later trained by a handler" to pass on information about the movement of Army and BSF troops, besides inputs on vital installations in the region. **Alleged spy Alana Hamir Sama** (40), resident of Kukma village in Bhuj taluka of Kutch district, and **his associate Shakoor Sumra** (38), resident of nearby Sumrapor village, were arrested Wednesday by the ATS from Bhuj bus station. According to senior officials, following high alert after the Army's surgical strike along the LoC, the ATS was scanning the movement of people visiting Pakistan when it came to know about Sama's frequent visits to the neighbouring country.

'Spy' pigeon's wings clipped to stop it flying back to Pakistan: Indian police
Pakistan Dawn, 2016 10 14
Islamabad - The **wings of a 'spy' pigeon taken into custody by Indian police** earlier in October have been clipped, an Indian Punjab police official told The Telegraph India on Wednesday. The 'spy' pigeon was found carrying what officials said was a warning note to Indian Prime Minister Narendra Modi near the heavily-militarised border as Pak-India tensions simmered following the Uri attack, subsequent ceasefire violations and an Indian 'surgical strike' - a claim Pakistan has rejected.

Japan gov't widens counter-cyberattack protection to more entities (Canada)
Kyodo News, Staff reporter, 2016 10 12
Tokyo - The **Japanese government decided Wednesday to extend its counter-cyberattack monitoring of key government agencies** to include nine government-affiliated bodies, including the national pension operator that saw more than 1 million sets of personal information leaked in a high- profile attack. The government's cybersecurity strategy task force selected the bodies for monitoring by the **National Center of Incident Readiness and Strategy for Cybersecurity, or NISC**, in line with an amended cybersecurity law that came into force this month following its enactment in April. Previously, the scope of monitoring was only government ministries and agencies. "The government must steadily administer the amended law to thoroughly deal with cyber measures for these organizations," Chief Cabinet Secretary Yoshihide Suga said at a meeting of the task force Wednesday. The nonbinding guidelines call for institutions to clarify their personnel's roles and responsibilities in dealing with the attacks, share information on attacks and threats with stakeholders in a timely manner and review cybersecurity strategy regularly. The G-7 comprises Britain, **Canada**, France, Germany, Italy, Japan and the United States.

N.K. spy agency official defected to S. Korea last year: source
Yonhap News Agency, Staff reporter, 2016 10 12
Seoul - A **senior official at North Korea's spy agency defected to South Korea last year, a source said Wednesday**, pointing to a rise in defections by North Korean elites **disillusioned with the repressive regime**. An unidentified official who worked for the Ministry of State Security escaped to the South last year, the source familiar with Pyongyang's affairs said, in an unusual defection by a North Korean in charge of gathering intelligence and cracking down on ordinary people. The source said that North Korean leader **Kim Jong-un** is believed to have been upset by the growing number of elite members defecting. Seoul's unification ministry said it has no specific information on the defection by the North Korean spy agency's official. More North Korean elites, including diplomats, have deserted their country in search of freedom, which Seoul says points to signs of cracks in the North's regime.

Return to Table of Contents/ Retour à la table des matières

Africa / Afrique

'Power of Sudan's Security Apparatus to Be Restricted' – PCP
All Africa, 2016 10 17
Khartoum— The recommendations of **Sudan's National Dialogue stipulate the restriction of the powers of the National Intelligence and Security Service (NISS) to the collection and analysis, says the Popular Congress Party**. The National Consensus Forces coalition rejects the outcomes of the Dialogue. In early January, the Sudanese parliament passed a number of amendments to the 2005 Interim Constitution. An important amendment concerned the

extension of the NISS competences, by which the institution became a full part of Sudan's regular forces. According to the chairman of the parliamentary Popular Congress Party (PCP) block, Dr Ismail Hussein Fadlallah, the "sinful" amendments would convert Sudan into a full-blown police state.

Bernard Cazeneuve appelle à la coopération contre le terrorisme et la lutte contre la radicalisation
All Africa, Noël Ndong, 2016 10 13
Dakar, Sénégal - En visite à Dakar au Sénégal dans le cadre de la coopération bilatérale, le ministre français de l'Intérieur, **Bernard Cazeneuve, a rencontré son homologue sénégalais, Abdoulaye Daouda Diallo. Au centre de leur entretien: la lutte contre le terrorisme et la radicalisation.** Une nouvelle convention a été signée. "L'islamisme radical est enkysté dans certains territoires, il faudrait du temps pour l'éradiquer. La propagande sur internet agit sur les plus vulnérables, bien que de plus en plus empêchée par les mesures que nous avons prises", a reconnu Bernard Cazeneuve.

Return to Table of Contents/ Retour à la table des matières

Americas / Amériques

Venezuela's intelligence chief accuses opposition of terrorist acts, assassination
United Press International, Staff report, 2016 10 12
Caracas - The **head of Venezuela's Bolivarian Intelligence Service, or SEBIN, has accused some opposition members of terrorist acts and assassination in efforts to remove President Nicolas Maduro from power**. **SEBIN Director Gustavo González López**, formerly the minister of interior and justice, said on Tuesday Carlos Ocariz, a mayor of the Sucre municipality in the Miranda state, is one of those being investigated over alleged terrorist acts. González López spoke about two incidents: a video released by the Justice First opposition party which González López said incites military rebellion, and the launch of a grenade at a Venezuelan National Guard post in the Sucre municipality.

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

19-10-2016 to/au 25-10-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Why security shouldn't be left only to security services
Toronto Star, Michelle Shephard, 2016 10 24
Analysis: The depressing reality first. Our terror years since Sept. 11, 2001, will continue for more to come. Syria's slaughter and other regional conflicts will persist. The refugee crisis is beyond staggering. In early 2015 when I pitched my Atkinson Fellowship "Generation 9/11" to study why young Canadians are attracted to groups such as Daesh, the situation was grim. Much has deteriorated since and we cannot ignore how it is all related. No politician should talk about counterterrorism efforts without also condemning state terrorism. Bashar Assad's regime, with Russia's support, is committing war crimes against Syrian civilians with impunity. Meanwhile groups like Daesh (also known as ISIS or ISIL) push their narrative of a world war against Muslims, even as they kill thousands of Muslims in their own war. Every country needs to help ease the refugee crisis. If Daesh was able to recruit from the disenfranchised of Generation 9/11, what will become of this next generation? In early 2012, I travelled with videographer Randy Risling to report on the thousands of children fleeing Syria's war. We called our series "Childhood Interrupted." Those children, who were in refugee camps in Turkey, are now teenagers and adults. Their childhood wasn't just interrupted, but lost. If we ignore their futures, we not only turn our backs on a humanitarian crisis, but we have handed terrorists a rich hunting ground for recruits. **Privately, the RCMP and CSIS say they are overwhelmed, and I have sympathy for their position. Not everybody can be monitored, or should be.** Aaron Driver appeared to be moving on until he was shot dead, armed with an improvised explosive device, in Strathroy, Ont. Michael Zehaf-Bibeau, who stormed Parliament Hill in 2014, was low on a list of Canadians that may pose a threat. **But if the federal agencies are grappling with the workload, why waste resources on the case of the B.C. couple John Nuttall and Amanda Korody?** In throwing out the charges against the former drug addicts, a judge blasted the RCMP for "abuse of power" in entrapping them. B.C. Supreme Court Justice Catherine Bruce said in her July verdict: "They were clearly overzealous and acted on the assumption that there were no limits to what was acceptable when investigating terrorism. "We do not need the police to create more (terrorists) out of marginalized people who have neither the capacity nor sufficient motivation to do it themselves." This case cries for an examination of RCMP misconduct, but also stresses the need to bolster community services that could have helped Nuttall and Korody before they fell prey to terrorist ideology (or a police sting). Zehaf-Bibeau was so desperate for help that he robbed a McDonald's with a stick so he could go back to jail and clean up.(Note: Michelle Shephard, the Star's national security correspondent, travelled to a half-dozen countries and interviewed foreign fighters, security experts, policy makers and religious leaders for this year's series. This is the final column in her series "Generation 9/11" that explored the issue of Daesh's foreign members and how Canada and the world should respond. Read the stories at www.thestar.com/news/atkinsonseries/generation911)

RCMP's counterterrorism centre in Ottawa serves as intersection of information
The Globe and Mail, Colin Freeze, 2016 10 24
Ottawa - **The Mounties have created a permanent place for counterterrorism detectives to work shoulder-to-shoulder - and database to database - with federal border guards, immigration officials and spy-agency analysts**. The RCMP's **national-security joint-operations centre (NSJOC)** in Ottawa is a "real-time and rapid information-sharing" crossroads where federal agents can **efficiently swap files, according to recently released records**. However, critics fear it will go places no watchdog can follow. The counterterrorism centre was largely unknown until RCMP Commissioner **Bob Paulson** made a brief reference to it in Parliament earlier this year. The Globe and Mail has acquired the centre's terms of reference under Access to Information laws. The centre brings federal agents of all stripes together in an RCMP facility in Ottawa where they can talk to each other and exchange information as part of the fight against terrorism. It formally came into existence in October, 2014, the same month two men inspired by the Islamic State killed two Canadian Forces soldiers. The next spring, executives at the **Communications Security Establishment, the Canadian Security Intelligence Service**, the **Canada Border Services Agency** and **Citizenship and Immigration Canada** signed the centre's terms of reference, under which they agree to embed at least one staff member with the RCMP at all times. Today, federal-security agencies are under renewed pressure to amass and share records. Recent disclosures indicate CSIS, the domestic spy agency, has been "ingesting bulk data sets " in hopes of predicting patterns of terrorism, and its foreign-focused counterpart, CSE, is mapping out "contact chains" of global communications to discern where threats lie. It's not clear how police would use such deductions. The records about the RCMP-led centre say that sharing information, early and often, can minimize the risk that federal police and spies trip over each other, and head off future problems.

Snowden says Trudeau afraid to kill anti-terrorism bill
It World Canada, Howard Solomon, 2016 10 19
Toronto - Whistleblower. Hero. Traitor. Patriot. These words and more have been used to describe former cybersecurity contractor **Edward Snowden**, who in 2013 copied and distributed thousand of documents to reporters and whose stories of Western intelligence agencies -- including **Canada's Communications Security Establishment (CSEC)** -- shook the world. This morning **Snowden told the annual SecTor cyber security conference in Toronto that Prime Minister Justin Trudeau want to amend the controversial Bill C-51 anti-terrorism law and not repeal it because he "is afraid of being attacked for being soft on terrorism."** Speaking by video from Russia, where he fled to avoid prosecution by U.S. authorities, Snowden said the legislation, needs three fixes: First, a judicial body should have oversight over federal intelligence agencies that has the power to prosecute authorities that have broken the law. Second, because intelligence agencies are trading personal information of citizens "like baseball cards" citizens should be told if the data sharing hasn't led to an arrest for criminal activity. And finally, what Snowden called the criminalization of speech through vague definitions of terrorism should be taken out of C -51. A lot of what police call terrorism is the activity of what he called "common criminals" or those who are trying to make a political point but don't constitute a "super criminal threat."

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

Obama Says U.S. Has No Idea Who Carried Out Cyberattack
Wall Street Journal, Carol E. Lee, Damian Paletta, 2016 10 25
Los Angeles - **President Barack Obama said the U.S. doesn't know who launched an online attack Friday that rendered more than 1,200 websites unreachable, including Netflix and Twitter**. "We don't have any idea who did that," Mr. Obama said during a taped appearance Monday for the late-night show hosted by Jimmy Kimmel. U.S. officials and cybersecurity experts believe attackers controlled a vast collection of internet-linked devices such as cameras, video recorders and routers, to essentially overwhelm parts of the internet and make dozens of popular websites unreachable. **The Department of Homeland Security on Monday said it was still "monitoring events" tied to the attack.** It said that following the incident, it held a conference call with 18 telecommunications service providers to discuss what happened, adding "at this time, we believe the attack has been mitigated." DHS said "one type of malware potentially used in this incident" is known as Mirai and targets devices such as cameras and entertainment systems that have internet links. DHS is working to develop rules to address these types of attacks, but the timing of such a move is unclear.

Ex-CIA director says 'Fox News has jumped the shark' and abandoned 'conservatism'
Washington Times, Douglas Ernst, 2016 10 24
Washington - **George W. Bush's former director of the NSA and the CIA likened Fox News' Sean Hannity to a Soviet-era apparatchik over the weekend**. Brookings Institute senior fellow Benjamin Wittes shared a scathing statement by Michael Hayden on Sunday in response to Mr. Hannity's support for WikiLeaks. The Fox host has cheered the group's release of stolen documents belonging to Hillary Clinton campaign chairman John Podesta. **U.S. intelligence agencies have blamed Russian state actors for the theft. "Fox News has almost entirely jumped the shark,"** Mr. Hayden wrote. "They have given up any semblance of conservatism and focused on an almost visceral hatred of all things Clinton and Obama." The former CIA head said that some exceptions to the rule include Chris Wallace, Megyn Kelly and Brett Baier.

Plans to send heavier weapons to CIA-backed rebels in Syria stall amid White House skepticism
Washington Post, Greg Miller, Adam Entous, 2016 10 24
Washington - As rebel-held sections of Aleppo crumbled under Russian bombing this month, **the Obama administration was secretly weighing plans to rush more firepower to CIA-backed units in Syria.** The proposal, which involved weapons that might help those forces defend themselves against Russian aircraft and artillery, made its way onto the agenda of a recent meeting President Obama held with his national security team. And that's as far as it got. **Neither approved nor rejected, the plan was left in a state of ambiguity that U.S. officials said reflects growing administration skepticism about escalating a covert CIA program that has trained and armed thousands of Syrian fighters over the past three years**. The operation has served as the centerpiece of the U.S. strategy to press Syrian President Bashar al-Assad to step aside. But U.S. officials said there are growing doubts that even an expanded version could achieve that outcome because of Moscow's intervention. Obama, officials said, now seems inclined to leave the fate of the CIA program up to the next occupant of the White House.

Military Warns Chinese Computer Gear Poses Cyber Spy Threat (Canada)
Washington Free Beacon, Bil Gertz, 2016 10 24

Washington - **The Pentagon's Joint Staff recently warned against using equipment made by China's Lenovo computer manufacturer amid concerns about cyber spying against Pentagon networks**, according to defense officials. A recent internal report produced by the **J-2 intelligence directorate** stated that cyber security officials are concerned that Lenovo computers and handheld devices could introduce compromised hardware into the Defense Department supply chain, posing cyber espionage risks, said officials familiar with the report. The "supply chain" is how the Pentagon refers to its global network of suppliers that provide key components for weapons and other military systems. **The J-2 report was sent Sept. 28, and also contained a warning that Lenovo was seeking to purchase American information technology companies in a bid to gain access to classified Pentagon and military information networks.** The report warned that use of Lenovo products could facilitate cyber intelligence-gathering against both classified and unclassified--but still sensitive--U.S. military networks. The cyber spying concerns are not limited to the Pentagon. The Australian Financial Review newspaper reported in 2013 that all of the **"Five Eyes" intelligence services--those in the United States, Britain, Australia, Canadian, and New Zealand**--strictly prohibit the use of Lenovo computers over concerns about the potential for cyber espionage.

Pentagon Expects Mosul Push to Unlock Trove of ISIS Intelligence
New York Times, Eric Schmitt, 2016 10 23
Washington - **The Pentagon is sending dozens of additional intelligence analysts to Iraq to pore over a trove of information that is expected to be recovered in the offensive to recapture Mosul from the Islamic State, data that could offer new clues about possible terrorist attacks in Europe**. The analysts will have several immediate priorities: Share with the Iraqi military any information crucial to the unfolding fight in Mosul; pass along insights useful to American officials planning an attack on Raqqa, the Islamic State's de facto capital in eastern Syria; hunt for clues about the location of the group's shadowy leader, Abu Bakr al- Baghdadi; and search for any information about terrorist cells in Europe and any attacks they may be plotting. Maj. Gen. Gary J. Volesky, the commander of American ground forces in Iraq, has called Mosul the Islamic State's Iraqi "crown jewel." Noting that the militants had been entrenched there for more than two years, he added on Wednesday, "Clearly, there's going to be intelligence that will be able to be exploited."

F.B.I. Is Fighting a Return to an Old Boys' Club
New York Times, Adam Goldman, 2016 10 23
Washington - When the call came in that a bomb had exploded in Manhattan, **Amy Hess quickly got to work. She helped direct teams of F.B.I. agents to New York to collect evidence, set up secure command posts in the streets so agents could discuss classified information, and alerted the digital forensics, fingerprint and facial recognition experts she manages in Quantico, Va., site of the F.B.I. academy and its lab**. By the next day, she and her team had played a crucial role in identifying Ahmad Khan Rahami, the man charged with planting the bomb in Chelsea along with a second, unexploded device. "We pulled out all the stops," said Ms. Hess, who as head of the bureau's science and technology branch oversees more than 6,000 F.B.I. employees. Inside the F.B.I., women in particular look up to Ms. Hess, and not just because they have nicknamed her the "rocket scientist" with a degree in aeronautical and astronautical engineering from Purdue University. She is also the first woman to head the science branch -- one of few female agents commanding such an important job at the F.B.I., a clubby agency where men are more predominant in senior positions than they were even three years ago. Ms. Hess, 50, put it simply: **"There is a lack of women in leadership roles."** Today at the F.B.I., women hold 12 percent of 220 senior agent positions, including nine who run field offices in places like Los Angeles; Oklahoma City; Louisville, Ky.; and Knoxville,

Tenn. That is a decline from 2013, when women held about 20 percent of senior agent jobs and 15 women ran field offices.

Homeland Security struggles to detain rising numbers of undocumented people
Wall Street Journal, Devlin Barrett, 2016 10 22
Washington - **Homeland Security officials are quietly scrambling to find 5,000 more prison and jail beds to handle a record number of undocumented immigrants being detained in the U.S.**, according to officials familiar with the discussions. **Homeland Security Secretary Jeh Johnson** met Tuesday with senior leaders at the **Immigration and Customs Enforcement agency** and the **Customs and Border Protection agency** -- both of which are in his department -- so officials could review their plans to handle **thousands more people expected to cross the border with Mexico in coming weeks**, the officials said. ICE is holding more than 40,000 people in detention centers -- more than it has ever had in custody before -- and has warned budget officials that it needs a quick infusion of $136 million more just to keep running detention centers until early December, according to internal Department of Homeland Security documents and officials. A spokeswoman for the Department of Homeland Security declined to comment on internal agency discussions. The agency is "committed to continuing to ensure that individuals are detained in a safe, secure and humane manner in line with our detention standards and our values as a nation," she said.

Man Who Took Trove of N.S.A. Data Has Court Date
New York Times, Scott Shane, 2016 10 22
Baltimore - **The intelligence contractor accused in the largest- ever breach of classified information was portrayed by his lawyer in court on Friday as a patriot and a dedicated worker who became compulsive about taking work home**. An unlocked garden shed, stuffed with more classified documents than the contractor, **Harold T. Martin III,** could ever read, might be a symptom of a mental disorder, the lawyer said. Mr. Martin, a rotund man with glasses whose striped gray jail garb stood out in an ornate federal courtroom here, sat silently during his first public appearance as his lawyer, James Wyda, argued that he should be released while awaiting trial. The prosecution, opposing the request, described Mr. Martin, 51, in starkly different terms: as a serial lawbreaker of staggering audacity. Over two decades as a contractor for the **National Security Agency and other government units, it said, he took home masses of secrets in full knowledge that it was illegal to do so.** And, the prosecution added, there is no way to be certain what he has done with the information, or whether he might be hiding more.

Theft by former NSA worker much worse than thought, prosecutors allege
Christian Science Monitor, Zhai Yun Tan, 2016 10 22
Washington - **A former National Security Agency contractor accused of stealing hoards of top secret government information is set to face more serious charges than previously announced**, with prosecutors hoping to prevent him from being released on bail. According to the federal prosecutors' court filing on Thursday, Harold T. Martin III committed a theft that was "breathtaking in its longevity and scale," **stealing enough material to fill up to 200 laptop computers**, according to the Associated Press. The information includes "specific operational plans against a known enemy of the United States," and handwritten notes with explanations that the government says is intended for an "audience outside of the Intelligence Community." "Given the nature of his offenses and knowledge of national secrets, he presents tremendous value to any foreign power that may wish to shelter him within or outside of the United States," prosecutors said. Prosecutors argue that Mr. Martin should not be released on bail because he is "a risk to the nation and to the physical safety of others," The Washington Post reports.

Ex-NSA contractor deemed flight risk in theft case
Washington Post, Ellen Nakashima, 2016 10 22
Baltimore - **A federal judge found Friday that a former National Security Agency contractor accused of carrying out what is thought to be the largest theft of classified secrets in U.S. history posed a flight risk and ordered that he continue to be held in jail.** U.S. Magistrate Judge A. David Copperthite ruled that Harold T. Martin III should not be released pending trial, despite the impassioned arguments of his defense attorney that the computer technology expert is a patriot who intended no harm to his country and suffered from a "compulsive disorder" that led him to steal classified material over a 20-year period. Defense attorney James Wyda conceded that Martin took the material, but he stressed that "there's no evidence that Hal shared this information with anyone" or that he intended to pass it to a foreign government. "There is nothing to indicate that Hal Martin is a traitor," Wyda told the judge, as Martin, a heavyset man wearing gray- striped jail garb, sat quietly at the defense table. "What we see is an individual who is a collector." He told the court that his client is not like **Edward Snowden, the former NSA contractor who gave classified material on U.S. surveillance programs to journalists**, or **Aldrich Ames, a onetime CIA officer who was recruited by the Soviet Union and betrayed agents working for the United States**. Wyda portrayed Martin, 51, as a "voracious learner committed to being excellent at his work" who gathered information to improve his knowledge. "What began as an effort to be better at his job," Wyda said, became over the years a compulsion. "Frankly," he said, "the mental health component is the only explanation."

Case of Former N.S.A. Contractor Escalates as Espionage Act Charges Loom
New York Times, Scott Shane, 2016 10 21
Baltimore - A **former intelligence contractor stole the equivalent of 500 million pages of government documents over two decades of work at seven companies, including top-secret plans for an operation against a hostile country**, prosecutors said in papers filed in Federal District Court here on Thursday. The prosecutors also said that the former contractor, **Harold T. Martin III**, who worked for the **National Security Agency** and other military and intelligence agencies, kept an "arsenal" of 10 firearms at home in Maryland, including an assault-style rifle and a loaded handgun that he kept illegally in his car. Mr. Martin was initially charged with theft of government property and mishandling of classified information, violations carrying a maximum sentence of 11 years. But the new filing said prosecutors planned to charge him with violating the Espionage Act and committing other felonies, crimes that could put him in prison for decades if he is convicted. He is scheduled to appear at a hearing in federal court on Friday afternoon for arguments about whether he will remain in detention. The government's filing deepens the mystery surrounding Mr. Martin's grand-scale compilation over decades of a home library of top-secret material, some of which F.B.I. agents found lying in the open in his car and home office. The new details in the government's filing paint a darker picture, offering hints -- though no proof -- that he might have taken the material to give it to others, conceivably even to a foreign nation. Prosecutors said he **had communicated with others in foreign languages, including Russian,** and downloaded information about the Russian language.

Did Hillary Clinton reveal classified intel at debate?
CNN.com, Jamie Crawford, 2016 10 21
Washington - The **Twitterverse was aflame in the hours after Wednesday night's debate with questions about whether or not Hillary Clinton divulged classified information about the country's nuclear arsenal. "There's about four minutes between the order being given** and the people responsible for launching nuclear weapons to do so," Clinton said, explaining the quick decision-making required of a commander in chief and questioning Donald Trump's

fitness for the job. "And that's why 10 people who have had that awesome responsibility have come out and, in an unprecedented way, said they would not trust Donald Trump with the nuclear codes or to have his finger on the nuclear button," she continued. But questions soon began to emerge about whether Clinton was too specific in her description of nuclear launch times and had perhaps revealed something she learned in a classified setting. **A Clinton campaign aide said the information didn't come from a classified briefing**, pointing to multiple instances when similar information has been disclosed in public or through open source material.

NSA Can Access More Phone Data Than Ever
ABC News, Lee Ferran, 2016 10 20
Washington - One of the reforms designed to rein in the surveillance authorities of the **National Security Agency has perhaps inadvertently solved a technical problem for the spy outfit and granted it potential access to much more data than before, a former top official told ABC News.** Before the signing of the **USA Freedom Act in** June 2015, one of the NSA's most controversial programs was the mass collection of telephonic metadata from millions of Americans -- the information about calls, including the telephone numbers involved, the time and the duration but not the calls' content -- under a broad interpretation of the Patriot Act's Section 215. From this large "haystack," as officials have called it, NSA analysts could get approval to run queries on specific numbers purportedly linked to international terrorism investigations. The problem for the NSA was that the haystack was only about 30 percent as big as it should've been; the NSA database was missing a lot of data. As The Washington Post reported in 2014, the agency was not getting information from all wireless carriers and it also couldn't handle the deluge of data that was coming in. On the technical side, **Chris Inglis, who served as the NSA's deputy director until January 2014, recently told ABC News that when major telecommunications companies previously handed over customer records, the NSA "just didn't ingest all of it."**

NSA chief: Cyber adds 'whole other dimension' to Russia's attempts to manipulate U.S. affairs
Baltimore Sun, Ian Duncan, 2016 10 20
Baltimore - The **head of the NSA said Thursday that Russia's hack of Democratic Party emails is consistent with its history of trying to manipulate and influence affairs in other countries** -- but the scope of such operations has changed dramatically. "Cyber adds a whole other dimension to this because it now enables individuals, actors, groups, nation states to acquire data at massive scale and then divulge that," **Adm. Michael S. Rogers** told cyber professionals at the sixth annual Cyber Maryland Conference in Baltimore. The job now for the National Security Agency and other parts of the government, Rogers said, is to make sure that Americans continue to have confidence in the electoral system. "As we work our way through this particular issue, that's always at the forefront of our minds," he said.

U.S. vote authorities warned to be alert to Russian hacks faking fraud - officials
Reuters, David Rohde, Mark Hosenball, 2016 10 21
Washington **- U.S. intelligence and law enforcement officials are warning that hackers with ties to Russia's intelligence services could try to undermine the credibility of the presidential election** by posting documents online purporting to show evidence of voter fraud. The officials, who spoke on condition of anonymity, said however, that the U.S. election system is so large, diffuse and antiquated that hackers would not be able to change the outcome of the Nov. 8 election. But hackers could post documents, some of which might be falsified, that are designed to create public perceptions of widespread voter fraud, the officials said. They said

that they did not have specific evidence of such a plan, but state and local election authorities had been warned to be vigilant for hacking attempts.

NSA: Hackers find an easy path to U.S. systems
FCW.com, Sean D. Carberry, 2016 10 20
Washington - For all the concern about zero-day exploits, a **senior NSA official said that the high-profile hacks of U.S. networks in the last two years show there are far easier ways for cybercriminals to infiltrate government systems**. Speaking at the American Enterprise Institute on Oct. 18, **Curtis Dukes, deputy national manager for national security systems at the NSA**, said that none of the high-profile government hacks the NSA responded to -- Office of Personnel and Management, the White House, State Department, Department of Defense -- used zero-day exploits. "Basically the adversary took advantage of poorly secured, poorly patched systems," said Dukes. "Once they had that initial foothold they the elevated privileges and then moved to mission objective," which ranged from stealing data to (in the case of the Sony hack) destroying it.

Trove of Stolen Data Is Said to Include Top-Secret U.S. Hacking Tools
New York Times, Multiple reporters, 2016 10 20
Washington - **Investigators pursuing what they believe to be the largest case of mishandling classified documents in United States history have found that the huge trove of stolen documents in the possession of a National Security Agency contractor** included top-secret N.S.A. hacking tools that two months ago were offered for sale on the internet. They have been hunting for electronic clues that could link those cybertools -- computer code posted online for auction by an anonymous group calling itself the Shadow Brokers -- to the home computers of the contractor, **Harold T. Martin III**, who was arrested in late August on charges of theft of government property and mishandling of classified information. But so far, the investigators have been frustrated in their attempt to prove that Mr. Martin deliberately leaked or sold the hacking tools to the Shadow Brokers or, alternatively, that someone hacked into his computer or otherwise took them without his knowledge. While they have found some forensic clues that he might be the source, the evidence is not conclusive, according to a dozen officials who have been involved in or have been briefed on the investigation. In **interviews, officials described how the Martin case has deeply shaken the secret world of intelligence**, from the N.S.A.'s sprawling campus at Fort Meade, Md., to the White House.

US, UK Cybersecurity Officials: Destructive Hacks Are Coming
Associated Press, Staff report, 2016 10 20
London - The world should brace itself for more physically destructive hacks, two senior cybersecurity officials said Wednesday, warning that a more dangerous era of hacking was already upon us. **Paul Chichester, the director of operations at Britain's new National Cyber Security Center, told an event hosted by British defense think tank RUSI that electronic intrusions were on their way to becoming more "destructive, disruptive and coercive**." "That will be our future," he told a crowd of officers, academics and industry experts gathered for a two-day symposium in central London. Chichester was seconded by Air Force Lt. **Gen. James K. McLaughlin, deputy commander at U.S. Cyber Command**, who told attendees that infrastructure-wrecking attacks were being seen "right now in the environment." Neither official went into specifics about what they'd seen or why they felt the threat was intensifying, although McLaughlin invoked a cyberattack in Ukraine which knocked out three separate power distribution companies last year. The Dec. 23 incident, believed to have been pulled off by a team of hackers using stolen passwords, left 225,000 people without electricity, according to a U.S. Department of Homeland Security bulletin published two months later.

Yahoo calls for greater transparency from intelligence services
Financial Times, Hannah Kuchler, 2016 10 20
San Francisco - **Yahoo is demanding US intelligence services reveal how they monitor online services,** after a report said the internet company secretly scanned customer emails. In a **letter to James Clapper, the US director of national intelligence**, Yahoo said citizens in a democracy require more information to understand and debate how the US uses legal authorities to obtain private data. Yahoo said it found itself unable to respond in detail to the accusations in a Reuters article earlier this month, which claimed that the company had secretly built custom software to scan users' incoming emails for specific information requested by US intelligence officials.

Media vulnerable to Election Night cyber attack
Politico, Darren Samuelsohn, Hadas Gold, 2016 10 19
Washington - **Despite spending hundreds of millions of dollars on security upgrades, U.S. media organizations have failed to properly protect their newsrooms from cyberattacks** on their websites, communications systems and even editing platforms -- opening themselves up to the possibility of a chaos-creating hack around Election Day. In just the past month, BuzzFeed has been vandalized, and both Newsweek and a leading cybersecurity blog were knocked offline after publishing articles that hackers apparently didn't appreciate. Federal law enforcement is investigating multiple attacks on news organizations, and journalists moderating the presidential debates say they've even gotten briefings from the FBI on proper cyber hygiene, prompting them to go back to paper and pens for prep work. "We do a lot of printing out," said Michele Remillard, an executive producer at C-SPAN, the network home to the backup moderator for all the debates.. Senior U.S. officials, current and former lawmakers and cybersecurity pros told POLITICO the threat against the media is real -- and they fret the consequences. Specifically, the **security community is worried The Associated Press' army of reporters could get hacked and the wire service** -- the newsroom that produces the results data on which the entire media world relies -- inadvertently starts releasing manipulated election tallies or that cybercriminals penetrate CNN's internal networks and change Wolf Blitzer's teleprompter.

Politics keeps the U.S. from securing private-sector networks, says former CIA chief Robert Gates
Computerworld, Patrick Thibodeau, 2016 10 19
Orlando - A person who had access to the nation's deepest secrets, **Robert Gates, the former CIA chief and U.S. Secretary of Defense from 2006 to 2011, is lot more open in retirement**. Gates had the crowd at the Gartner Symposium/ITxpo laughing over his observations about IT and applauding at some of the things he believes in. Gates divided cyber threats into four areas. There is the collection of data for national security purposes, something the U.S. has been doing since the Civil War when it tapped into telegraph lines. The second threat is acquiring information for economic advantage.

America's election is giving the world some serious anxiety
Washington Post, David Ignatius, 2016 10 19
Column - Making predictions three weeks before the U.S. election is risky, but the likeliest bet right now is that the center will hold in American politics and Hillary Clinton will be elected president. That's important for lots of reasons, the biggest of which is that it could begin to stabilize a very unsettled world. **To many analysts, Vladimir Putin's Russia has seemed on the march while the United States and its allies are in retreat**. The danger of U.S.-Russian conflict was described by **Rolf Mowatt- Larssen, a former senior CIA officer**, in a recent

article. "As a life-long observer of Russia, I have never been as concerned as I am now on the state of Russian-American relations," he wrote. "A dangerous zero sum game pattern has emerged as US and Russia make moves and countermoves that mimic practice during the Cold War."

Ex-CIA chief: Russian hackers trying to 'mess with our heads'
CNN.com, Nicole Gaouette, 2016 10 19
Washington - A **former head of the CIA said Tuesday that Russian hacking of US political groups is intended to "mess with our heads"** and shake confidence in the American electoral system -- rather than influence the outcome on Election Day. **Retired Gen. Michael Hayden** said that he doesn't believe Russian President Vladimir Putin is trying to sway the election in favor of Republican nominee Donald Trump, but using the hacked information to disrupt the electoral process. "This is too much of a carom shot for Putin to think he knows where that ball's going to end," Hayden said, speaking at the Heritage Foundation in Washington. "I think they're doing this to mess with our heads, to erode confidence in our political process."

Ex-F.B.I. Official Acknowledges Role in a New Clinton Email Controversy
New York Times, Eric Lichtblau, Steven Lee Myers, 2016 10 19
Washington - A **former F.B.I. official at the center of the latest controversy over Hillary Clinton's private emails acknowledged on Tuesday that an offer to swap favors with a State Department counterpart on an email classification issue had originated with him** -- until he realized the deal involved Mrs. Clinton and the 2012 attack in Benghazi, Libya. "When I found that out, all bets were off; it wasn't even negotiable," the **former F.B.I. official, Brian McCauley,** said in a telephone interview. Republicans have seized on the episode to accuse the State Department of trying to protect Mrs. Clinton, but Mr. McCauley's account could undercut those attempts because he said he, not the State Department, had suggested the "quid pro quo." Mr. McCauley recounted in the interview that Patrick F. Kennedy, a senior State Department official, called him in spring 2015 looking for help in getting the F.B.I. to agree not to classify the disputed email. Mr. McCauley said he had agreed to try to help him if Mr. Kennedy would help him get the State Department to restore two spots that the F.B.I. had lost recently in the Baghdad embassy.

Feds need clarity on cyber structures
fed scoop.com (US), Shaun Waterman, 2016 10 19
Washington - The federal government needs to get its act together on cybersecurity, and there needs to be a public debate about the proper role for agencies like the **Department of Homeland Security and the National Security Agency**, public and private sector leaders said Tuesday. "We really need to define what we want our government to do in cybersecurity, former **Rep. Mike Rogers** told an audience at FedScoop's FedTalks. "We have lots of capability. The NSA has lots of capability," he told a packed auditorium in Washington at the annual event. By giving DHS, rather than NSA, the lead in defending civilian government networks and working with the private sector to protect the nation's vital industries, the U.S. had "take[n] our best players off the field," complained Rogers, who chaired the House Permanent Select Committee on Intelligence. "Candidly," Rogers said, that decision "was politically driven and not policy driven. People were a little nervous about having NSA ... dealing directly with them" and their networks -- even companies that had a prior relationship with the NSA or the Pentagon were nervous.

CIA's In-Q-Tel Invests In Data Analytics Company MapD
Wall Street Journal, Carl Zakrzewski, 2016 10 19

Washington— The **venture-capital arm of the Central Intelligence Agency, In-Q-Tel, said on Tuesday that it has invested in MapD Technologies Inc**., a database and visualization startup.MapD Chief Executive Todd Mostak built the database powered by a graphics-processing unit when he was doing research at the Massachusetts Institute of Technology and needed to visualize social-media posts for a thesis he was writing about the Middle East. The CPU-powered systems that were available to him weren't powerful enough, so Mr. Mostak built his own GPU-powered system. Now a U.S. government agency, a large social media company and Verizon Wireless are also relying on his company to help them quickly visualize large data sets. The tool can query billions of records in milliseconds, eliminating delays for the people who use them.

Rogers: 'We're working our way through' process to split NSA- CYBERCOM roles
Inside Defence (US), Marjorie Censer, 2016 10 18
Washington - **Adm. Mike Rogers, the chief of U.S. Cyber Command and the National Security Agency, said today he is thinking through the "right time" and "right process" to split the roles he hold**s. Speaking at a FedTalks event in Washington, Rogers said the idea behind the shared role was for **CYBERCOM**, in its early days, to harness the "insight, capabilities and knowledge" of NSA. Now, he's asking: "Are the assumptions that we made still accurate? Have things changed? Is the environment different?" The challenge in splitting the roles, Rogers added, is "what's the right time, what's the right process so that we do it in a way that enables both organizations to fulfill their missions with minimal risk? "So we're working our way through that process," he continued. "In the end, this is a decision that the president of the United States is going to make, and we'll see where that process takes us."

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

Half of Ukip supporters think MI5 is out to get them, poll shows
The Independent (UK), Ben Kentish, 2016 10 24
London **- Almost half of UKIP members think MI5 is trying to destroy their party, according to a new poll**. The YouGov survey found 46 per cent of members agreed with the statement **"Intelligence services like MI5 have been working to undermine UKIP". The poll echoes an earlier finding that almost a third of Ukip supporters believed MI5 was involved in a plot to rig the EU referendum result**. Other conspiracy theories are also popular among party activists. More than half (55 per cent) think some UKIP members have been planted by Conservative strategists to undermine the party, while 40 per cent believe the EU referendum was the subject of electoral fraud, with officials rubbing out and changing votes. Almost nine in 10 (89 per cent) believe the media is being deliberately biased in its coverage of their party.

GCHQ using cyber attacks on Isil to aid battle to take Mosul
Daily Telegraph, Ben Farmer, 2016 10 22
London - **GCHQ is using cyber warfare for the first time against Isil militants as part of the campaign to retake Mosul**, the Defence Secretary has said. The cyber attacks are understood to have targeted the communications of Islamic State of Iraq and the Levant to disrupt co-ordination in the Iraqi city. Sir Michael Fallon told a conference organised by the Royal United Services Institute, a think tank on cyber warfare: "We are conducting military operations against

Daesh [Isil] as part of the international coalition, and I can confirm that we are using offensive cyber for the first time in this campaign."

US firms could make Ireland terrorist target, says CIA head
Irish Times, Colin Gleeson, 2016 10 21
Dublin - The **director of the CIA has suggested the Republic may be a target for Islamic terrorism due to the prevalence of US multinationals there. John Brennan**, who succeeded David Petraeus as the head of the United States intelligence agency in 2013, said it was important for Irish authorities to be "vigilant" of the threats posed. "I don't think any country should feel immune from the reach of these terrorist organizations," he said in an interview with Irish-American website Irish Central. "Ireland first of all is an open and welcoming country, and also there are also a lot of Americans there and American businesses. "I was in Ireland last August and I **met with the Irish intelligence heads** and talked to them about the importance of sharing information. If there is anything that looks or seems a bit off putting, those pieces of the puzzle need to be put together," he said.

GCHQ using cyber attacks on Isil to aid battle to take Mosul
London Daily Telegraph, Ben Farmer, 2016 10 21
London - **GCHQ is using cyber warfare for the first time against Isil militants as part of the campaign to retake Mosul**, the Defence Secretary has said. The cyber attacks are understood to have targeted the communications of Islamic State of Iraq and the Levant to disrupt co-ordination in the Iraqi city. Sir Michael Fallon told a conference organised by the Royal United Services Institute, a think tank on cyber warfare: "We are conducting military operations against Daesh [Isil] as part of the international coalition, and I can confirm that we are using offensive cyber for the first time in this campaign." He said £265 million is being pumped into "rooting out cyber vulnerabilities" in military and wider cyber- systems.

Can governments really keep us safe from terrorism without invading our privacy?
Wired (UK), Ruby Lott-Lavigna, 2016 10 20
London - **GCHQ has many negative connotations attached to it - including illegally collecting data from the UK public** - but **David Omand, former head of GCHQ** and now professor at Kings, is hoping for a change in the way governments deal with our private information. Referring to new legislation that is currently going through parliament - the **'Investigatory Powers Law' -** he explained how regulation is being implemented to create transparency in the way the UK government deals with cybersecurity. "What is going on, as we speak, is a phase change in the relationship between the secret state and parliament," explained Omand. "One way of looking at this is that the secret activity of the state is now being fully bought under the modern rule of law." So where does the line stand with mining data for security reasons? Is there a balance to be reached between privacy and security? According to Omand, "2017 is the year of reconciliation, in which we recognise as a mature democracy, it is possible to have sufficient security and sufficient privacy." "The key to that is rule of law. Courts have to have comprehensible, black letter law."

Hackers are not as 'sophisticated as they think they are'
Wired (UK), Matthew Levy, 2016 10 20
London - The **way we talk about cyberattacks** has created a culture of fear around online security, said **Ian Levy, technical director at the National Centre for Cyber Security. The newly-formed offshoot of GCHQ** will be responsible for coordinating UK cybersecurity efforts and keeping the UK safe from online threats. "The context in which you judge something also influences how you interpret it," he told the audience at WIRED Security in London. Media coverage of cyberattacks is crammed full of scary buzzwords. Cyberattacks - invariably

represented by a lone hooded teenager in a dark room - are described as 'sophisticated' and 'unprecedented.' Levy pins at least part of the blame for this language on the cybersecurity industry itself. "There is no other bit of public policy where the tone is set by a group of massively incentivised people," he said.

UK spies infiltrated Isis leadership, ex-jihadis claim
The Independent (UK), Kim Sengupta, 2016 10 20
Urfa, Turkey - "They are afraid of a lot of things now. They are afraid of the bombing, they are afraid of the attack that's coming and they are also really afraid of the foreign spies who are among them". This was Rashid's description of what was going on inside Isis. **And the Western intelligence agency that has infiltrated Isis the most, claimed the Belgian jihadi, was the British. Rachid is one of the thousands of foreign fighters who had gone to join Syria's jihad**, graduating in extremism among rebel groups to two years serving with Isis. But disillusioned, he says, with the Islamists and fearing what lay ahead, he has fled across the border to Turkey. Rachid, a mechanic before he took up the gun in the name of Islam, was part of a small but steady flow of fighters leaving Isis as it faces an assault on Mosul, its last stronghold in Iraq and waited for the coming offensive against Raqqa, the capital of its "caliphate" in Syria. The contact with Rachid came through an intermediary in Turkey after I wrote an article in The Independent last month about thousands of jihadis from who, with Isis facing defeat, will be seeking to return.

Ireland to follow UK in setting up national cyber security centre
Computer Weekly (UK), Warwick Ashford, 2016 10 19
Dublin - **Ireland plans to set up a national cyber security centre**, according to **Denis Naughten, the country's communications minister**. The news comes less than a month after the **UK's National Cyber Security Centre (NCSC)** officially opened for business, combining all the government's cyber security agencies under one roof. "I will bring a memorandum to cabinet next week to establish a national cyber security centre that will focus on securing government networks," Naughten told the (ISC)2 EMEA Congress 2016 in Dublin. The centre will also cover the security of critical national infrastructure as well as assist industry and individuals to protect their digital assets.

Keeping Britain safe: how GCHQ's new cyber security agency will protect us from hackers
Wired (UK), Matthew Reynolds, 2016 10 18
London - The Doughnut - **GCHQ's vast, Cheltenham-based nerve centre - is a building straight from the pages of a spy novel. Its imposing circular walls are surrounded by fences topped with razor wire and multiple vehicle checkpoints. Visitors are seldom allowed inside the building which, Edward Snowdon's NSA leaks**, is the centre of government mass surveillance in the UK. The intelligence agency's latest spin-off, the National Cyber Security Centre, couldn't look more different. Occupying two floors of a commercial office block in Victoria, London, the NCSC is shedding its parent agency's secretive persona in favour of a more collaborative approach. There's even going to be a Shake Shack on the ground floor. "NCSC as an organisation is going to be open by default," says Ian Levy, the NCSC's technical director. The fledgling agency only opened its doors on October 3, but it's already started its task of keeping the public and the UK's critical national infrastructure safe from cyberattacks launched by states, organised crime gangs and lone-wolf hackers. For Levy, partnerships with the UK's cyber security community will be key to keeping the country safe online.

Return to Table of Contents/ Retour à la table des matières

Australia/ Australie

Army kit in eye-spy conspiracy (Canada)
The Advertiser, Charles Miranda, 2016 10 21
Canberra - The **Chinese military could "track" Australian soldiers after a firm in China was given the contract to make dress uniforms for the Defence Force**. That was the claim made by Labor senator Kim Carr at a parliamentary review into the Defence portfolio yesterday. It could have focused on armaments procurement and the war in the Middle East. Instead, Senator Carr fired conspiracy theory-style questions about the formal dress of officers, including those worn by officers giving evidence. While combat uniforms are made in Australia, a 2015 tender for dress uniforms saw no Australian company with the capacity to make them locally. The contract was awarded to Bendigo-based **Australian Defence Apparel**, which subcontracted it to a Chinese firm.Senator Carr said ADA's parent company in Canada, Logistik Unicorp, conceded it had radio frequency identification technology to track goods.

Ex-spy chief warns of net threats
Sydney Morning Herald, Deborah Snow and David Wroe, 2016 10 20
Sydney - The **task of being an intelligence chief has become tougher with the rise of cyber threats and terrorism, according to the former head of the Australian Security Intelligence Organisation, David Irvine**, who says he would like to see a "much stronger" national cyber industry. Speaking during a rare interview in Canberra, Mr Irvine said "when you put cyber on top of [terrorism], it takes a bit of time off your sleep at night. The two issues have grown exponentially within a couple of decades and while the nature of the threats is the same, the vector has changed. And cyber is a new and very potent vector." Mr Irvine, who led Australia's overseas spy agency ASIS before he headed up ASIO, said he'd been "horrified" at the revelations of Edward Snowden, the subcontractor to the National Security Agency who exposed vast top- secret US government programs for monitoring global communications. "People say, well nobody lost their lives as a result of Snowden, but how do you know that? You run through your mind all the possible consequences of having your capabilities, which are there to defend the country, exposed ..."

Kids of Aussies exposed to extremism: ASIO
Australian Associated Press, Roje Adaimy, 2016 10 19
Canberra - **Up to 70 children of Australians have been exposed to extremist groups in the battlefields of Syria or Iraq, the country's security chief has revealed. Duncan Lewis, director-general of the Australian Security Intelligence Organisation**, said these children either travelled to the conflict zones with their Australian parents or were born there. He told a Senate committee late on Tuesday night that ASIO is investigating around 190 people in Australia who are actively supporting groups like IS through recruiting, fundraising or wanting to join themselves. That includes about 40 Australians who have returned from Syria or Iraq. "The long-term impact of the returnees will be a security issue for this country's intelligence and law enforcement agencies for many years to come," he said. Mr Lewis confirmed up to 68 Australians are believed to have been killed in the conflicts - 11 of them since May. Around 110 people are still fighting or engaged with terrorist groups in Syria and Iraq.

Radical right-wing groups a threat: ASIO
Australian Associated Press, Staff reporter, 2016 10 19
Melbourne - **Reclaim Australia says it has never condoned violence but national intelligence bosses say radical anti-Islamic groups are a growing threat to Australia's security. ASIO director-general Duncan Lewis said Reclaim Australia,** in particular, was of interest to intelligence agencies. Authorities charged a member of the right-wing group under federal terror laws for the first time in August for allegedly collecting or making documents to prepare for terrorist acts. Mr Lewis said Reclaim Australia has "offered violence" in the past and expects they will continue to when they confront pro-Islamic groups. "To the extent that there is a possibility of violence, or there is indeed violence being offered, that is of interest to us. That is business for ASIO," he told a Senate committee late on Tuesday night. "It is a real problem and it is something that we're very, very acutely aware of and I have people working that particular issue." **But Reclaim Australia said it does not condone violence**. "

Return to Table of Contents/ Retour à la table des matières

New Zealand/Nouvelle-Zélande

Light coverage/couverture légère.

Return to Table of Contents/ Retour à la table des matières

International

China/Chine

Chinese police officials study Belarus' experience of public order maintenance
BelaPan, 2016 10 20
Minsk— A delegation of **China's Ministry of Public Security** stayed in Minsk on October 19 and 20 to study Belarus' experience of **public order maintenance**, said the Belarusian interior ministry's press office. Deputy Interior Minister Mikalay Melchanka reportedly told the delegation that law enforcement agencies in Belarus and China shared years-long friendly ties, and that bilateral relations had reached a "high level of strategic constructive partnership."

Return to Table of Contents/ Retour à la table des matières

Russia/Russie

Lawmaker raises fears about Russian satellites
Washington Post, Christian Davenport, 2016 10 22

Washington - In a letter to the Pentagon on Friday, **Rep. Duncan D. Hunter** said he was concerned that a **contract to provide Internet service to deployed soldiers could allow the use of Russian satellites, jeopardizing troops' privacy and security.** Previous service at bases' Internet cafes had "stringent security measures," Hunter wrote to Army Lt. Gen. Alan Lynn, the head of the **Defense Information Systems Agency (DISA**). But he said he is worried that the "contracting arrangement creates unnecessary security risks, given that our deployed warfighters could be exposed to transmitting their personal information over unprotected networks that are controlled by foreign and potentially hostile entities." In an interview, Hunter (R- Calif.), who served three tours as a Marine, said: "This is one of the dumbest things we could do. Why give the Russians the ability to basically spy on American military personnel when there are so many other options?" A DISA spokesman said the agency could not discuss the provisions of the contract or which companies may have submitted offers.

How Russia Pulled Off the Biggest Election Hack in U.S. History
Esquire, Thomas Rid, 2016 10 21
New York - On an April afternoon earlier this year, Russian president **Vladimir Putin** headlined a gathering of some four hundred journalists, bloggers, and media executives in St. Petersburg. Dressed in a sleek navy suit, Putin looked relaxed, even comfortable, as he took questions. About an hour into the forum, a young blogger in a navy zip sweater took the microphone and asked Putin what he thought of the "so- called Panama Papers." When Putin heard the blogger's question, his face lit up with a familiar smirk. He nodded slowly and confidently before reciting a litany of humiliations that the United States had inflicted on Russia. Putin reminded his audience about the sidelining of Russia during the 1998 war in Kosovo and what he saw as American meddling in Ukraine more recently. **Returning to the Panama Papers, Putin cited WikiLeaks to insist that "officials and state agencies in the United States are behind all this."** The Americans' aim, he said, was to weaken Russia from within: "to spread distrust for the ruling authorities and the bodies of power within society." Though a narrow interpretation of Putin's accusation was defensible--as WikiLeaks had pointed out, one of the members of the Panama Papers consortium had received financial support from USAID, a federal agency--his swaggering assurance about America's activities has a more plausible explanation: Putin's own government had been preparing a vast, covert, and unprecedented campaign of political sabotage against the United States and its allies for more than a year. The Russian campaign burst into public view only this past June, when The Washington Post reported that "Russian government hackers" had penetrated the servers of the Democratic National Committee. The hackers, hiding behind ominous aliases like **Guccifer 2.0 and DC Leaks**, claimed their first victim in July, in the person of Debbie Wasserman Schultz, the DNC chair, whose private emails were published by WikiLeaks in the days leading up to the Democratic convention.. But in many ways, the DNC hack was merely a prelude to what many security researchers see as a still more audacious feat: the hacking of **America's most secretive intelligence agency, the NSA**.

Digital Trail Betrays Identity Of Russian 'Hacker' Detained In Prague
Radio Free Europe, Dmitry Treshchanin, Nick Shchetko, 2016 10 20
Prague - An investigation by RFE/RL's Current Time TV has determined that the **Russian national accused by American officials of hacking U.S. targets and arrested earlier this month in the Czech capital is 29-year-old Moscow resident Yevgeny Nikulin**. Czech authorities this week said the suspect was detained in downtown Prague on October 5 in response to an Interpol warrant requested by the United States and now faces a Czech extradition hearing. Czech police and local media have identified him only as "Yevgeniy N," and the Russian and U.S. governments revealed only that he was a Russian citizen. Current Time's investigation uncovered Nikulin's Instagram account under the handle "i.tak.soidet," displaying a taste for luxury cars and jewelry and a digital trail that led through Belarus and Poland to the

Czech Republic in the weeks before the Prague arrest. It is unclear exactly what role Nikulin is suspected of playing in the alleged U.S. website hacks or even which websites were involved. A spokesperson from the U.S. Embassy in Prague confirmed that a Russian had been detained who was "suspected of hacking U.S. targets."

Wheels within wheels
The Economist, Staff report, 2016 10 20
London - MYSTERY, MIRACLE AND authority are three powers alone able to hold the conscience of people captive, explains Fyodor Dostoyevsky's Grand Inquisitor in "The Brothers Karamazov". Mr Putin has mastered all three. Yet none of these is as important as secrecy, the main tool of a good spy. Nobody really knows what goes on behind the Kremlin's thick walls, or inside Mr Putin's head. But several things are becoming clearer. Mr Putin's rule is turning increasingly personal; a generational shift is taking place within his entourage; **and the FSB, the successor organisation to the KGB, is emerging as the main mechanism for exercising power, often at the expense of all other security services**, including the police. Mr Putin had always relied heavily on his former KGB colleagues, but after the annexation of Crimea the expansion of the FSB gained new momentum and greater public legitimacy. It now openly wields political and economic power. Mr Putin has recently appointed three members of his security detail and one former KGB officer as regional governors. After Stalin's death in 1953, the KGB was a "combat division" of the Communist Party, tightly controlled by its central committee, which did not want to see a repeat of Stalin's purges. When the party collapsed in 1991 the KGB lost its lustre, but the new rulers never dismantled it. Though the party could not survive without ideology, the KGB could. Today the FSB is personally overseen by Mr Putin. "There is no political control over the FSB.

Moscow says still no evidence from US proving alleged Russian hacker attacks
ITAR-TASS World Service, Staff report, 2016 10 18
Moscow - **Moscow has received no evidence from the United States proving Russia's alleged hacker attacks on US institutions**, Russian Foreign Ministry Spokeswoman Maria Zakharova said on Tuesday. "There have been no proof, do data, no passwords, no hyperlinks. Nothing," she said. Washington's inability to provide any proof can only mean that such allegations target domestic audience and are part of the presidential campaign, she said, adding that attempts at reducing the presidential campaign to accusations against Russia are inglorious for a great power. "It is a global disgrace," she said.

Return to Table of Contents/ Retour à la table des matières

Europe

Malte : cinq morts dans le crash d'un avion de reconnaissance de la défense française
La Matinale du Monde, Journaliste maison, 2016 10 25
Malte - **Un avion effectuant des missions de reconnaissance en Méditerranée pour le ministère français de la défense s'est écrasé, lundi 24 octobre dans la matinée à Malte, tuant les cinq hommes se trouvant à son bord, ont annoncé des responsables**. L'appareil a décollé vers 7 h 20 de l'aéroport international de Malte mais a piqué vers le sol quelques secondes plus tard, s'écrasant dans une boule de feu. Enquêtes ouvertes A Paris, le ministère de la défense a refusé de préciser la destination de l'avion ou l'objet de sa mission de reconnaissance. Plusieurs enquêtes ont été ouvertes, dont une interne « pour déterminer les causes de l'accident, en coordination avec les autorités locales » , a ajouté le ministère, qui n'a

pas précisé si les victimes étaient toutes françaises. Le gouvernement maltais a cependant annoncé dans un communiqué que les dépouilles de cinq hommes français avaient été retrouvées sur le lieu du drame. Parmi les cinq personnes à bord, trois relevaient « du ministère de la défense » - elles travaillaient pour la **Direction générale de la sécurité extérieure (DGSE) -** et deux étaient des salariés d'un contractant privé**, la société luxembourgeoise CAE Aviation**, qui détenait l'appareil, a précisé le ministre. **Les trois employés de la DGSE intervenaient notamment en Libye lors de missions de renseignement**.

German Terrorism Case Highlights Europe's Security Challenges
New York Times, Alison Smale, Melissa Eddy, 2016 10 25
Berlin - **The warning came to the German security authorities in early September from "our best partners," as they euphemistically refer to the American intelligence agencies: A terrorist assault might be in the works**. In the weeks that followed, the Germans identified a suspect, a refugee from Syria. They unearthed evidence that he had been casing a Berlin airport for an attack, and they recovered powerful explosives from his apartment, only to see him slip through their fingers. When they eventually captured him, the suspect promptly hanged himself in his jail cell. The case was notable for its dramatic turns. But it also underscored two central challenges facing the Continent: getting a handle on the security risk related to the arrival of more than a million migrants last year, and addressing the continued reliance of European governments on intelligence from the United States to avert attacks. Both issues have been plaguing Europe since the high-profile attacks in France and Belgium over the past two years. Governments have scrambled to counter the threat even as migrants, many with little or no documentation of their identity or country of origin, came over their borders in previously unheard-of numbers. The challenge has become more pressing in Germany in recent months after a spate of arrests and attacks, some linked to migrants. **"In a way, we have outsourced our counterterrorism to the United States," said Guido Steinberg, a terrorism expert at the German Institute for International and Security Affairs. "The Germans are not ready to build up their intelligence capabilities for political reasons, so this will continue."** The **recognition of how reliant Germany remains on the United States for its safety stands in contrast to Germany's hostile reaction in 2013, when Edward J. Snowden revealed the extent of United States surveillance programs, including one that extended to Chancellor Angela Merkel's cellphone.** "American agencies are Europe's best counterterrorists," said Peter Neumann, a terrorism expert at King's College London. "That is the big secret that no one wants to talk about."

Bavarian agency increases surveillance of anti-government extremists

Deutsche Welle, 2016 10 22
Munich - **Authorities in the German state of Bavaria are due to increase surveillance of anti-government extremists following a deadly shooting last Wednesday, the head of the state's intelligence agency has told dpa**. The shooting, which saw a 49-year-old fire at four policemen, killing one, took place in the small town of Georgensgmuend near Nuremberg. "Surveillance of the Reich Citizens' Movement was already intensified in the last months, but now we will increase it again," Burkhard Koerner, the head of Bavaria's Office for the Protection of the Constitution, said. "In this scene there are people who become increasingly radicalised and their irritation at the state of things can grow into real hatred of the state," Koerner said. "That's why I have said it many times in the last months: it may not all be extremism, but there are people involved here who are dangerous." Koerner's agency says that 30 to 40 members of the Reich Citizens' Movement are also part of the state's right-wing extremist scene, but the

total number of people in the movement remains unknown. "We particularly want to look at how many people involved have gun licences," Koerner said.

NATO Adds New Chief of Intelligence
Wall Street Journal, Julian E. Barnes, 2016 10 22
Brussels— The **North Atlantic Treaty Organization appointed its first intelligence chief, a post designed to help the alliance improve information sharing and counterterrorism coordination**.Officials said Friday that alliance **Secretary-General Jens Stoltenberg** was appointing longtime **German diplomat Arndt Freytag von Loringhoven** as assistant secretary-general for intelligence and security. Mr. von Loringhoven **served as vice president of Germany's Federal Intelligence Service** from 2007 to 2010. Officials have said the post will focus initially on improving intelligence sharing on Russia's military buildup, as well as addressing duplication in civilian and military intelligence efforts. The new post could also help improve counterterrorism intelligence sharing -- pushing NATO into an area often left to bilateral cooperation.

Un article de la loi renseignement censuré
Le Monde, Jean-Baptiste Jacquin, 2016 10 22
Paris— C'est un petit article de loi en vigueur depuis vingt-cinq ans que le Conseil constitutionnel a censuré dans une décision rendue vendredi 21 octobre. Cet **article permettait tout bonnement aux services de renseignement de procéder sans le moindre contrôle à la surveillance de communications par voie hertzienne**. Les gardiens de la Constitution le déclarent contraire à l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 en portant " une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances ". Ils le déclarent inconstitutionnel et demandent au législateur d'élaborer un nouveau texte d'ici au 31 décembre 2017. " Un trou législatif béant "C'est en invoquant cette disposition particulièrement floue que **Bernard Squarcini**, l'ancien patron de la **Direction centrale du renseignement intérieur (DCRI),** avait pris la liberté de procéder à des écoutes dans l'affaire des fadettes du Monde. Lors du débat sur la loi renseignement de 2015, quelques mois après les attentats contre Charlie Hebdo et l'Hyper Cacher, personne ne semblait s'être intéressé à cet article introduit par la loi de 1991 sur le secret des correspondances. Cette dernière avait elle-même été votée après le scandale des écoutes de l'Elysée où François Mitterrand avait fait écouter des personnalités, dont le journaliste du Monde Edwy Plenel.

Le Conseil constitutionnel dit non à la surveillance de masse sans contrôle
Le Monde, Jean-Baptiste Jacquin, 2016 10 22
Paris - C'est un petit article de loi en vigueur depuis vingt-cinq ans que le Conseil constitutionnel a censuré dans une décision rendue vendredi 21 octobre. **Cet article permettait tout bonnement aux services de renseignement de procéder sans le moindre contrôle à la surveillance de communications par voie hertzienne**. Les gardiens de la Constitution le déclarent contraire à l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 en portant « une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances . Ils le déclarent inconstitutionnel et **demandent au législateur d'élaborer un nouveau texte d'ici au 31 décembre 2017**. **Au nom de « la défense des intérêts nationaux » , les pouvoirs publics pouvaient ainsi surveiller les déplacements de sous-marins étrangers ou les mouvements de troupes sur un théâtre d'opération, mais également des communications par téléphone mobile entre particuliers, des échanges par Wi-Fi ou Bluetooth**. Rebaptisé article L. 811-5 dans la loi renseignement de juillet 2015, cet article permettait aux services de renseignement de s'affranchir des contrôles que cette loi imposait, en précisant, par exemple, que la surveillance de particuliers ne peut être autorisée

par le premier ministre qu'après avis de la **Commission nationale de contrôle des techniques de renseignement (CNCTR).** C'est en invoquant cette disposition particulièrement floue que Bernard Squarcini, l'ancien patron de la **Direction centrale du renseignement intérieur (DCRI),** avait pris la liberté de procéder à des écoutes dans l'affaire des fadettes du Monde . Lors du débat sur la loi renseignement de 2015, quelques mois après les attentats contre Charlie Hebdo et l'Hyper Cacher, personne ne semblait s'être intéressé à cet article introduit par la loi de 1991 sur le secret des correspondances. Cette dernière avait elle-même été votée après le scandale des écoutes de l'Elysée où François Mitterrand avait fait écouter des personnalités, dont le journaliste du Monde Edwy Plenel.

Germany reforms its main intelligence service
Deutsche Welle, Staff report, 2016 10 21
Berlin - **Germany's lower house of parliament, the Bundestag, has passed a comprehensive reform of the country's main intelligence service, the BND**. The new legislation strengthens government monitoring of intelligence activities while explicitly allowing the BND to **carry out certain types of surveillance activities**. The reform comes in the wake of the 2013 revelations by American whistleblower Edward Snowden that a number of national intelligence services, including the BND, had spied on behalf of the **US National Security Agency (NSA)** and that the NSA had spied on its allies. That prompted the formation of a German parliamentary committee to draft intelligence agency reforms. The new legislation subjects the BND to monitoring by an "independent panel" of two judges and a federal prosecutor and a "permanent commissioner" from the Interior Ministry. It stipulates that surveillance of international communications networks must be authorized by the Chancellor's Office rather than by the BND itself and explicitly prohibits economic and industrial espionage. The new laws also provide for better protection for whistleblowers within intelligence services and subjects the BND to annual public hearings instead of private ones, as has been the case. The reform permits the BND to cooperate with foreign intelligence services like the NSA if it serves specific purposes, including fighting terrorism, supporting the German military on foreign missions or collecting information concerning the safety of Germans abroad.

German parliament agrees to new security service controls
DPA News Agency, 2016 10 21
Berlin— The **German parliament on Friday agreed on tougher governmental controls of the nation's foreign intelligence agency BND**, following allegations that the BND aided the United States' intelligence service in spying on Berlin's European allies. Opposition parties Die Linke and the environmentalist Greens voted against the new rules, which were passed in the Bundestag by a majority of Chancellor Angela Merkel's conservative political bloc and its junior coalition partner, the Social Democrats. Under the legislation agreed by the lower house of the German parliament, a three-member independent panel comprising two judges and a federal prosecutor will oversee the BND's activities. The legislation stipulates that the chancellor's office will in future have to authorize the BND's surveillance of international telecommunications.

Foreign intel agencies behind Gülenists: former minister
Hurriyet Daily News, Staff report, 2016 10 20
Ankara - A **former police chief and interior minister, Mehmet Agar**, has told a parliamentary commission investigating the July 15 coup attempt that all illegal organizations, like the Gülenist network, **have had links with foreign intelligence services**. "Every secret organization in Turkey has foreign links. Usually, those links involve foreign intelligence services," Mehmet Agar told the commission on Oct. 20. Agar did not detail which foreign services were behind the Gülenist network blamed for the July coup attempt. Attending the commission, Agar indicated

that while struggling against illegal organizations, mistakes could cause sympathizers to become militants.

Slovak Finance Ministry drafts country's first cyber-security law
SC Magazine, Jaroslaw Adamowski, 2016 10 20
Bratislava— **Slovakia is in the process of drafting its first cyber-security law** which will address not only the security of finance and health but also critical utilities infrastructure. Slovakia's Ministry of Finance is currently drafting the country's first cyber-security law, according to Slovak deputy prime minister for investments and information Peter Pellegrini."Right now, in cooperation with **the National Security Authority**, we are finalising works on a new law on cyber-security," Pellegrini told local news site Tablet.tv. "One thing is to protect banks' data assets and medical records, but we must also talk about how the country will respond if a cyber-attack is performed on its grids or water supply systems."Meanwhile, local observers say that, due to the lack of a comprehensive cyber-security law, whenever Slovak companies have their data stolen, local police investigate such instances as simple acts of theft. Slovakia's decision-makers started to streamline more efforts to cyber-security in the wake of Russia's military intervention in Ukraine.

Czechs Arrest Man Wanted by the F.B.I. for Hacking
New York Times, Rick Lyman, Hana de Goeij, 2016 10 20
Prague - A **man identified as a Russian hacker suspected of pursuing targets in the United States has been arrested in the Czech Republic**, the police announced Tuesday evening. The suspect was captured in a raid at a hotel in central Prague on Oct. 5, about 12 hours after the authorities heard that he was in the country, where he drove around in a luxury car with his girlfriend, according to the police. The man did not resist arrest, but he had medical problems and was briefly hospitalized, the police said in a statement. David Schön, a police spokesman, said on Wednesday that the arrest of the man, whose name has not been released, was not announced immediately "for tactical reasons." The Russian Embassy in Prague called for the man to be released. Jakub Janda, who studies the Russian government and is a deputy director of the European Values Think- Tank in Prague, said that the arrest served as confirmation that "the Czech Republic is so far considered a safe base for Russian intelligence and influence activities focused on Western targets." He added, "Prague is unofficially considered to be a springboard for some Kremlin activities inside Europe, also using huge Russian diplomatic presence of approximately 140 staff." Mr. Janda also said that the arrest showed that "Western governments are waking up and finally **considering hostile Russian intelligence and disinformation operations** to be an open and urgent threat, even at the level of the U.S. administration."

Dragan accuser spied for Croatia
The Australian, Jacquelin Magnay and Ivica Profaca, 2016 10 20
Split, Croatia - An **international war crimes trial** against Australian citizen and Serbian paramilitary commander **Dragan Vasiljkovic** exploded into an angry war of words as one of his main accusers was revealed to have been working for **Croatian intelligence**, raising questions about the use of his testimony. In a second setback, a key prosecution witness, a Serbian cook named Pero Dragisic, was one of three who failed to turn up to give evidence yesterday. But the testimony that ignited controversy was that of Velibor Bracic, 48, who told the international court sitting in Split that he was kicked in the head while on the ground by Mr Vasiljkovic shortly after being captured on June 16, 1991. Mr Vasiljkovic, better known as Captain Dragan in the Balkans and as Daniel Snedden in Australia, became agitated as he cross-examined Mr Bracic, telling the judge that he had waited 11 years for this moment. During the cross-examination Mr Bracic admitted: "I did some work for our **(Croatian) intelligence."** Mr Bracic refused to directly

answer whether at the time of his arrest he was working as a spy. He said he had been caught on the Bosnia and Croatia border, north of Knin, while undertaking reconnaissance as a reserve in the Croatian police force.

Turkey takes on a new anti-terror strategy, Erdogan says
Daily Sabah, Staff report, 2016 10 19
Ankara - **President Recep Tayyip Erdogan said Wednesday that Turkey has employed new understanding when it comes to counterterror operations**, stressing that the government will take necessary steps to eliminate all terror threats before terror groups take action. Addressing village headmen at the Bestepe Presidential Complex in Ankara, the president said that Turkey will no longer follow what he called the "wrong security approach," saying that "From now on, we will not wait for troubles to come knocking on our doors." Underlining that Turkey has been through difficult times both politically and economically, the president said that the Turkish people have suffered for many years due to internal conflicts which he referred to as "brothers killing brothers." "We have lost thousands of our people due to brothers fighting each other. We do not want to pay a price anymore. I am announcing this today; from now on, Turkey has left its wrong understanding of security behind." Erdogan highlighted that **Ankara's new counterterrorism approach** will tackle the problem at its source rather than dealing with the consequences of the terror threat.

« Vengeance » française
L'Express, Boris Thiolay, 2016 10 19
Paris - Les derniers assassinats ciblés ordonnés par les autorités françaises contre des ennemis d'Etat visent en priorité « les commanditaires et les planificateurs des attentats de Paris, qui se trouvent en Syrie », confie à L'Express un expert en sécurité de premier plan. Dans le livre Un président ne devrait pas dire ça... (Stock), publié la semaine dernière, François Hollande reconnaît avoir décidé, avant octobre 2015, « quatre au moins » de ces opérations « Homo » (homicide). **Ces exécutions sont menées par la Direction générale de la sécurité extérieure (DGSE) ou les services d'un pays allié,** Etats-Unis en tête. Notre expert poursuit : « Depuis janvier 2016, l'élimination des djihadistes responsables des massacres du 13 novembre [photo] est devenue systématique. Il s'agit à la fois d'une vengeance assumée par la France et d'un signal envoyé à tous les individus impliqués. » Parmi ces derniers, se trouvent plusieurs djihadistes français.

Intelligence agency warns of ISIL attacks in five Turkish provinces
Hurriyet Daily News, Staff report, 2016 10 18
Ankara - The **National Intelligence Agency (MIT) has issued warnings against imminent attacks by the Islamic State of Iraq and the Levant (ISIL) in five Turkish provinces**. MIT sent a warning to all 81 provinces of Turkey, saying jihadists could launch attacks in Istanbul, the southeastern province of Gaziantep, Ankara, the southern province of Antalya and the western province of Izmir. According to the MIT report, public transport is among ISIL militants' targets, daily Cumhuriyet reported on Oct. 18. The warning dated Oct. 12 and coded "urgent" said the aforementioned five provinces were among the high-risk areas.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Security agencies avert suicide attacks in Beirut's southern suburbs
Lebanon Daily Star, Staff Report, 2016 10 24
Beirut - **A joint security investigation has paved the way for security agencies to avert a number of attacks in Beirut's southern suburbs,** a media report said Saturday. A security report published in As-Safir newspaper said that **Lebanese Army Intelligence** and **General Security had busted a terror network and clamped down on members planning to carry out attacks during Ashoura commemorations in Beirut's southern suburbs**. Sources told the daily that General Security detained one of the group's members in Beirut's Cola area, who allegedly admitted to planning a suicide attack using an explosive belt in Al-Rasoul Al-Azam Hospital. The sources added that investigations had revealed that extremists had provided the alleged suicide bomber with logistical support. Three suspects were handed over to the Army Intelligence.

Pentagon chief in Irbil for closer assessment of Mosul fight
Associated Press, Lolita C. Baldor, 2016 10 23
Irbil - **U.S. Defence Secretary Ash Carter visited Irbil on Sunday for a closer assessment of the fight against the Islamic State group in northern Iraq and to hear from Kurdish leaders whose forces launched a new offensive in the operation to wrest Mosul from the militants' control**. Carter met with Kurdish leader Masoud Barzani, as well as U.S. service members who are not far from the battle. The Pentagon chief praised the efforts of the Kurdish forces, known as peshmerga, and acknowledged their battle losses. ``They fight extremely well. But because they're fighting hard, they suffer ... casualties,'' said Carter, who spent Saturday in Baghdad getting updates from his military leadership and meeting with Iraqi Prime Minister Haider al-Abadi. The U.S. is prepared to provide additional support for the fight if requested by Iraq and U.S. commanders, Carter said in the capital. Peshmerga Brig. Gen. Halgord Hekmet, a spokesman for the Kurdish forces, told reporters that 25 of their troops have been killed since the battle to retake Mosul began and a ``large number'' had been wounded. Speaking through an interpreter, he said the peshmerga have had good coalition air support, but could use more military resources, especially armoured vehicles.

Russia preparing to spy on Syria internet, activists warn
Now Lebanon, Albin Szakola, 2016 10 21
Beirut - An activist group dedicated to ensuring safer online communication for Syrians has warned that maintenance work being conducted on an undersea cable providing internet to the country is part of a **Russian espionage effort**. SalamaTech Project issued a statement Wednesday that Syrian Telecom's announcement of repairs on the fiber-optic cable off Syria's Mediterranean coast "confirms" that a **Russian** deep sea exploration vessel spotted sailing in the area "is either **already spying on this internet cable or will be in the future**." The organization cited an unnamed security expert as saying that the Russian ship will likely route the maritime cable through the Russian naval base in Tartous, allowing Moscow "to eavesdrop on internet communications between Syria and the rest of the World Wide Web." Questions have been raised over the presence of the Russian oceanographic research vessel Yantar near an undersea fiber-optic cable providing internet to Syria.

Return to Table of Contents/ Retour à la table des matières

Asia/Asie

Singapore using cyber diplomacy as weapon against cybercrimes
Straits Times, Lim Yan Liang, 2016 10 24
Singapore - What more can Singapore do in a digital world where dependence on technology trades security for greater efficiency and connectivity? With more countries using technology as a component of military response, the first thing to do is to treat the threat as seriously as a conventional one. To this end, **Singapore has been deploying 'cyber diplomacy' - building alliances with other countries, both to swop expertise, such as the latest in attack methods**, and to regularly exercise and test its defences. **Singapore's Cyber Security Agency (CSA) has signed bilateral cyber agreements with five countries: France, the UK, India, the Netherlands and the US.** The agreement with the US, signed in August, is the first cyber agreement between an Asean nation and the US. This opens the door to regular exchanges on cyber issues and effectively gives Singapore a voice when the larger countries try to shape global cyber norms, according to experts.

Intelligence wing in State needs to be strengthened
The Hindu, Special Correspondent, 2016 10 21
Bengaluru - Chief **Minister Siddaramaiah said the intelligence wing of the State needs to be strengthen for better law and order maintenance**. Addressing the investiture ceremony at Rajbhavan on Thursday, Mr. Siddaramaiah said the staff deputed to the intelligence wing are not trained to gather and analyse intelligence inputs. Merely collecting media reports is not intelligence, he said, adding that the staff should analyse and update the State about what could happen rather than focussing on what has already happened. He directed the Home department to provide exclusive training to selected staff for the job. Many police personnel who were not fit or trained were deputed to the intelligence wing.

'Attacks' test coordination of security agencies
Straits Times, Tiffany Fumiko Tay, Danson Cheong, 2016 10 20
Singapore - Under cover of darkness, the "terrorists" sneaked into Singapore on speedboats on Monday night and launched multiple attacks. Armed with rifles, grenades and explosive vests, they hit the Marina Country Club in Punggol first before fanning out across the island. They later struck almost simultaneously at shopping malls in Tampines and Bishan, killing civilians at will. These attacks set the scene for the **simulated terror incident faced by security agencies** over the last two days, in the largest counter-terrorism exercise held here so far. Led by the police, the 18-hour islandwide operation that began on Monday morning involved almost 2,500 officers from the **Home Team, 660 Singapore Armed Forces** (SAF) soldiers and about 60 community volunteers. The officers responded to attack scenarios at six different locations.

House agrees to expand military role in terror fight
The Jakarta Post, Nurul Fitri, 2016 10 21
Jakarta— After months of debate over a plan to strengthen military involvement in **counterterrorism measures**, the House of Representatives on Thursday **approved six conditions under which soldiers could step in and arrest assailants**. The new role, which will be included in the Terrorism Law revision, will go beyond what is mandated in the **Indonesian Military (TNI) Law**, which only allows soldiers to assist terrorism operations under the command of the National Police. If the proposal goes to the plenary session for passage in the next sitting session next month, the TNI will be allowed to launch their own operations in terrorism attacks involving the president, vice president and their families; Indonesian citizens

abroad; Indonesian Embassies; Indonesian ships and airplanes and foreign ships and airplanes in the country's territory. It will also allow the military to step in if a terrorist act extends beyond the country's territory but threatens national sovereignty and security. Another major proposal in the bill is to **assign the National Counterterrorism Agency (BNPT) to handle and coordinate all institutions**, including the TNI and police in the operations, from preventive measures, operations and rehabilitation.

Indian, Afghan intelligence agencies supporting terrorism in Pakistan: IB chief
Pakistan Dawn, Sanaullah Khan, 2016 10 19
Islamabad - **Intelligence Bureau (IB) Director General Aftab Sultan**, while speaking in the Senate standing committee meeting on Tuesday, said a large number of terrorists arrested during the last three years had connections with and were **working for the Indian and Afghan intelligence agencies.** "Out of the 865 terrorists arrested during the last three years, a significant number had connections with India's RAW and the Afghan NDS," said the chief of intelligence agency. The IB chief also said that China- Pakistan Economic Corridor (CPEC) is endangered by foreign intelligence agencies and anti-state elements. Replying to a question regarding missing persons during the Senate sub-committee's meeting, Sultan stated that the IB was conducting 478 inquiries for missing persons, out of which 427 inquiries have been completed.

Allegations surrounding ex-opposition chief seem true: spy chief
Yonhap News Agency, Staff reporter, 2016 10 19
Seoul - **Lee Byung-ho, the head of the National Intelligence Service (NIS)**, said Wednesday he believes the memoir written by an ex- foreign minister that is fueling fresh controversy related to Moon Jae-in, former head of the main opposition Minjoo Party of Korea, is based on facts. Moon has been accused by the ruling bloc of allegedly playing a part in contacting Pyongyang and getting feedback that was reflected in Seoul's decision-making process as revealed in the book. Lee said he can "neither confirm nor deny" that there is evidence that backs up the claims made in the book. "It is not the right time to speak on the matter, considering the case's impact on national security," **the NIS head** was quoted as saying by lawmakers during the parliamentary audit which took place at its headquarters.

This Former C.I.A Official Thinks North Korea Could Be A Big Threat To The U.S.
Fortune, Madeline Farber, 2016 10 19
New York - After spending more than 20 years in the **Central Intelligence Agency, Jami Miscik** knows a thing or two about foreign relations. During an interview at Fortune's Most Powerful Women Summit on Tuesday, she gave a harsh warning to whomever is sworn in as president in January: Don't underestimate North Korea's nuclear power. "North Korea is one of the issues that we aren't paying enough attention to," she said.

Return to Table of Contents/ Retour à la table des matières

Africa/Afrique

Top spy to head telecoms regulator
The Zimbabwe Independent, 2016 10 20
Harare— In a move calculated to control cyberspace and facilitate spying on citizens, government has consolidated its grip on the telecommunications sector by appointing a senior

Central Intelligence Organisation (CIO) officer as the director-general of the Postal and Telecommunications Regulatory Authority of Zimbabwe (Potraz). Potraz this week announced that **Gift Kallisto Machengete**, who is a director of finance and administration in the President's Office, has been appointed head of the telecommunications regulatory body. The development comes at a time the government has been desperately trying to control the use of the internet and social media in the wake of growing discontent over deepening socio-economic hardships.

L'Algérie plaide en faveur d'une convention internationale globale pour éradiquer le terrorisme
All Africa, Journaliste maison, 2016 10 19
Tachkent, Uzbekistan - **L'Algérie a plaidé, par la voix du secrétaire général du ministère des Affaires étrangères, Hassane Rabehi, mercredi à Tachkent, en faveur de l'adoption d'une convention internationale "globale" afin d'éradiquer le terrorisme**. Intervenant à l'occasion de la 43ème session du Conseil des ministres des Affaires étrangères de l'Organisation de la Coopération islamique (OCI), dont les travaux ont débuté mardi dans la capitale ouzbek, M. Rabehi a insisté sur "l'importance d'adopter des mécanismes de lutte efficaces, à savoir une convention internationale globale ainsi que la mise en oeuvre des instruments déjà existants, notamment la convention de l'OCI sur le terrorisme et la stratégie internationale des Nations unies en la matière.

Return to Table of Contents/ Retour à la table des matières

Americas/Amériques

Microsoft to show code in Brazil to calm fears about spy 'back doors'
Reuters, Staff report, 2016 10 20
Brasilia - Microsoft Corp, still stung by accusations that it installed "back doors" for the U.S. government to access customers' communications, opened a center in Brazil on Wednesday where officials will be able to inspect its programming code, in an attempt to allay suspicions in the region that its software programs are **vulnerable to spying**. Behind reinforced walls and with strict security settings, the world's biggest software company showed off its fourth 'Transparency Center' in Brasilia, where experts from Latin American and Caribbean governments will be able to view the source code of its products. The effort to build trust follows heightened suspicions in the region after former **U.S. National Security Agency** contractor **Edward Snowden** leaked documents in 2013 that showed the agency was capturing massive amounts of data from emails handled by major U.S. technology companies, including Microsoft. The leak, in addition to another Snowden disclosure that the United States had been spying on communications including those of former Brazilian President Dilma Rousseff, prompted Brazil and other governments around the world to reconsider how much they could trust U.S. technology companies not to install back doors at the request of **U.S. intelligence agencies**. At the new site, visited on Wednesday by officials including the speaker of Brazil's Congress, no electronics will be allowed into the secure viewing room.

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

26-10-2016 to/au 01-11-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

New anti-terrorism bill abandons Liberal call for real-time parliamentary 'oversight' into CSIS operations
Ottawa Citizen, Ian McLeod, 2016 10 30
Ottawa - The **cornerstone of the Liberals' promised national security reforms -- parliamentary "oversight" of federal spy activities - would not allow lawmakers to scrutinize the most potentially troubling of those actions until after they're completed, if at all**. The criticism is one of several expected to be voiced this week over **Bill C-22**, which will set up a committee of MPs and senators to monitor the country's spooks. The panel - - whose members will have to pass security checks -- is **intended to police the Canadian Security Intelligence Service (CSIS) and 16 other federal entities with national security responsibilities**, many of which now operate without independent scrutiny. Its mandate also extends to examining the "legislative, regulatory, policy, administrative and financial framework for national security and intelligence." The Commons public safety committee begins public hearings on the bill Tuesday. While national security experts praise C-22 for seeking to make spies more accountable, the New Democratic Party is expected to call for at least five significant amendments, starting with the removal of eight exemptions the government can claim to deny committee requests for information.

Extremism 'motivated by jihadist beliefs' top source of Canadian terrorism since 2010, study says
National Post, Stewart Bell, 2016 10 30
Toronto - **Religious extremism has become the top motive for Canadian terrorism, replacing environmentalism, according to an academic study prepared for Public Safety** Canada. While environmentalist causes were the main driver of Canadian terrorist incidents in the 1990s and 2000s, religious motives have taken over the lead since 2010, the study found. Between 2010 and 2015, 29 per cent of terrorist incidents were religiously motivated while 7 per cent were categorized as "anarchist," and 3 per cent were "supremacist." The motives for 61% were unknown. All "religious" terrorism dating back to 2001 was "motivated by jihadist beliefs," said the March 2016 study, obtained by the National Post under the Access to Information Act. The **Canadian Network for Research on Terrorism, Security and Society** conducted the study for the government for officials preparing the **2016 Public Report on the Terrorist Threat to Canada**. "Since their emergence in the 1980s, environmentalist-motivated incidents have been slowly increasing as a proportion of overall terrorist activity," said the study. "This trend shifted, however, in 2010-2015, when religious attacks emerged as the most prominent type of terrorism, along with pockets of anarchist and supremacist activity." The 2010 Ottawa plot to conduct bombings for al-Qaida, the 2013 plot to attack a Toronto-bound passenger train and the 2014 killings of Canadian Forces members by ISIL-inspired terrorists all occurred during that time frame.But in a separate report that was also submitted to Public Safety officials preparing the 2016 threat report, the **federal government's Integrated Terrorism Assessment Centre singled out the Islamic State of Iraq and the Levant**. The de-classified document said that in Canada, Australia, the United States and Western Europe, "the greatest threat comes from individuals inspired and directed by ISIL

Media Coalition and Civil Liberties Groups Granted Say in VICE Case Against RCMP
Vice News Canada, Tamara Khandaker, 2016 10 28

Ottawa - An **Ontario judge ruled Thursday that a media coalition and two civil liberties organizations can intervene on behalf of a VICE Canada journalist, as he fights a production order filed by the RCMP**. VICE will be back in court in February, fighting a previous ruling that ordered national security reporter **Ben Makuch** to hand over Kik messenger chat logs between him and an alleged ISIS fighter. Thursday's ruling means that they'll have back-up. The judge granted intervener status for all three parties, despite opposition from the Crown, which argued that they were duplicating arguments and raising new issues that would shift the focus away from VICE's appeal. But Justin Safayeni, lawyer for the coalition, argued the case would have a broad impact on the rights of all media in Canada. Safayeni is representing eight organizations including the CBC, the Canadian Media Guild, and Canadian Journalists for Free Expression.

Canada, US Top Border Officials Meet to Discuss Security
Sputnik, Staff report, 2016 10 28
Washington - Top **Canadian and US security officials met in Ottawa to discuss information sharing to protect the join border while promoting trade, Canadian Minister of Public Safety and Emergency Preparedness Ralph Goodale said** in a news release. US **Secretary of Homeland Security Jeh Johnson** and Goodale claimed the US-Canadian border has achieved significant progress on a wide range of initiatives to facilitate trade and travel. "We talked about progress on...initiatives such as Entry/Exit and information sharing for the purposes of national security," Goodale said in the release on Thursday.

RCMP launches new "terrorism awareness guide"
Montreal Gazette, Catherine Solyom, 2016 10 27
Montreal - With a level of detail unheard of from law enforcement, **the RCMP's new "Terrorism and Violent Extremism Awareness Guide (www.rcmp- grc.gc.ca) " tackles everything from how to see whether your kids are becoming radicalized online,** to how to check for signs of explosive testing: look for dead plants and unusual corrosion in the sink. Destined for parents, teachers, colleagues and friends of people at risk of becoming radicalized to violence, the guide includes a whole section on "indicators" of radicalization for police use as well, whether it's of the right-wing, left-wing or Islamist variety. Among things to look out for: Suspicious use of the Internet. The guide asks: "Does my child have several accounts on social media and does he/she use different identities in a specific network?" Signs he or she may be planning to travel to a conflict area: Accessing information on obtaining multiple passports, selling personal belongings.

Terrorisme et radicalisation La GRC lance un guide de prévention
La Presse canadienne, Stéphanie Marin, 2016 10 27
Montréal - La **Gendarmerie royale du Canada (GRC) a lancé mercredi un guide de prévention du terrorisme et de la radicalisation menant à la violence, destiné aux parents, aux enseignants et aux proches des personnes à risque**. Le guide, intitulé «**Guide de sensibilisation au terrorisme et à l'extrémisme violent»,** vise à les aider à mieux comprendre et à reconnaître le phénomène de la radicalisation. «Il n'existe aucun profil type du terroriste», prévient-on d'emblée. Mais pour identifier les personnes à risque, il énonce, entre autres choses, les signes avant-coureurs de radicalisation et ceux de la planification d'un attentat. Il discute également du rôle de l'internet et de la propagande. «En plus de diffuser de la propagande haineuse, internet donne accès à des conseils tactiques pour déjouer la sécurité. Il devient un camp d'entraînement virtuel et peut aider à la préparation d'attentats», est-il expliqué dans le guide de 135 pages.

RCMP crafts strategy for returning terrorists
National Post, Stewart Bell, 2016 10 27
Ottawa - Foreseeing a possible "flood of foreign fighters" from Syria, the **RCMP has circulated a strategy that involves trying to understand the returning fighters' intentions and working with communities.** The plan calls for monitoring the social media activity of the returnees, placing them on the no-fly list and asking Passport Canada to revoke their travel documents and flag their future passport applications. The RCMP has also compiled a list of indicators to ascertain the "future posture" of returning fighters that includes whether they are employed, married, "raising funds linked to a little-known charity" or "proselytizing." The "range of responses" for dealing with returnees who have received terrorist training abroad or taken part in foreign conflicts is outlined in a report obtained by the National Post under the Access to Information Act.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

A Veteran Spy Has Given the FBI Information Alleging a Russian Operation to Cultivate Donald Trump
Mother Jones, David Corn, 2016 11 01
San Francisco - On Friday, **FBI Director James Comey** set off a political blast when he informed congressional leaders that the bureau had stumbled across emails that might be pertinent to its completed inquiry into Hillary Clinton's handling of emails when she was secretary of state. On Sunday, **Senate Minority Leader Harry Reid upped the ante. He sent Comey a fiery letter saying the FBI chief may have broken the law and pointed to a potentially greater controversy**: "In my communications with you and other top officials in the national security community, it has become clear that you possess explosive information about close ties and coordination between Donald Trump, his top advisors, and the Russian government...The public has a right to know this information." A **former senior intelligence officer for a Western country who specialized in Russian counterintelligence tells Mother Jones that in recent months he provided the bureau with memos, based on his recent interactions with Russian sources, contending the Russian government has for years tried to co-opt and assist Trump--and that the FBI requested more information from him.** Does this mean the FBI is investigating whether Russian intelligence has attempted to develop a secret relationship with Trump or cultivate him as an asset? Was the former intelligence officer and his material deemed credible or not? An FBI spokeswoman says, "Normally, we don't talk about whether we are investigating anything." But a senior US government official not involved in this case but familiar with the former spy tells Mother Jones that he has been a credible source with a proven record of providing reliable, sensitive, and important information to the US government. In June, the former Western intelligence officer--who spent almost two decades on Russian intelligence matters and who now works with a US firm that gathers information on Russia for corporate clients--was assigned the task of researching Trump's dealings in Russia and elsewhere, according to the former spy and his associates in this American firm.

FBI's Comey opposed naming Russians, citing election timing: Source
CNBC, Eamon Javers, 2016 11 01
Washington - **FBI Director James Comey argued privately that it was too close to Election Day for the United States government to name Russia as meddling in the U.S. election and ultimately ensured that the FBI's name was not on the document that the U.S.**

government put out, a former bureau official tells CNBC. The official said some government insiders are perplexed as to why Comey would have election timing concerns with the Russian disclosure but not with the Huma Abedin email discovery disclosure he made Friday. In the end, the Department of Homeland Security and The Office of the Director of National Intelligence issued the statement on Oct. 7, saying: "The U.S. intelligence community is confident that the Russian Government directed the recent compromises of emails from U.S. persons and institutions, including from U.S. political organizations. ... These thefts and disclosures are intended to interfere with the U.S. election process."

Investigating Donald Trump, F.B.I. Sees No Clear Link to Russia
New York Times, Eric Lichtblau, Steven Lee Myers, 2016 11 01
Washington - For **much of the summer, the F.B.I. pursued a widening investigation into a Russian role in the American presidential campaign**. Agents scrutinized advisers close to Donald J. Trump, looked for financial connections with Russian financial figures, searched for those involved in hacking the computers of Democrats, and even chased a lead -- which they ultimately came to doubt -- about a possible secret channel of email communication from the Trump Organization to a Russian bank. **Law enforcement officials say that none of the investigations so far have found any conclusive or direct link between Mr. Trump and the Russian government.** And even the hacking into Democratic emails, F.B.I. and intelligence officials now believe, was aimed at disrupting the presidential election rather than electing Mr. Trump. Hillary Clinton's supporters, angry over what they regard as a lack of scrutiny of Mr. Trump by law enforcement officials, pushed for these investigations. In recent days they have also demanded that James B. Comey, the director of the F.B.I., discuss them publicly, as he did last week when he announced that a new batch of emails possibly connected to Mrs. Clinton had been discovered.

Hackers reveal apparent targets of NSA cyber espionage
The Hill, Joe Uchill, 2016 10 31
Washington - The **hacker or hackers who stole National Security Agency-built cyber tools have dumped new files in what appears to be yet another change of plans in monetizing the heist**. The new files provide some insight into the targets of the NSA-affiliated hacking team called The Equation Group. Those targets include government servers in China and universities in Pakistan and Saudi Arabia. This is the second dump of files that came from the group The **ShadowBrokers**, who in August released sample files containing previously unknown hacking techniques used to circumvent popular security hardware. The August files also contained a tracking code used by the NSA that matched previously unreleased Edward Snowden documents, appearing to confirm the breach's provenance. In August, the group offered the complete cache of documents for auction. Not seeing the bidding totals they wanted, the group changed to a crowdfunding approach, saying it would release all files publicly if enough people donated money to a bitcoin address.

South African Spy Company Used by Gadaffi Touts its NSA-Like Capabilities
The Intercept, Jenna McLaughlin, 2016 10 31
Washington - The **South African company best known for selling Muammar Gaddafi's regime spy equipment used to monitor millions of Libyans' international phone calls is now claiming it can intercept communications on a scale that rivals a government spy agency**, according to a company brochure obtained by The Intercept. In a 2016 pamphlet produced by VASTech SA Pty Ltd., the company outlines its current capabilities for governments, militaries, and law enforcement agencies around the world, claiming it can conduct "passive detection" of communications transmitted from satellites, fix-and-mobile phones, and fiber optic cable.

When the FBI Has a Phone It Can't Crack, It Calls These Israeli Hackers
The Intercept, Kim Zetter, 2016 10 31
Washington - Earlier this year, at the height of a very **public battle between the FBI and Apple** over whether the computer maker would help decrypt a mass murderer's locked iPhone, it appeared that a little-known, 17-year-old Israeli firm named **Cellebrite Mobile Synchronization** might finally get its moment in the spotlight. After weeks of insisting that only Apple could help the feds unlock the phone of San Bernardino killer Syed Rizwan Farook, the Justice Department suddenly revealed that a third party had provided a way to get into the device. Speculation swirled around the identity of that party until an Israeli newspaper reported it was **Cellebrite. It turns out the company was not the third party that helped the FBI**. A Cellebrite representative said as much during a panel discussion at a high-tech crimes conference in Minnesota this past April, according to a conference attendee who spoke with The Intercept. And sources who spoke with the Washington Post earlier this year also ruled out Cellebrite's involvement, though Yossi Carmil, one of Cellebrite's CEOs, declined to comment on the matter when asked by The Intercept. But the attention around the false report obscured a bigger, more interesting truth: Cellebrite's researchers have become, over the last decade, the FBI's go-to hackers for mobile forensics.

Agents Cleared to Scrutinize Email Cache
New York Times, Multiple reporters, 2016 10 31
Washington - **Federal investigators have obtained a warrant to begin searching a large cache of emails belonging to a top aide to Hillary Clinton**, law enforcement officials said on Sunday, as prosecutors and F.B.I. agents scrambled under intense public pressure to assess their significance before **Election Day**. **It remains unclear whether they can finish their work by then.** "The process has begun," a federal law enforcement official said. The hurried pace at the Justice Department and the F.B.I. raises the prospect that law enforcement officials will again publicly discuss a continuing investigation involving a presidential candidate in the final days of the campaign. The F.B.I. director, **James B. Comey**, has faced extraordinary criticism since he sent an ambiguous letter to congressional leaders telling them that agents had discovered new emails. Agents in an unrelated investigation of Anthony D. Weiner, the disgraced former congressman, found the emails, belonging to his estranged wife, Huma Abedin, the aide to Mrs. Clinton, this month.

FBI agents waited weeks to tell Comey about emails possibly relevant to Clinton probe
Washington Post, Multiple reporters, 2016 10 31
Washington - **FBI agents investigating Hillary Clinton's use of a private email server while secretary of state knew early this month that messages recovered in a separate probe might be germane to their case, but they waited weeks before briefing the FBI director**, according to people familiar with the case. Director **James B. Comey** has written that he was informed of the development Thursday, and he sent a letter to legislators the next day letting them know that he thought the team should take "appropriate investigative steps designed to allow investigators to review these emails." That missive ignited a political firestorm less than two weeks before the election. Almost instantly, Comey came under intense criticism for his timing and for bucking the Justice Department's guidance not to tell Congress about the development. And his announcement means that Clinton could have to contend with the news that the FBI has resumed its investigation of her use of a private email server -- without any clarity on whether its investigators will find anything significant -- up to and beyond Election Day.

Inside Evan McMullin's 10 years undercover in the CIA
Washington Post, Josh Rogin, 2016 10 31

Column - Conservative independent presidential candidate **Evan McMullin** is rising in the polls and stands a fair chance of stealing the red state of Utah from GOP nominee Donald Trump. So it's no surprise that pro- Trump Republicans and others are raising questions about his record as an undercover CIA officer. **Vetting a former spy for the nation's highest office isn't easy, considering the classified nature of his government service**. This has left McMullin vulnerable to attacks he cannot publicly address. But I interviewed six former CIA officers who worked with McMullin during his 10 years inside the agency. What emerged was a picture of a young case officer who volunteered for duty in the world's most dangerous places and had a unique talent for recruiting members of extremist organizations as assets. Kevin Hulbert, a former senior CIA official in the directorate of operations who worked with McMullin overseas, told me that McMullin's steady personality, honesty and work ethic reassured potential intelligence sources who were risking their lives to help the United States. "People who would be assets were drawn to that type of person. They needed to trust that he wouldn't get them killed," Hulbert said. "There were a lot of people who took an easier route at the agency. Evan was always in the middle of the fight."

Why FBI director James B. Comey was able to defy Justice bosses on Clinton email announcement
Washington Post, Sari Horwitz, 2016 10 31
Washington - **Justice Department officials could have overruled FBI Director James B. Comey's surprising decision to notify Congress about the renewed investigation into Hillary Clinton's email server, but they stopped short of ordering him to back down**. Their decision partly reflected the institutional power of the FBI director, Comey's personality and the political realities they were facing, according to current and former Justice officials. In this case, officials said Comey put the department in an untenable position by informing them that he was sending a letter to Congress because he had an obligation to lawmakers or they would feel misled. "At the end of the day, if you have the FBI director telling Justice that he has an obligation to tell Congress, there is no way you can direct the FBI to do otherwise," said one official, who spoke on the condition of anonymity. "That's too fraught. You can't direct someone to withhold information from Congress. That's not a prudent way to do things."

James Comey is a good man, but he made a serious mistake
Washington Post, Former Attorney General Eric Holder, 2016 10 31
Op-ed - I began my career in the Justice Department's Public Integrity Section 40 years ago, investigating cases of official corruption. In the years since, I have seen America's justice system firsthand from nearly every angle -- as a prosecutor, judge, attorney in private practice, and attorney general of the United States. I understand the gravity of the work our Justice Department performs every day to defend the security of our nation, protect the American people, uphold the rule of law and be fair. That is why **I am deeply concerned about FBI Director James B. Comey's decision to write a vague letter to Congress about emails potentially connected to a matter of public, and political, interest**. That decision was incorrect. It violated long-standing Justice Department policies and tradition. And it ran counter to guidance that I put in place four years ago laying out the proper way to conduct investigations during an election season. Indeed, except in exceptional circumstances, the department will not even acknowledge the existence of an investigation. The department also has a policy of not taking unnecessary action close in time to Election Day that might influence an election's outcome. These rules have been followed during Republican and Democratic administrations. They aren't designed to help any particular individual or to serve any political interest. Instead, they are intended to ensure that every investigation proceeds fairly and judiciously; to maintain the public trust in the department's ability to do its job free of political influence; and to prevent investigations from unfairly or unintentionally casting public suspicion on public officials who

have done nothing wrong. Director Comey broke with these fundamental principles. I fear he has unintentionally and negatively affected public trust in both the Justice Department and the FBI. **I served with Jim Comey and I know him well. This is a very difficult piece for me to write. He is a man of integrity and honor. I respect him. But good men make mistakes. In this instance, he has committed a serious error with potentially severe implications**.

The FBI Director's Unworthy Choice
Wall Street Journal, Former Attorney General Michael B. Mukasey, 2016 10 31
Op-ed - We need not worry unduly about the factual void at the center of the FBI director's announcement on Friday that the bureau had found emails -- perhaps thousands -- "pertinent" in some unspecified way to its investigation into Hillary Clinton's handling of classified emails while she was secretary of state. True, **we don't know what is actually in the emails of Huma Abedin, Mrs. Clinton's close aide, but we can nonetheless draw some conclusions about how FBI Director James Comey came to issue his Delphic notice to Congress**, and what the near-term future course of this investigation will be. Regrettably, those conclusions do no credit to him, or to the leadership of the Justice Department, of which the FBI is a part. Friday's announcement had a history. Note: Mr. Mukasey served as U.S. attorney general (2007-09).

The spy who couldn't spell: how the biggest heist in the history of US espionage was foiled
The Guardian (London), Yudhijit Bhattacharjee, 2016 10 30
Washington - One Monday morning in December 2000, **FBI Special Agent Steven Carr** hurried out of his cubicle at the bureau's Washington DC field office and bounded down two flights of stairs to **pick up a package that had just arrived by FedEx from the FBI's office in New York**. Carr was 38, thoughtful and intense, meticulous in his work. Carr raced back to his desk and laid out the contents of the package in front of him: a sheaf of papers running into a few dozen pages. They were from three envelopes that had been handed to the FBI by a confidential informant at the Libyan consulate in New York. The envelopes had been individually mailed to the consulate by an unknown sender. Breathlessly, Carr thumbed through the sheets. Based on directions sent from New York, he was able to sort the papers into three sets, corresponding to the three envelopes. All three had an identical cover sheet, at the top of which was a warning in all caps. "THIS LETTER CONTAINS SENSITIVE INFORMATION." In the first envelope was a four-page letter with 149 lines of typed text consisting of alphabets and numbers. The second envelope included instructions on how to decode the letter. The third envelope included two sets of code sheets. One set contained a list of ciphers. The other, running to six pages, listed dozens of words along with their encoded abbreviations: a system commonly known as brevity codes. Together, the two sets were meant to serve as the key for the decryption. Carr flipped through the letter, skimming the alphanumeric sequence. It looked like gibberish. There was no way to make sense of it without the code sheets and the decoding instructions. By mailing the three separately, the sender had sought to secure the communication against the possibility that one envelope might get intercepted by a US intelligence agency. **Carr had never seen anything like it before. The sender of the envelopes was no doubt a bona fide member of the US intelligence community, with access to "top secret" documents, intent on establishing a clandestine relationship with a foreign intelligence service.** The person had, in fact, already committed espionage by giving classified information to an enemy country. Carr might as well have been looking at a warning sign for a national security threat flashing in neon red.

James Comey broke with Loretta Lynch and Justice Department tradition
The New Yorker, Jane Mayer, 2016 10 30

Washington - On Friday, **James Comey, the director of the Federal Bureau of Investigation, acting independently of Attorney General Loretta Lynch, sent a letter to Congress saying that the F.B.I. had discovered e- mails that were potentially relevant to the investigation of Hillary Clinton's private server.** Coming less than two weeks before the Presidential election, Comey's decision to make public new evidence that may **raise additional legal questions about Clinton was contrary to the views of the Attorney General, according to a well-informed Administration official. Lynch expressed her preference that Comey follow the department's longstanding practice of not commenting on ongoing investigations**, and not taking any action that could influence the outcome of an election, but he said that he felt compelled to do otherwise. Comey's decision is a striking break with the policies of the Department of Justice, according to current and former federal legal officials. Comey, who is a Republican appointee of President Obama, has a reputation for integrity and independence, but his latest action is stirring an extraordinary level of concern among legal authorities, who see it as potentially affecting the outcome of the Presidential and congressional elections. "You don't do this," one former senior Justice Department official exclaimed. "It's aberrational. It violates decades of practice."

The NSA deputy chief on Edward Snowden's true motivations
Washington Post Magazine, Joe Heim, 2016 10 30
Interview - **Richard Ledgett Jr., 58, has worked at the National Security Agency since 1988**. He and his wife live in Maryland and have three children. Washington Post: If (Edward) Snowden were sitting across from you, what would you say? Richard Ledgett: I'd ask him, Why did you do what you did? The narrative that he's told publicly about this actually doesn't track if you parse the timelines. **He says he was motivated by Jim Clapper's remarks to Senator Wyden and the revelation that those remarks weren't accurate**. If you look at the timeline, Snowden was actually stealing material and in contact with reporters eight months before that, so that doesn't track. Q: So even if the timeline doesn't scan, do you question his motivation? A: I do. I know a lot about this. I probably spent more time than anybody but our chief investigator on the actual investigation on this. I know a lot that I still can't talk about because it's sensitive investigational stuff. And if he does ever come back to the United States it will be part of the government's case against him. The things that I can say, I think a lot of what was in the House Intelligence Committee's report where they talk about him actually being mad about being disciplined -- I think that actually tracks more with motivation. Q: Do you think history will ultimately decide what Snowden did helped the country? A: That's a really hard one. I think if you weigh the benefit and the harm, the balance comes out pretty far on the harm side. That doesn't mean that there was absolutely no good to what he did. And I think that's an important nuance. It's heavily weighted towards harm. The little bit of good is forcing a conversation that we probably should have had earlier. And for me that was a lesson learned. That we should have talked about the particular authority, the Patriot Act authority, earlier in the process

N.S.A. Appears to Have Missed 'Big Red Flags' in Suspect's Behavior
New York Times, Scott Shane, 2016 10 30
Washington - **Year after year, both in his messy personal life and his brazen theft of classified documents from the National Security Agency, Harold T. Martin III put to the test the government's costly system for protecting secrets**. And year after year, the system failed. Mr. Martin got and kept a top-secret security clearance despite a record that included drinking problems, a drunken-driving arrest, two divorces, unpaid tax bills, a charge of computer harassment and a bizarre episode in which he posed as a police officer in a traffic dispute. Under clearance rules, such events should have triggered closer scrutiny by the security agencies where he worked as a contractor. Yet **even after extensive leaks by Pfc. Bradley Manning in 2010 and Edward Snowden in 2013 prompted new layers of safeguards, Mr.**

Martin was able to walk out of the N.S.A. with highly classified material, adding it to the jumbled piles in his house, shed and car. A federal judge in Baltimore ruled on Friday that Mr. Martin, 51, must remain jailed on charges of stealing government documents and mishandling classified information over two decades. Prosecutors say they will add new charges under the Espionage Act. Mr. Martin, whose arrest in August was disclosed by The New York Times this month, has admitted to taking the material but denies giving secrets to anyone else.

Judge denies request to release ex-NSA contractor accused of stealing data
Washington Post, Ellen Nakashima, 2016 10 29
Baltimore - An **attorney for the former National Security Agency contractor accused of stealing unprecedented amounts of classified government data** said at a hearing Friday that his client has a compulsive hoarding habit that runs in the family and should not continue to be detained. But **U.S. District Judge Richard D. Bennett declined a request that Harold T. Martin III be released from jail,** ruling that he was a flight risk. Bennett affirmed a magistrate judge's ruling from last week that Martin continue to be detained pending an eventual trial or resolution of the case. The former contractor was arrested Aug. 29 at his home in Glen Burnie, Md., and charged in a sealed complaint with felony theft of government property and the unauthorized removal of classified materials, a misdemeanor.

F.B.I. Chief James Comey Is in Political Crossfire Again Over Emails
New York Times, Multiple Reporters, 2016 10 29
Washington - **James B. Comey, the director of the F.B.I., faced a dilemma on Thursday when deputies briefed him about a new trove of emails**, discovered in the course of an investigation of former Representative Anthony D. Weiner, that they said might be connected to the dormant inquiry into Hillary Clinton's private email server. Mr. Comey, who had cleared Mrs. Clinton of any criminal wrongdoing in the email affair this summer, could let Congress know about the new developments immediately, bureau officials said, an unusual step that would risk accusations that he was unfairly harming Mrs. Clinton's presidential campaign less than two weeks before the election. Or he could delay any announcement and examine the new emails more closely, risking criticism that he had suppressed important new information if it came out after the election, despite his pledges of "transparency" in the investigation. Mr. Comey, a Republican appointed by President Obama three years ago, decided that he could live with criticism of his judgment, aides said. So **on Friday morning, the F.B.I.'s congressional liaison emailed a letter from the director to the chairmen of eight congressional committees -- virtually ensuring that it would be quickly publicized by eager Republicans**.

Booz Allen Hamilton hires former FBI director to review its security measures
Baltimore Sun, Ian Duncan, 2016 10 28
Baltimore - **Booz Allen Hamilton**, a major intelligence community contractor, **said Thursday that it has hired a former FBI director to review its security measures after one of its employees was with charged with stealing reams of classified documents. Harold T. Martin III**, who used to work for the NSA, was arrested in August, accused of a two-decade theft spree and stashing data that could amount to the equivalent of half a billion pages at his Glen Burnie home. Craig Veith, a spokesman for Booz Allen, said former **FBI director Robert Mueller had started a review of its "security, personnel, and management processes and practices"** on Oct. 19. In a federal court filing on Thursday, prosecutors said classified information stolen by Martin included the names of covert intelligence officers. In arguing that Martin should remain locked up, federal prosecutors said in their filing that a "substantial portion" of the 50 terabytes of digital information seized from Martin at his home was "highly classified." That information included the names of intelligence officers who operate "under

cover outside the United States" and could endanger their lives, the safety of those they work with and could **compromise American intelligence operations**.

How Snowden Smartened Up Our Spying
Newsweek, Jack Goldsmith, 2016 10 28
Column - At **the dawn of the Snowden revelations, many wondered whether the U.S. intelligence community would be destroyed**. Some hoped that it would. But the opposite has happened: Despite **undoubted intelligence losses**, new collection barriers and diplomatic embarrassments, the community has emerged as a stronger organization despite, indeed because of, Snowden. Snowden forced the intelligence community out of its suboptimal and unsustainable obsession with secrecy. "Before the unauthorized disclosures, we were always conservative about discussing specifics of our collection programs, based on the truism that the more adversaries know about what we're doing, the more they can avoid our surveillance," **Director of National Intelligence James Clapper** said in 2013. Post-Snowden, the intelligence community operates on the principle that secrecy is not an absolute value, but one that needs to be traded off for other values, including domestic legitimacy. Snowden made it realize that, in the words of **former NSA Director Michael Hayden**, "although the public cannot be briefed on everything, there has to be enough out there so that the majority of the population believe what they are doing is acceptable.". Note: Jack Goldsmith is a senior fellow at the Hoover Institution and the Henry L. Shattuck professor of law at Harvard University. From 2003 to 2004, he served as the assistant attorney general, Office of Legal Counsel. From 2002 to 2003, he served as the special counsel to the general counsel of the Department of Defense.

When CIA and NSA Workers Blow the Whistle, Congress Plays Deaf
The Intercept, Patrick G. Eddington, 2016 10 27
Comment - **Do the committees that oversee the vast U.S. spying apparatus take intelligence community whistleblowers seriously?** Do they earnestly investigate reports of waste, fraud, abuse, professional negligence, or crimes against the Constitution reported by employees or contractors working for agencies like the CIA or NSA? **For the last 20 years, the answer has been a resounding "no." My own experience in 1995-96 is illustrative**. Over a two-year period working with my wife, Robin (who was a CIA detailee to a Senate committee at the time), we discovered that, contrary to the public statements by then-Chairman of the Joint Chiefs Colin Powell and other senior George H. W. Bush administration officials (including CIA Director John Deutch), American troops had in fact been exposed to chemical agents during and after the 1991 war with Saddam Hussein. While the Senate Banking Committee under then-Chairman Don Riegle, D-Mich., was trying to uncover the truth of this, officials at the Pentagon and CIA were working to bury it. At the CIA, I objected internally -- and was immediately placed under investigation by the CIA's Office of Security. That became clear just days after we delivered the first of our several internal briefings to increasingly senior officials at the CIA and other intelligence agencies. In February 1995, I received a phone call from CIA Security asking whether I'd had any contacts with the media. I had not, but I had mentioned to CIA officials we'd met with that I knew that the CBS newsmagazine "60 Minutes" was working on a piece about the Gulf War chemical cover-up. This call would not be the last I'd receive from CIA Security about the matter, nor the only action the agency would take against us.

CIA to share 11 million declassified documents through agency's website
Washington Times, Andrew Blake, 2016 10 27
Washington - The **CIA this week said it will make more than 11 million declassified documents searchable on the agency's website**. The sizable collection of previously privileged documents currently **resides on a database called the CIA Records Search Tool, or CREST**, and for years has only been accessible by using computers at the National Archives

and Records Administration in College Park, Md. Ryan Trapani, a spokesman for the intelligence agency, told the Federal of American Scientists on Tuesday that CREST documents will soon be uploaded to the CIA's official website, CIA.gov. "When loaded on the website they will be full-text searchable and have the same features currently available on the CREST system at NARA," he said.

Congress: Cuba to Share Critical U.S. Intel With Iranian Spies
Washington Free Beacon, Adam Kredo, 2016 10 27
Washington - **Obama administration efforts to bolster the sharing of critical intelligence data with Cuba is likely to benefit Iran**, which has been quietly bolstering its foothold in the country with the communist government's approval, according to conversations with members of Congress and other sources familiar with the matter. A little noticed Obama administration directive on Cuba, released Oct. 14, instructed the U.S. director of national intelligence to assist and cooperate with Cuba's intelligence services. The directive has raised red flags on Capitol Hill, where some lawmakers are concerned that Cuba will pass along critical U.S. intelligence to the Iranians, who have made moves in recent years to extend their influence in the communist country and other Latin American countries hostile to the United States. The Obama administration's move to share intelligence with Cuba is likely to be celebrated by Iran, according to congressional sources tracking the matter.

Report: Chinese Spies Stole Pentagon Secrets
Washington Free Beacon, Bill Gertz, 2016 10 27
Washington - **Chinese spies repeatedly infiltrated U.S. national security agencies, including official email accounts**, and stole U.S. secrets on Pentagon war plans for a future conflict with China, according to a forthcoming congressional commission report. "The United States faces a large and growing threat to its national security from Chinese intelligence collection operations," states the late draft report of the U.S.-China Economic and Security Review Commission. "**Among the most serious threats are China's efforts at cyber and human infiltration of U.S. national security entities**." Chinese intelligence activities have "risen significantly" in the past 15 years and are conducted through several spy services, including the Ministry of State Security (MSS), the People's Liberation Army (PLA), and Communist Party military organizations such as the PLA General Political Department and the Party's United Front Work Department. A copy of the draft annual report for 2016 was obtained by the Washington Free Beacon. The final report will be released Nov. 16. The report identified repeated infiltrations by Chinese spies of U.S. national security entities, including the FBI and the U.S. Pacific Command.

U.S. has secretly expanded its global network of drone bases to North Africa
Washington Post, Adam Entous, Missy Ryan, 2016 10 26
Washington - The **Pentagon has secretly expanded its global network of drone bases to North Africa, deploying unmanned aircraft and U.S. military personnel to a facility in Tunisia to conduct spy missions in neighboring Libya.** The Air Force Reaper drones began flying out of the Tunisian base in late June and have played a key role in an extended U.S. air offensive against an Islamic State stronghold in neighboring Libya. The Obama administration pressed for access to the Tunisian base as part of a security strategy for the broader Middle East that calls for placing drones and small Special Operations teams at a number of facilities within striking distance of militants who could pose a threat to the West. U.S. officials, speaking on condition of anonymity to discuss an operation that has not been acknowledged, said the drones being flown out of Tunisia were currently unarmed and were principally being used to collect intelligence on Islamic State targets in Sirte, Libya, where the United States has conducted more than 300 airstrikes since August. U**.S. officials said they sought access to**

the air base in Tunisia to close a critical "blind spot" for U.S. and Western intelligence services in North Africa, which has become the Islamic State's largest base of operations outside Syria and Iraq. The region is also home to al-Qaeda-linked fighters.

Denuclearizing N. Korea a 'lost cause,' US intel chief says
Agence France-Presse, Staff report, 2016 10 26
Washington - **Convincing North Korea to abandon nuclear weapons is a "lost cause," America's top intelligence official said**, causing concern in the State Department and ally South Korea over an issue of long-standing US policy. The United States has always maintained it cannot accept North Korea as a nuclear state and, under President Barack Obama, has made any talks with the North conditional on Pyongyang first making some tangible commitment towards denuclearisation. But in remarks to the Council on Foreign Relations think-tank, **US Director of National Intelligence James Clapper** on Tuesday suggested such a policy was based on wishful thinking. "The notion of getting the North Koreans to denuclearize is probably a lost cause.

WikiLeaks 'sowing the seeds of its own destruction' says former NSA chief
International Business Times (UK), James Murdock, 2016 10 26
London - A **former deputy director of the US National Security Agency (NSA), John C Inglis, believes that WikiLeaks - the whistleblowing platform led by Julian Assange - has become "internally confused" in recent years and that "natural forces" may soon wipe it out**. "WikiLeaks might be in fact be sowing the seeds of its own destruction," Inglis told IBTimes UK in an exclusive interview on 25 October, indicating the organisation has overstepped a boundary by leaking material which has the potential to influence the upcoming US presidential election. The US government has namechecked Assange's organisation as being complicit in a Russian-led plot to influence the elections and - allegedly after a close word from US Secretary of State John Kerry - the government of Ecuador, which is hosting Assange under political asylum, was forced to step in.

FBI, Justice Dept. prep for Election Day security concerns
Associated Press, Staff report, 2016 10 26
Washington - The **Justice Department and FBI say they will have officials ready on Election Day to respond to potential crimes, with monitors at select polling places and lawyers and agents who will field complaints regarding voter intimidation, fraud and other problems**. In addition, a centralized command post at FBI headquarters will monitor specific threats reported across the country. A Justice Department statement Tuesday outlining its Election Day response said attorneys from the civil rights and criminal divisions would work to ensure that voters have their ballots "counted free of discrimination, intimidation or fraud in the election process."

Rep. McCaul: I told Trump Russia was behind the hacks, but he thinks there's no proof
Politico, Brent Griffiths, 2016 10 25
Washington - A **top Republican on national security said he advised Donald Trump that Russia was using hacked information to influence the election process, but the GOP presidential nominee didn't appear to believe him**. "I think he has in his mind that there's not the proof," **House Homeland Security Chairman Mike McCaul** said Tuesday during a Texas Tribune event in Austin. "Now he hasn't had the briefing I had, but I made it clear that in my judgment it was a nation-state." McCaul, a Trump supporter, told Tribune CEO Evan Smith that he was brought in to brief Trump on national security after the first presidential debate -- a topic the Texas Republican conceded is "not [Trump's] strength."

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

'There will be terrorist attacks in Britain,' says MI5 chief
The Guardian (London), Paul Johnson, Ewen MacAskill, 2016 11 01
London - Sitting in the office of the president of the Royal Society, where he has just been the surprise guest speaker at its annual diversity conference, (**MI5 director Andrew**)Parker, who has made speeches and appeared once on the BBC Today programme, **has a worldview that centres on three areas of threat.** The **first is Islamic-inspired terror,** which he calls enduring and generational. "International terrorism in its latest shape, based on twisted ideology, brings terror to our streets and most of the developed world, including North America, Australia and Turkey," he says. "Currently, the flavour of it is Daesh, or Isil [Islamic State], and we still have the al-Qaida brand. This is something we have to understand: it's here to stay. It is an enduring threat and it's at least a generational challenge for us to deal with." He says the number of terror plots thwarted in the past three years stands at 12. "That sort of tempo of terrorist plot and attempts is concerning and it's enduring. Attacks in this country are higher than I have experienced in the rest of my career - and I've been working at MI5 for 33 years. The reality is that because of the investment in services like mine, the UK has got good defences. My expectation is that we will find and stop most attempts at terrorism in this country." He lets the word "most" sink in before adding: **"There will be terrorist attacks in this country. The threat level is severe and that means likely."**

MI5 head: 'increasingly aggressive' Russia a growing threat to UK
The Guardian (London), Ewen MacAskill, Paul Johnson, 2016 11 01
London - **Russia poses an increasing threat to the stability of the UK and is using all the sophisticated tools at its disposal to achieve its aims, the director general of MI5** has told the Guardian. In the first newspaper interview given by an incumbent MI5 chief in the service's 107- year history, **Andrew Parker said that at a time when much of the focus was on Islamic extremism, covert action from other countries was a growing danger**. Most prominent was Russia. "It is using its whole range of state organs and powers to push its foreign policy abroad in increasingly aggressive ways - involving propaganda, espionage, subversion and cyber- attacks. Russia is at work across Europe and in the UK today. It is MI5's job to get in the way of that." **Parker said Russia still had plenty of intelligence officers on the ground in the UK, but what was different now from the days of the cold war was the advent of cyberwarfare**.. Said that budget increases would see MI5 expand from 4,000 to 5,000 officers over the next five years. . Rejected criticism that the investigatory powers bill, due before parliament this week, was going too far in enabling intrusive surveillance, arguing that it correctly balances privacy and security. . Dismissed claims that Brexit would affect cooperation with European intelligence services. . Said his aim was to equalise the gender balance in MI5 and recruit many more operatives from ethnic minority backgrounds.

L'espionnage britannique met en garde contre une Russie "agressive"
Le Figaro avec l'Agence France-Presse, Journaliste maison, 2016 11 01
Londres - Le chef **du service de renseignement britannique MI5, Andrew Parker, met en garde, dans une interview au Guardian contre les méthodes "de plus en plus agressives" de la Russie** et son recours aux cyber- technologies pour s'opposer à l'Occident. Moscou, a-t-il expliqué, "s'appuie sur toute sa gamme d'organes étatiques et toute sa puissance pour faire avancer sa politique étrangère de façon de plus en plus agressive, et cela comprend la propagande, l'espionnage, la subversion et les cyber-attaques". "La Russie est à l'oeuvre dans toute l'Europe et au Royaume-Uni. La tâche du MI5 est de lui barrer la route", a-t-il poursuivi. Ces déclarations surviennent une dizaine de jours après qu'une flotte navale russe de huit navires, en route pour les côtes syriennes, a fait l'objet de surveillance en mer du Nord de la part d'une frégate britannique.

Why do we still accept that governments collect and snoop on our data?
The Guardian (London), Scarlet Kim, 2016 10 30
Comment: In recent weeks, the **Hollywood film about Edward Snowden and the movement to pardon the NSA whistleblower have renewed worldwide attention on the scope and substance of government surveillance programs**. In the United States, however, the debate has often been a narrow one, focused on the rights of Americans under domestic law but mostly blind to the privacy rights of millions of others affected by this surveillance. Indeed, just last week, a British court held that **British intelligence agencies acted unlawfully by concealing bulk spying programs from the public for over a decade**. Soon, in a lawsuit brought by Privacy International, the ACLU and eight other organizations, the influential European court of human rights will also weigh in on surveillance programs revealed by Snowden, and the result could have implications far beyond Europe. Although the debate in the US has led to some piecemeal reforms - including the USA Freedom Act and modest policy changes - many of the most intrusive government surveillance programs remain largely intact. These include programs conducted not just by the NSA, but also by its close partner in the United Kingdom, called the **Government Communications Headquarters (GCHQ),** with whom the NSA swaps vast sets of private data. This bulk surveillance violates rights to privacy and freedom of expression - rights that are guaranteed not only under US domestic law, but also under international human rights law. That latter legal framework speaks a universal language, enumerating fundamental rights that every person enjoys by virtue of our common humanity.

'Abandoned' IRA supergrass lay dead in his flat for up to a week
The Belfast Telegraph, Suzanne Breen, 2016 11 01
Belfast— IRA **informer Raymond Gilmour has been found dead in his flat in Kent, where he had been lying abandoned and alone,** for up to a week. An autopsy is being carried out but friends believe that Gilmour (55), who was an alcoholic with serious psychological problems, died from natural causes. He was on disability benefit at the time of his death. His friend and fellow agent, Martin McGartland, last night said: **"It is disgraceful that Ray died in these circumstances. He spent years begging MI5 for financial and psychological help**. Instead, they turned their back on him. He was a broken man, a wreck of a human being, and they left him to die in the Gilmour gave evidence against 31 men and women in one of Northern Ireland's best known republican supergrass trials. After the case collapsed in 1984, he was resettled in England by MI5 and given a new identity.

Confessions of an MI5 agent: 'Isil were planning to behead me - the butcher's knives were ready'
The Telegraph, Tom Ough, 2016 10 29

Analysis: **I'd been in MI5 for a few years when I found myself on the most dangerous mission of my career. I was sent to follow a potential Islamist terrorist in Camden Market**, north London, as part of a surveillance operation. He started on foot, then got into a car. We had planted an eavesdropping device in it, which should have been live-monitored back at Thames House, MI5 headquarters, but there was an incident going on elsewhere and resources had been diverted. What we didn't realise was that the target had guessed he was being followed. He and his friends had planned a snatch - to **kidnap an MI5 agent**. I didn't know it at the time but they had set up a room, in a house they used, with plastic sheeting on the floor, black flags, video cameras and butcher's knives - I believe they wanted to try the kidnappee under Sharia law, then behead him online.

EU security intelligence critical to fighting terror, says senior police officer
The Independent (UK), Ashley Cowburn, 2016 10 27
London - **Access to information in Europe-wide security databases, including the European Arrest Warrant, is "mission critical" in fighting terrorism**, one of Britain's most senior policewomen has said. **Helen Ball, the deputy assistant commissioner at the Metropolitan Police, also indicated that citizens in Europe would be at a greater threat from terrorism if Britain failed to work with its allies on the continent after Brexit**. Ms Ball, who has been with the police force for over two decades, also ranked the European Arrest Warrant as ten out of ten in combating international terrorism. When asked by the Lords' EU Home Affairs sub-committee about the importance of the European Arrest Warrant (EAW) on a scale of 1-10, Ms Ball replied: "At the moment we have very low usage of the European Arrest Warrant and there are very good reasons for that and as I look to the future I suspect we will have greater use of it.

James Bond would fail grade at MI6, says head of intelligence service
Press Association, Staff report, 2016 10 26
London - **James Bond would fail to make the grade if he tried to become a spy today, the head of MI6 has said**. Although the suave fictional secret agent is tenacious and patriotic his morally dubious character would see him rejected by the intelligence service, **Alex Younger** said. In a rare question and answer session, the spy chief insisted that a strong ethical core is one of the main qualities potential recruits need. He told the Black History Month website: " We know that it we undermine British values, even in the name of defending them, then we have failed. Our staff are not from another planet. "They are ordinary men and women operating in the face of complex moral, ethical and physical challenges, often in the most forbidding environments on earth. "**In contrast to James Bond, MI6 officers are not for taking moral shortcuts. In fact, a strong ethical core is one of the first qualities we look for in our staff**. "It's safe to say that James Bond wouldn't get through our recruitment process and, whilst we share his qualities of patriotism, energy and tenacity, an intelligence officer in the real MI6 has a high degree of emotional intelligence, values teamwork and always has respect for the law... unlike Mr Bond."

Return to Table of Contents/ Retour à la table des matières

Australia/ Australie

Australia and China agree to share financial crime intelligence
Reuters, Staff reporter, 2016 11 01

Beijing/Sydney - **Australia and China agreed on Tuesday to share intelligence about potential financial crime as part of a crackdown on cross-border money laundering and terrorism financing**, as Australian Justice Minister Michael Keenan visits Beijing. Keenan told reporters during his visit that he had also raised concerns with Chinese officials over four Australian citizens detained for "gambling crimes" in connection with Crown Resorts but said he did not discuss specifics of the charges. The intelligence sharing agreement between Australian financial intelligence agency **AUSTRAC and its Chinese counterpart CAMLMAC** would allow both countries to target and disrupt organised criminal networks. "The more granularity we can get on the intelligence and the more information that we can share together, the more likely we're able to find the needle in the haystack essentially, which is the bad financial transaction," Keenan said.

Deputy Commissioner Cath Burn keeps control of counter-terrorism operations after NSW police shakeup
ABC (Australia), Jessica Kidd, 2016 11 01
Canberra - **Deputy Police Commissioner Catherine Burn has retained control of counter-terrorism operations as part of a major restructure of the NSW Police Force**. It comes as the number of deputy commissioners is increased from three to five under . Ms Burn previously had responsibility for Specialist Operations, which included Counter Terrorism and Special Tactics, the Special Services Group, Traffic and Highway Patrol Command and the Police Transport Command. Today, a spokeswoman for Commissioner Andrew Scipione confirmed Ms Burn had been appointed the Deputy Commissioner for Counter Terrorism and Investigations. She also confirmed that Deputy Commissioner Dave Hudson would head Specialist Support. The spokeswoman said recruitment was underway for the remaining deputy positions. "An internal recruitment process has started today across NSW Police Force to the roles of Deputy Commissioner Metropolitan Field Operations and Deputy Commissioner Regional NSW Field Operations," she said.

Soviet spy infiltrated ASIO, book reveals
Associated Press, 2016 10 26
Canberra - The **authors behind the official history of Australia's security agency threatened to quit if they weren't allowed to reveal the organisation had been infiltrated by Soviet spies**. Academic John Blaxland and researcher Rhys Crawley were given unfettered access to **ASIO's archives for The Secret Cold War**, the third volume of the series covering 1975 to 1989. But the pair had to fight to include evidence that suggested at least one mole from the **Russian intelligence service** had penetrated the agency for many years, and ASIO's inability to identify it. "This is the part of the story that is, arguably, the most embarrassing to ASIO," Dr Blaxland said following the book's launch at ASIO's Canberra headquarters on Wednesday. "This is a demoralising story. This is a story of failure. This is a story of people spending their life's work and seeing it go to the sand effectively. "But to the credit of ASIO, particularly the director-general, they decided to keep the story of penetration in and explain what happened as best we could up to 1989." They did, however, prevent names and specific details - including the number of suspected moles - from being published for legal and operational reasons.

Return to Table of Contents/ Retour à la table des matières

New Zealand/Nouvelle-Zélande

India-New Zealand can be partners in security, stability: Prez
Press TV News (India), 2016 10 28
New Delhi - **President Pranab Mukherjee has said India and New Zealand can become partners for promoting security**, stability and prosperity in their regions and beyond, as he welcomed visiting **Kiwi Prime Minister John Key**. Key called on the President at RashtrapatiBhavan yesterday. Mukherjee, while welcoming the PM and his delegation, said India values its relationship with his country and the sustained momentum of high level contacts reaffirms the growing strength and dynamism of bilateral engagement between India and New Zealand.. "India and New Zealand can be partners in promoting security, stability and prosperity in the region and beyond. The two countries can work together in areas such as maritime security and ensuring freedom of navigation and in **countering terrorism**," he said.

Return to Table of Contents/ Retour à la table des matières

International

China/Chine

Cyber law aimed at foreign hackers
South China Morning Post, Viola Zhou, 2016 11 01
Beijing - **Beijing has proposed a revised internet law to punish foreigners who hack Chinese websites as it steps up its campaign against cyberattacks it blames on the West.** Although it was hard for governments to identify those behind cybercrimes, the move paved the way for China to take legal action against other states, analysts said. The proposed **cybersecurity law changes** would let the government freeze assets of foreign individuals or groups if they damaged China's key information infrastructure, Xinhua reported. Police would apply "other necessary punishment" to those outside the country who attacked, intruded, disrupted or harmed Chinese websites, according to the revised draft quoted in the report. The draft had been sent to the Standing Committee of the National People's Congress for approval, Xinhua said. China claims to be a victim of global cybercrimes, reporting growing numbers of attacks from overseas every year.

China's draft cybersecurity law gets 3rd reading
Xinhua News Agency, Staff reporter, 2016 10 31
Beijing - **China's draft cybersecurity law was submitted to legislators for its third reading at the bimonthly session of the National People's Congress (NPC) Standing Committee**, which began Monday. The draft allows police and other law enforcers to take measures including freezing assets, against overseas individuals or organizations that "attack, intrude, interfere with or sabotage the nation's key information infrastructure."

Return to Table of Contents/ Retour à la table des matières

Russia/Russie

Kremlin says British spy chief's claims of Russian threat 'unfounded'
Agence France-Presse, 2016 11 01
Moscow— The **Kremlin on Tuesday dismissed as baseless claims by a British intelligence agency chief that Russia is acting in "increasingly aggressive ways" and using new**

technologies against the West. The **head of Britain's MI5 intelligence agency Andrew Parker, on Monday said Russia is "using its whole range of state organs and powers to push its foreign policy abroad in increasingly aggressive ways** -- involving propaganda, espionage, subversion and cyber-attacks." **Kremlin spokesman Dmitry Peskov told reporters Tuesday that Russia "could not agree" with Parker's claims**. "We have repeatedly commented on cyber-attacks: as long as someone does not provide evidence, any statements -- be they by the head of MI5, the president of the United States and other decision-makers -- we will consider unfounded and baseless," Peskov said.

Putin's Top Security Advisor Lays Out Vision of Global Security in 5 Easy Steps
Sputnik, Staff report, 2016 11 01
Moscow - The **Security Council is charged with working out the president's decisions on national security affairs**. In this light, Sputnik asked Secretary Patrushev to lay out his views regarding the security situation in the world today, and the regions which he sees as the most problematic. "The situation in the world is not becoming any easier," the official admitted. "There is a growing competition for global influence and the use of global resources." **Other threats Moscow takes seriously include the "unprecedented threat" of global terrorism, represented first and foremost by the Daesh (ISIL/ISIS) terrorist group.**

Putin says Russia is successfully countering terrorism, extremism
ITAR-TASS World Service, Staff report, 2016 10 31
Astrakhan - **Russian President Vladimir Putin has stated that Russia is successfully confronting terrorism and extremism**, but urged to remain vigilant to prevent such threats. "Russia is successfully countering global threats. These are extremism and terrorism," he told a meeting of the **Council for Interethnic Relations**. Putin pointed to the need to pay close attention to preventing extremism and interethnic tensions. "The more so since there are growing trends in today's world to erode traditional values, while interethnic and interreligious discord and animosities are being fomented," he said, adding that "of course, we must and will counter these destructive trends."

Les hommes neufs de Vladimir Poutine
Le Monde, Isabelle Mandraud, 2016 10 28
Moscou - En vue de l'élection présidentielle de 2018, **le président russe se débarrasse de sa vieille garde, pour placer une équipe plus jeune qui « ne tutoie pas le chef ».** Un renouvellement qui accentue la personnalisation du régime. La garde prétorienne de Vladimir Poutine a changé. En l'espace de quelques semaines, plusieurs proches du chef de l'Etat russe ont été écartés et remplacés par d'autres collaborateurs, plus jeunes, souvent peu connus, comme **Anton Vaïno, 44 ans, promu chef de l'administration présidentielle; Sergueï Kirienko, 54 ans, chargé de la politique intérieure; ou Viatcheslav Volodine, 52 ans, nommé président de la Douma, la chambre basse du Parlement**. Tous partagent un point commun qui les différencie de leurs aînés, «ils ne tutoient pas le président», ainsi que le souligne le politologue Andreï Kolesnikov, mais ils ont, surtout, une mission bien précise devant eux: préparer l'élection présidentielle de 2018. L'été, au Kremlin, est souvent une période propice au ménage. Le 12août, l'un des personnages les plus influents du pays, Sergueï Ivanov, 63 ans, qui régnait depuis décembre2011 sur l'administration présidentielle, a été débarqué tout comme, un an auparavant, à la même période, Vladimir Iakounine, 68 ans, le puissant patron des chemins de fer russes pendant dix ans. **Ces deux proches de Vladimir Poutine étaient issus du même sérail que le président, le KGB, et faisaient partie d'une génération parvenue en même temps au pouvoir.**

In Russia's cyberscene: Kremlin desires, private hackers, and patriotism
Christian Science Monitor, Fred Weir, 2016 10 27
Moscow - **While much is known about US cyber-war and -espionage capabilities thanks to the massive data leaks of former NSA contractor Edward Snowden, Russia's capacity for such is much more obscure**. But the experience of **Alexander Vyarya**, which came to light virtually without notice last year, may offer a few telling glimpses of it. Mr. Vyarya, a young Russian programmer, was a team member at Qrator, a leading Russian cybersecurity company that specializes in mitigating the effects of distributed denial-of-service [DDoS] attacks. According to his account, given to the **independent Russian online news service Medusa**, the company was approached by an intermediary from Russia's Ministry of Communications looking for a specialist to help with a particular problem. Vyarya was "loaned" on an unofficial basis to Rostek, the Russian state technology conglomerate, in early 2015, and sent to an office in Sofia, Bulgaria. There, he was asked to help develop software not to block, but to amplify DDoS attacks. He did - and he was appalled when the program was "tried out" before his eyes on targets like Ukraine's Defense Ministry and the liberal Russian magazine Slon, he later told Medusa.

How the Kremlin Handles Hacks: Deny, Deny, Deny
Bloomberg View, Leonid Bershidsky, 2016 10 26
Column - The **U.S. presidential election has made "Russian hackers" a powerful brand**. There is, however, another that surpasses it: **Ukrainian hackers**. And the story of their most recent hack contains valuable lessons for U.S. politicians, particularly Hillary Clinton and the Democrats. A **Ukrainian hacker collective calling itself CyberHunta -- a mocking reference to Russian propaganda outlets'** moniker for the Kiev government, the junta -- claimed on Oct. 23 to have broken into an electronic mailbox that belongs to VladislavSurkov, President Vladimir Putin's adviser for dealing with former Soviet breakaway regions. The purported hacked e-mails supposedly contain sensitive information, including, for example, a lengthy plan of "urgent measures for the destabilization of the situation in Ukraine." Unlike Clinton's allies after their e-mails were published, the Kremlin immediately denied the authenticity of the leaked communications. Putin's press secretary, Dmitri Peskov, told reporters that Surkov didn't use e-mail, so those who claim to have broken into has mailbox "must have had to sweat quite a lot" to forge messages.

Hacked: Putin's Aide's Emails Detail Alleged Detailed Plot To Destabilize Ukraine
Foreign Policy, Reid Standish, 2016 10 25
Washington - A **Ukrainian hacker group claims to have obtained emails from VladislavSurkov, a top aide to Russian President Vladimir Putin, that detail a purported Kremlin plan to destabilize Ukraine in the coming months**. **CyberJunta**, the group behind the alleged hack, released late on Sunday email exchanges belonging to Surkov, a scan of passports belonging to Surkov and his family, and 22 pages from documents outlining a plan to support nationalist and separatist politicians and to encourage early parliamentary elections in Ukraine, all with the aim of undermining the government in Kiev. "It is necessary to create favorable conditions for controllable political forces to enter the new parliament," said a report released by the hacking group. **OleksandrTkachuk, the chief of staff to the head of the SBU, Ukraine's intelligence service,** said on TV Tuesday that experts from the agency examined the documents released by CyberJunta, and believe them to be real. Speaking to reporters on Tuesday, Kremlin spokesman Dmitry Peskov denied Surkov's involvement in any plot to foment unrest in Ukraine, and said that the documents released by the hacking group were not real.

Return to Table of Contents/ Retour à la table des matières

Europe

Des employés du SRC peu discrets sur Internet
Tribune de Genève, Caroline Zuercher, 2016 10 31
Berne - Des **collaborateurs du Service de renseignement se présentent sur des réseaux sociaux professionnels Certains collaborateurs, actuels ou anciens, du Service de renseignement de la Confédération (SRC) ne font guère preuve de discrétion**. Ils se dévoilent sur des plates-formes Internet, **LinkedIn ou Xing**, et y décrivent leurs compétences et leur cahier des charges, révèle Schweiz amSonntag. Le dominical mentionne notamment le cas d'un employé qui explique travailler comme spécialiste ComCenter - un service qui réceptionne, classe et transmet les informations en Suisse et à l'étranger. Un autre, externe, a été impliqué dans le développement d'un système de base de données dont il donne quelques informations. Et le journal d'ajouter que le **directeur du SRC, Markus Seiler**, **possède un profil LinkedIn.**

Les « espions » suisses font leur pub sur le Net
Le Matin (Suisse), Ph. C., 2016 10 31
Berne - Il **semble bien loin le temps où les James Bond du pays de Tell n'avaient même pas le droit de dire à leur femme en quoi consistait leur job**! Aujourd'hui, nous révèle laSchweizamSonntag, il suffit de surfer sur LinkedIn ou Xing pour voir d'anciens ou d'actuels **employés du Service de renseignement de la Confédération (SRC)**vanter leurs mérites et leurs compétences. Des qualités - et donc des noms - visibles et accessibles à tout un chacun. Ainsi, un ex-employé décrit-il comment il a pris part au développement d'une nouvelle base de données contenant des informations ultrasensibles sur la sécurité de l'Etat. Un autre parle de son travail au sein d'une unité de renseignement stratégique, chargée de fournir des analyses au chef de l'armée.

Enquête sur le 13 Novembre : le patron de la DGSE interrogé par un juge antiterroriste
Le Parisien, Thibault Raisse, 2016 10 29
Paris - **La justice a tenté de connaître auprès de la Direction générale de la sécurité extérieure (DGSE) le nom du commanditaire des attentats de Paris**. Un refus poli lui a été opposé... Qui ne tente rien n'a rien. Selon nos informations, l'un des juges antiterroristes en charge des investigations sur les attentats du 13 Novembre a interrogé **Bernard Bajolet**, le patron de la Direction générale de la sécurité extérieure (DGSE), le 29 juillet. Une initiative inédite et osée, puisque la DGSE, rattachée au ministère de la Défense, n'a aucun compte à rendre à l'institution judiciaire. Le chef des services de contre-espionnage français a néanmoins subi un interrogatoire en tant que témoin après ses propos tenus en mai devant la commission parlementaire sur les attaques de Paris et Saint-Denis. « Il est vrai qu'Abaaoud était un coordinateur mais pas le commanditaire. Nous connaissons le commanditaire mais je resterai discret sur ce point », avait-il indiqué. Une déclaration qui a manifestement suscité l'intérêt du juge d'instruction venu questionner le haut fonctionnaire à l'hôtel des Invalides (Paris VIIe). Après avoir rappelé cette confession faite aux parlementaires, le magistrat met les pieds dans le plat. « Pouvez-vous, dans ces conditions, donner le nom du commanditaire des attentats du 13 novembre 2015 ? » interroge-t-il « La demande de déclassification mettrait en danger nos sources », prévient le chef du renseignement extérieur, qui ajoute qu'en matière de terrorisme la **DGSE travaille en collaboration avec la DGSI, le renseignement intérieur**, avec qui les juges antiterroristes sont habilités à échanger des informations.

Serbian daily says Russian security chief extracts agents
Serbian daily Blic, via BBC Monitoring Europe, 2016 10 29

Belgrade— **Nikolai Patrushev, Russia's main intelligence official, has paid a visit to Serbia in order to bring back to Moscow three Russian spies**, suspected of involvement in the developments in **Montenegro**, Blic has learned. During his two-day stay, Patrushev, known as the boss of all of the Russian secret services, had several bilateral meetings with top Serbian officials. His main goal was to iron out the situation after the exposure of three Russian operatives. As Blic has learned, they were discovered in the past 10 days during the actions of the Serbian security services related to the developments in Montenegro on the eve of the election there, when, as Podgorica claims, there was an attempted coup.
After his two-day visit, the Russian spies departed with Patrushev for Moscow. As Blic has learned, they had stayed in Belgrade. **"Handing over spies is not unusual, so neither is this case**. They withdraw, and if they are really valuable, their services send them to another country," Blic's source said.

Bosnian ministry denies forming new intelligence agency
Bosnia-Herzegovina Federation public TV via BBC Monitoring Europe, 2016 10 28
Sarajevo— The **Bosnia and Hercegovina [B-H] Defence Ministry has reacted following the media reports concerning procedures to amend the Defence Law and to form of a new intelligence agency within the B-H Armed Forces with powers to observe civilians**. The Ministry said that the legislative amendments did not mention a new agency, observing citizens, or extending powers of the **Military Intelligence Department** beyond the army barracks. The proposed amendments are related to specific improvements in the work of Military Intelligence Department in the areas of data exchange and cooperation with security agencies. [Teletovic] At the end of last year, the B-H Defence Ministry launched an initiative to amend certain provisions concerning intelligence and security work, that is, Article 9, in order to allow the Military Intelligence Department to seek all strategic information and data from intelligence-security agencies, which has not been the case so far. This does not involve any transfer of powers, but the aim is to make sure that the existing powers are defined better, B-H assistant defence minister said. He added that the media uproar was aiming at abolition of the military intelligence battalion, which would be impermissible.

Lithuanian State Security Department introduces hotline to boost national security
Lithuanian News Agency, 2016 10 27
Vilnius— The **State Security Department of the Republic of Lithuania (VSD) has launched a hotline and begun a public awareness campaign. VSD Director Darius Jauniskis** says that the anonymous hotline will enable Lithuanian citizens to more actively contribute to enhancing the country's security. According to Jauniskis, military experts, journalists, politicians and public figures widely discuss military, hybrid, propaganda and information threats. Meanwhile, the public rarely addresses the threat against national security posed by hostile intelligence agencies. Yet they pose no less of a threat and may target any Lithuanian citizen, which has rarely been discussed. The **first intelligence agency of independent Lithuania was established under the military on 27 October 1918.** At the time the Armed Forces was the only guarantee of Lithuania's national security and the secret service that operated under the military gradually became a well organised intelligence agency.

L'antiterrorisme belge
Le Soir, Ludivine Ponciau, 2016 10 27
Bruxelles - Un **rapport d'experts évalue l'efficacité des mesures antiterroristes**. La **Belgique** a **sous-estimé l'intérêt de la lutte contre le financement du terrorisme**. Au-delà des sommes en jeu, ces données financières auraient pu faire avancer bien des enquêtes. Près d'un an après les attentats de Paris, l'Institut Egmont publie une évaluation des mesures préventives et répressives prises en matière de lutte contre le terrorisme depuis les attentats de

Charlie Hebdo par sept experts issus du monde académique. Un rapport assez sévère pour le gouvernement Michel et dont Le Soir a pu prendre connaissance. L'un des volets du rapport pointe l'inertie dont a fait preuve la Belgique en matière de lutte contre le financement du terrorisme alors que « la quête de l'argent est vitale pour les terroristes », souligne France Lemeunier, coauteure du rapport.

La piste des services secrets se confirme
Le Quotidien (Luxembourg), 2016 10 26
La Valette, Malte— **Parmi les cinq occupants qui ont trouvé la mort dans le crash d'un avion de la compagnie luxembourgeoise CAE Aviation, lundi à Malte, trois étaient des membres de la direction technique de la DGSE (Direction générale de la sécurité extérieure), les services secrets français,** ont rapporté des médias français hier, dont Le Monde. L'information n'a pas été officiellement confirmée par les autorités françaises qui s'étaient contentées lundi de reconnaître que l'appareil effectuait des missions de reconnaissance en Méditerranée pour le compte du ministère de la Défense. Les deux autres victimes de l'accident, pilote et copilote, étaient des salariés de CAE Aviation. La société, fondée en 1971, est établie au Findel et possède également une implantation à Lapalisse, dans le département français de l'Allier, où elle assure l'entraînement au parachutisme des forces spéciales de plusieurs armées européennes.

Le crash de Malte lève un coin de voile sur les vols de la DGSE
Le Monde, Jacques Follorou, 2016 10 26
Malte - **Un avion ALSR (avion léger de surveillance et de reconnaissance), loué par la Direction générale de la sécurité extérieure (DGSE) à la société CAE aviation, s'est écrasé**, lundi 24 octobre au matin, à Malte, juste après le décollage. Les cinq occupants, trois personnels de la direction technique de la DGSE et deux pilotes de CAE, sont morts dans l'embrasement de l'appareil, après avoir tenté, en vain, de revenir vers l'aéroport. Les autorités maltaises pensaient qu'il s'agissait d'un aéronef utilisé, depuis cinq mois, par les douanes françaises " pour surveiller les trafics " . Mais le **ministère de la défense français a dû finir par reconnaître, laconique, que l'avion " effectuait des missions de reconnaissance en Méditerranée " et que trois victimes appartenaient à son effectif.**

Montenegro investigating Russian role in alleged election coup plot
The Guardian, Julian Borger, 2016 10 25
London— **Montenegro's prime minister has said his government is investigating a possible Russian role in an alleged 16 October coup plot aiming at derailing the country's elections**.Milo Djukanovic said that there was a " strong connection of a foreign factor" in the alleged conspiracy to take over the Montenegrin parliament on election day, adding that the country's authorities would investigate the extent of involvement of both Russia and Serbia. **Twenty people, including the former commander of special police in neighbouring Serbia, were arrested on the day of the would-be coup attempt**. The Serbian prime minister, Aleksandar Vucic, announced on Monday night that Serbian police had made more arrests of people suspected of following Djukanovic and planning unspecified crimes in Montenegro. **Russia's security chief, Nikolai Patrushev, was expected in Belgrade to hold talks with Serbian leaders in the wake of the arrests**, according to reports from the Serbian capital. Those reports said Patrushev had come to discuss terrorism, the migrant crisis in Europe, and alleged extremism in Kosovo. Adding to the febrile atmosphere, the Serbian government announced that an **interior ministry official had been arrested for contacts with western intelligence.** The interior minister, Nebojsa Stefanovic, said the authorities had "neutralized this person through effective action" but gave no further details.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Intelligence minister says military diplomacy is important
Tehran Times, 2016 10 31
Tehran - The **Iranian intelligence minister on Sunday said military diplomacy is important in international calculations. Mahmoud Alavi** made the remarks while addressing a conference featuring Iran's military attachés and defense and police representatives of the armed forces. "Military attachés, as well as defense and police representatives of the Islamic Republic of Iran, play an important role in preserving the achievements and national interests of the country," Alavi noted. He added, "They also use every opportunity and seek to reduce regional threats against our country."

The KGB's long history of running agents in Israel
Jerusalem Post, Yossi Melman, 2016 10 28
Jerusalem - Researchers, historians, **Shin Bet counter-espionage operatives and even the broader public did not need Israeli daily newspaper YediotAharonot's exposé this week about Israeli Soviet spies in order to know that Soviet intelligence** tried and succeeded in penetrating into the heart of Israel's diplomatic-security-intelligence establishment. The depth of the penetration by the Soviet Union's **KGB and GRU** (military intelligence), or of the intelligence services of communist satellite states, has been testified to by a long line of agents who were convicted in Israel from the 1950s through to the 1990s. It is a long and impressive list of "moles," quality agents that penetrated every important department in Israel. These are the serious and important spies that caused the most damage to the **Israeli defense and intelligence establishment**. I

Secret Files Expose KGB Spies in Israel's Top Political and Military Echelon
Haaretz, OferAderet, 2016 10 27
Jerusalem - The **KGB**, Russia's espionage organization, **recruited and ran spies among Israel's Knesset members, senior army officers and intelligence community**, as well as lower-level workers on classified projects, according to an investigation by journalist Ronen Bergman. The first part of his investigation will be published by YediothAhronoth on Friday. The report is based on secret KGB documents copied over decades by an archivist at the spy organization, VasiliMitrokhin, from the 1960s to the 1980s. He defected to Britain in 1992 and gave the documents to British intelligence. Some were published in books and the press over decades, triggering an international uproar as KGB agents operating in the United States, Britain and other countries were outed by name. Mitrokhin died in Britain in 2004. Half a year ago, the British espionage agency MI6 agreed to the publication of additional parts of the archive Mitrokhin left behind, in which Bergman found material on KGB activity in Israel.

Iran spy chief questioned after letting gay US politician into country
Jerusalem Post, Benjamin Weinthal, 2016 10 27
Jerusalem - **Iran's top spymaster was harshly criticized by the country's parliament on Wednesday after it was discovered that he secretly invited an openly-gay American politician to the Islamic Republic,** according to Al-Arabiya. Under questioning, Intelligence Minister **Mahmoud Alavi** confirmed that Democratic Utah State Senator **Jim Dabakis** had traveled to the country last month and "was kept under full surveillance during his secret visit." Homosexuality in Iran is against the law and is punishable by imprisonment, corporal

punishment, or by execution. Alavi also noted that no one had objected to Dabakis' previous visit to Iran in 2010, when former president Mahmoud Ahmedinejad, whose government was supported by hardliners, was in power, Al-Arabiya reported.

Agents Trail Utah Senator Who's Gay on Iran Visit
New York Times, Rick Gladstone, 2016 10 26
New York - **Iran's intelligence minister normally does not find himself on the receiving end of criticism by fellow hard-liners asking how he could possibly have overlooked a visit by a gay state legislator from the United States**. But that is what happened on Tuesday in Iran's Parliament, where the minister, **Mahmoud Alawi, faced tough questioning about a six-day visit this summer by Jim Dabakis, a state senator** from Utah and the Democratic Party's state chairman, who is gay. Mr. Alawi's answer: His agents knew the visitor's every move. "The minister made it clear that the American politician was kept under surveillance by the intelligence forces during his stay in Iran," the official Tasnim News Agency said in its report about Mr. Alawi's parliamentary testimony. Tasnim made no reference in its report to Mr. Dabakis's sexual orientation. Tasnim said the minister had "assured the lawmakers that all schemes with the aim of making inroads into Iran are under control of the intelligence forces." Mr. Alawi's disclosure was news to Mr. Dabakis, an art dealer in Salt Lake City who has advocated cultural exchanges between the United States and Iran to ease the countries' decades-old estrangement. He also visited Iran in 2010. **"I'm just surprised that Iranian intelligence doesn't have anything better to do,"** Mr. Dabakis said in a telephone interview.

Return to Table of Contents/ Retour à la table des matières

Asia/Asie

Seoul, Tokyo hold talks on intelligence-sharing pact
Yonhap News Agency, Staff reporter, 2016 11 01
Seoul - **South Korea and Japan held working-level talks in Tokyo Tuesday to reach an understanding on an intelligence-sharing pact that could allow the neighbors to better cope with North Korea's evolving nuclear and missile threats**, the defense ministry said. "The two sides resumed talks based on the terms they tentatively agreed to in 2012 and discussed a wide range of issues such as future meeting schedules and agendas," the Ministry of National Defense said in a statement. The next gathering will be decided through consultations with Japan, it said. Last week, the two neighbors agreed to reopen talks on a bilateral General **Security of Military Information Agreement** (GSOMIA), with the goal of concluding the pact by the end of the year. The U.S. welcomed the decision, saying the potential deal between its two Asian allies would bolster cooperation amid growing threats posed by Pyongyang. The communist regime has escalated saber-rattling with its nuclear and missile development programs. It conducted two nuclear tests and launched a series of missiles this year.

Samajwadi MP's aide was spying for Pakistan
Press Trust of India, 2016 10 31
New Delhi - **Samajwadi Party's Rajya Sabha MP MunavvarSaleem's personal assistant Farhat Khan, who was arrested on Saturday in connection with the espionage racket**, was in touch with **Pakistani intelligence operatives** for the last 18 years and **was leaking sensitive documents and information, police** said. "Farhat Khan was in touch with Pakistani intelligence operatives for the last 18 years. He used to be paid Rs. 20,000 for the information

and documents he shared with them," said a senior police officer. Farhat had worked with other SP leaders before he became Mr. Saleem's PA around 10-11 months back, the officer said. Since he was working with a Rajya Sabha MP, he was privy to a lot of information pertaining to Government of India and documents, he said.

Al-Qaeda leader targeted in Afghanistan kept low profile but worried spies
Washington Post, Wesley Morgan, 2016 10 30
Kabul - When Army Capt. Hugh Miller heard a group of police officers trading stories about a militant called **Farouq al-Qahtani** at their base in Afghanistan's Konar province one day four years ago, he didn't know what all the fuss was about. "I don't think I even sent a report up about it," Miller, who was deployed as a combat adviser at the time, said in a recent interview. "I didn't know the guy was a big deal." **Qahtani, a Saudi native with a Qatari passport whose real name was Nayef Salam Muhammad Ujaym al-Hababi, was targeted on Oct. 23** in an airstrike in Konar's remote Helgal valley, the Pentagon announced Wednesday. Little-known outside **counterterrorism circles**, he was indeed a big deal: Though only in his mid- 30s, Qahtani was thought to be the senior al-Qaeda operative remaining in Afghanistan at a time when many of the group's bigwigs had decamped for Syria, and U.S. government documents suggest he may have been involved in plotting attacks abroad. Konar and neighboring Nuristan, which blend together in the jagged 12,000-foot mountains that Qahtani has frequented for the past six years, have been the scene of some of the costliest and most publicized episodes of the American war in Afghanistan: **Operation Red Wings**, where 19 Special Operations members were killed; the many firefights in the infamous Korengal valley, where the documentary "Restrepo" was filmed; the battles of Wanat and Ganjgal, which led to both acrimonious investigations and high-profile awards for combat heroism.

Information minister relieved of his office
Dawn, Amir Wasim, 2016 10 30
Karachi— **Senator Pervaiz Rashid has been relieved of his responsibilities as the federal minister for Information, Broadcasting and National Heritage**. According to a handout issued by the PM Office on Saturday, the information minister **was held responsible for a "lapse"** following the controversy in the wake of a news report published in Dawn, which both the government and the military termed a breach of national security. There has been an uproar in the country since the publication of the story 'Act against militants or face international isolation, civilians tell military' in Dawn on Oct 6, which gave details of an undisclosed meeting attended by a large number of civilian officials, including the prime minister, three chief ministers, the foreign secretary and officials from civil and military intelligence agencies. Saturday's handout noted that the minister was "directed to step down from office to enable holding of an independent and detailed inquiry". "**An inquiry committee including senior officers of Inter-Services Intelligence (ISI), Military Intelligence (MI) and Intelligence Bureau (IB) is being formed by the government to clearly apportion blame**..", the statement said. However, it was not clear who from within the government is going to head the committee.

Rajnath Singh asks Home Secretary to closely monitor spying case
Web India News, 2016 10 29
New Delhi - **Union Home Minister Rajnath Singh has ordered Home Secretary Rajiv Mehrishi to closely monitor the case in which Delhi Police have arrested ISI agents spying for Pakistan** in India and to report the Minister accordingly. These spy agents have developed a big nexus in the country and have been carrying out espionage activities in India by passing defence secret documents and maps to ISI. Intelligence sources said that their arrest has revealed that very vital documents and maps have reportedly been leaked to Pakistan

intelligence agency ISI which could be dangerous for Indian security system at borders. Seeing the gravity of the situation, the Home Ministry has ordered to increase the deployment of more battalions across Indo-Pak borders in Rajasthan as well.

Pak govt sacks minister over news report on rift with army
Press Trust of India, 2016 10 29
Lahore— The **Pakistan government today sacked Information Minister Pervaiz Rashid over the recent "leaked" media report about a rift between the civilian and military leaderships** on support to militancy. The Prime Minister's spokesman Musadiq Malik confirmed that "initial evidence" was against Rashid in the **leak of sensitive information of a high profile national security meeting**. "Investigation into controversial story is in the final stage and it will be shared with media in a couple of days. Who was responsible for the leakage of sensitive information to the Dawn reporter will be known soon," Malik said adding "investigation is still underway". Rashid is a close aide of Prime Minister Nawaz Sharif and reports suggest that the anti-army information could not have been leaked to the media without his consent.

Espionage case: Pak official held, expelled for spying; ties take another hit
Times of India, Staff Report, 2016 10 28
New Delhi - The already dim prospects of any improvement in India- Pakistan relations were dealt another blow on Thursday with **Delhi Police busting an espionage ring whose 'kingpin' is a Pakistan high commission official.** The government declared Mehmood Akhtar persona non grata after he was nabbed buying classified documents from **two men from Rajasthan at the Delhi zoo.** Indian officials found that Akhtar enjoyed immunity even though he wasn't a diplomatic passport holder. Besides **MaulanaRamzan Khan and SubhashJangid** who were nabbed from the zoo, Akhtar was in touch with Shoaib from Rajasthan. An FIR under Sections 3 and 5 of the Official Secrets Act has been registered against the accused, joint commissioner (crime) Ravindra Yadav said.

India Says Visa Officer Was a Spy for Pakistan
New York Times, Ellen Barry, 2016 10 28
New Delhi - **India** announced on Thursday that it was **expelling a Pakistani officer at the country's diplomatic mission in New Delhi**, accusing him of using his consular position to develop an **espionage ring**, a move likely to worsen tensions between the nuclear-armed neighbors. The Delhi police said the officer, Mehmood Akhtar, had served for more than two years in the mission's visa section, which they said had allowed him to recruit Indian citizens to spy for Pakistan. A statement from the Pakistani Foreign Ministry rejected the accusations as "false and unsubstantiated." In a tit-for-tat announcement Thursday evening, Pakistan announced it would expel an Indian official posted in Islamabad, giving his family 48 hours to leave the country.

S. Korean opposition party voices against intelligence sharing with Japan
Xinhua News Agency, YooSeungki, 2016 10 28
Seoul - **South Korean main opposition Minjoo Party on Friday expressed its strong objection to the resumption of talks with Japan to share military intelligence on the Democratic People's Republic of Korea (DPRK).** Woo Sang-ho, floor leader of the party, said at a supreme council meeting that it can never be accepted to militarily join hands with Japan which has yet to sincerely repent over its past atrocities during the World War Two and its colonization of the Korean peninsula from 1910 to 1945. He said the adoption of the military intelligence-sharing accord between Seoul and Tokyo will prop up Japan's militaristic ambition, urging the South Korean government to stop the talks which will make people enrage again.

South Korea Plans to Revive Talks With Japan on Sharing Intelligence
New York Times, Choe Sang-Hun, 2016 10 28
Seoul - **South Korea said on Thursday that it would restart talks with Japan about a military intelligence-sharing pact**, four years after a similar agreement was canceled in the face of a domestic furor. Officials at the Defense Ministry said in a news briefing on Thursday that such an agreement would allow South Korea to better address the growing nuclear and missile threats from North Korea. The South hopes to sign a deal by the end of the year, the officials said. The United States has also pressed Japan and South Korea, its allies, to increase military cooperation so that the three countries could more effectively work together to monitor and confront the military threats from the North.

Seoul, Japan to resume talks on exchange of military intelligence
Yonhap News Agency, Staff reporter, 2016 10 27
Seoul - **South Korea and Japan have agreed to resume talks for the exchange of military intelligence on North Korea's nuclear development programs**, their foreign ministries said Thursday. "The decision came to resume talks that would allow the two countries to exchange military intelligence in the face of unprecedented nuclear and missile threats from North Korea," **Seoul's Vice Foreign Minister Lim Sung-nam** said in a press conference in Tokyo. His **Japanese counterpart Shinsuke Sugiyama** said Tokyo will sincerely respond to the decision. "Military threats posed by North Korea (to neighboring countries) are now entering another elevated level. We need to make a response different from previous ones," he said. Chief Cabinet Secretary YoshihideSuga stressed the need for Seoul and Tokyo to increase security-related cooperation to better counter the North's increasing threats.

Draft of new counter-terror law triggers old fears in Sri Lanka
The Hindu, Meera Srinivasan, 2016 10 27
Colombo - **Even as Sri Lanka drafts a new law to counter terrorism, human rights activists and lawyers here fear it might be worse than the Prevention of Terrorism Act (PTA)** they want repealed and replaced. One of the key demands around regime change in Sri Lanka in January 2015 -- when former President Mahinda Rajapaksa was unseated --was to repeal the PTA. "After the new government came to power, all of us expected a shift, but now people are disappointed," says senior human rights lawyer K.S. Ratnavale.

RAW, NDS patronising terror groups in Afghanistan, national security adviser tells US envoy
Pakistan Dawn, Sanaullah Khan, 2016 10 27
Islamabad - **Pakistan on Wednesday conveyed to the United States that India's Research and Analysis Wing (RAW) and Afghanistan's National Directorate of Security (NDS) are patronising terrorists groups to attack soft targets in the country**. **National Security Adviser Lt Gen (retd) Nasser Khan Janjua** conveyed the message to **US ambassador David Hale** in a meeting today, said the statement released by the office of the NSA. The meeting was held to discuss the terrorist attack on Police Training College Quetta, counter-terrorism operations and cross-border attacks. Janjua also emphasised on the need to break the nexus between terrorists groups operation under the **supervision of NDS and RAW**. Pakistan has asked for US assistance to tackle the situation. The NSA informed the ambassador that the terrorists who attacked the police training college were constantly in contact with their leadership and handlers in Afghanistan.

Efforts to get N. Korea to denuclearize 'probably a lost cause': U.S. intelligence chief
Yonhap News Agency, Chang Jae-soon, 2016 10 26

Washington/Seoul - **Any effort to get North Korea to give up its nuclear program "is probably a lost cause"** and putting a cap on the regime's nuclear capabilities is the "best we could probably hope for," the U.S. intelligence chief said Tuesday. "I think the notion of getting the North Koreans to denuclearize is probably a lost cause. That is their ticket to their survival. I got a good taste of that when I was there about how the world looks from their vantage and they're under siege and they're very paranoid," **Director of National Intelligence James Clapper said during a Council on Foreign Relations discussion**. He was referring to his 2014 visit to Pyongyang to win the release of two detained Americans. "So the notion of giving up their nuclear capability, whatever it is, is a nonstarter with them ... The best we could probably hope for is some sort of a cap, but they're not going to do that just because we ask them. There's going to have to be some significant inducements," he said during the event in New York that was live-streamed on the CFR's website.

Return to Table of Contents/ Retour à la table des matières

Africa/Afrique

Lancement à Tunis du centre Tunisien de recherches et d'études sur le terrorisme
African Manager (Tunisie), Journaliste maison, 2016 10 26
Tunis - Le **forum tunisien pour les droits économiques et sociaux (FTDES) a annoncé, mercredi, le lancement du Centre Tunisien de Recherches et d'Etudes sur le Terrorisme (CTRET).** Lors d'une conférence organisée à Tunis pour présenter cette nouvelle structure et annoncer les résultats de sa première étude, Abderra**hmane Hedhili**, président du FTDES a souligné que le centre aura pour mission la réalisation des études visant à analyser le phénomène du terrorisme et à connaître ses différents mécanismes et son développement afin de réfléchir à des solutions anticipées pouvant réduire la prolifération de ce fléau à long terme. Hedhili a indiqué que depuis la révolution à ce jour, des milliers de jeunes sans emploi ont émigré clandestinement alors que d'autres ont été attirés par les réseaux terroristes et de contrebande. "

Return to Table of Contents/ Retour à la table des matières

Americas/Amériques

Venezuelan business owner denounces gov't "harassment" of his family
EFE News Service, 2016 11 01
Caracas— **Lorenzo Mendoza, president of Empresas Polar, the largest private food company in Venezuela, denounced Monday what he considered the "harassment" by the government intelligence service** of himself, his family and the more than 30,000 employees of his company. "I wish to reject as strongly as possible the harassment and persecution of which I am the victim - I, my workers and my family - by the political police of the **Sebin" national intelligence service**, Mendoza told reporters at Polar headquarters on the east side of Caracas. The statement came four days after a group of Sebin agents, armed with assault rifles and wearing ski masks, were stationed outside the company's headquarters and around his home. According to Polar, they are still there. Mendoza believes the agents' presence is unjustified and, to the contrary, is part of an organized intimidation process that the government has been developing against him "for several years now."

Venezuela food company Polar denounces harassment by intelligence agents
Reuters, 2016 11 01
Caracas— **Venezuelan food company Polar, the South American nation's largest private firm, on Monday denounced harassment by state intelligence agents** who have been stationed at the gates of its headquarters since late last week. Lorenzo Mendoza, owner of the conglomerate, said armed and masked officers from the **Sebin intelligence agency** have also been stationed outside his residence for no apparent reason. "I simply wanted to make this statement to reject the persecution and harassment that my workers, my family, and I have been subjected to by the political police," said Mendoza, surrounded by cheering workers, in comments to reporters. The agents were stationed outside the company's headquarters after the opposition coalition announced a one-day strike for Friday to demand a recall referendum on the rule of Maduro, who is struggling to control an unraveling socialist economy. **Reuters was unable to obtain comment from the office of the vice presidency, which oversees Sebin**

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

02-11-2016 to/au 08-11-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

La GRC et la surveillance des journalistes: rien de rassurant
L'Actualité, Alec Castonguay, 2016 11 08
Ottawa - Est-ce que la GRC a déjà espionné des journalistes, à l'image du SPVM et de la SQ? À Ottawa, depuis une semaine, c'est le festival du faux-fuyant pour ne pas répondre. Depuis les révélations sur la surveillance des journalistes par la police de Montréal et la Sûreté du Québec, la réaction du gouvernement Trudeau a de quoi rendre perplexe. Et inquiet. Même si le premier ministre et ses ministres répètent que la liberté de la presse est un pilier «essentiel pour une démocratie qui fonctionne bien et une société libre», et qu'ils suivent cette situation de près, ils se comportent davantage comme un gouvernement qui souhaite que la controverse ne franchisse pas la rivière des Outaouais. Le ministre de la Sécurité publique, **Ralph Goodale, qualifie la surveillance des journalistes au Québec de «très inquiétante», mais il ne cherche pas à faire toute la lumière sur les agissements passés de la GRC et du Service canadien du renseignement de sécurité (SCRS), qui sont sous sa responsabilité**. En août 2007, des policiers de la GRC ont pris en filature pendant neuf jours le journaliste de La Presse, **Joël-Denis Bellavance**, afin de tenter de coincer la source qui lui avait remis un document secret du **SCRS** concernant **Adil Charkaoui**. Les enquêteurs s'étaient toutefois fait refuser l'interception des numéros entrants et sortants de son téléphone cellulaire, une mesure jugée trop intrusive dans sa vie et son travail.

More than 10,000 document security incidents in Trudeau government's 1st year
CBC News, Staff reporter, 2016 11 08
Ottawa - **There have been more than 10,000 incidents of classified or secure documents being improperly left or stored since Prime Minister Justin Trudeau's government came to office.** According to a document quietly tabled in the House of Commons, the highest number of incidents took place in Public Services and Procurement Canada, which reported 2,912 cases of documents not handled according to the security level dictated for the documents between Nov. 4, 2015, and Sept. 19, 2016. The Global Affairs Department was a close second with 2,712 incidents. The **Canadian Security Intelligence Service, Canada's spy agency, came third with 659 cases.** The agency said 12 of the incidents were sent for further investigation. It is not known whether any of the incidents led to security or privacy breaches.. Public Safety Minister Ralph Goodale's office had six cases during the time frame covered by the government's answer. In total, the **Public Safety Department had 272 incidents**. While the **Communications Security Establishment**, which conducts electronic monitoring and surveillance, reported 491 incidents, it was quick to point out that its operations are carried out in a high-security zone and none of the documents left the building.

RCMP intelligence centre compiled list of 89 Indigenous rights activists considered "threats"
APTN National News, Jorge Barrera, 2016 11 08
Ottawa—Rattled by Idle No More and Mi'kmaq-led anti-shale gas demonstrations, the **RCMP compiled a list of 89 individuals considered "threats" as part of an operation aimed at improving the federal police force's intelligence capacity when facing Indigenous rights demonstrations, according to an internal intelligence repor**t. The operation, dubbed **Project SITKA**, was launched in early 2014 to identify key individuals "willing and capable of utilizing unlawful tactics" during Indigenous rights demonstrations, according to the RCMP report, obtained under the Access to Information Act by two researchers working on a book about state

surveillance of Indigenous peoples. The intelligence report was to provide a "snapshot of individual threats associated to Aboriginal public order events" for that year. The report, completed in 2015 by the **Mounties' National Intelligence Coordination Centre**, recommended the RCMP remove Indigenous rights activism from the terrorism-extremism umbrella and instead create a new category for intelligence gathering on the issue. The report also recommended the RCMP maintain updated profiles on identified Indigenous rights activists in police databases. The researchers obtained the RCMP report in an Access to Information request package from the **Canadian Security Intelligence Service** (CSIS). The RCMP did not provide comment on the report as of this article's posting. CSIS did not respond to a request for comment.

MPs question PM's power over upcoming National Security Committee
Hill Times, Rachel Aiello, 2016 11 07
Ottawa - The **government's bill proposing the establishment of a new National Security and Intelligence Committee of Parliamentarians needs to be amended to give its members more access to information and lessen the prime minister's ability to interfere**, Parliamentarians heard last week. The proposed committee under Bill C-22 is mandated to review activities carried out by any department that relates to national security or intelligence and report annually on its reviews and findings. Unlike other parliamentary committees, this one would report directly to the prime minister, members would require a security clearance, and all meetings would be held in private. In addition, the chair--who the PMO announced in January to be Liberal MP David McGuinty (Ottawa South, Ont.)--would receive a $42,000 "additional annual allowance" and the up to eight members will be paid an extra $11,900, which is the going rate for chairs of House of Commons committees. As it's drafted, the new committee would have less teeth than other federal security expert bodies, have a narrower scope of access to information, and the prime minister would be able to veto studies or redact the committee's reports at his discretion if there's something judged to be potentially jeopardizing national security. During the first two days dedicated to Bill C-22 at the House Public Safety and National Security Committee, members heard from Public Safety and National Security Minister Ralph Goodale (Regina-Wascana, Sask.), Government House Leader BardishChagger (Waterloo, Ont.); their top advisers; **the heads of Canada's security agencies, the RCMP, CSIS, CBSA, and CSE; and top experts and past watchdogs**.

CSIS claims it has been transparent with ministers about data collection
Globe and Mail, Colin Freeze, 2016 11 07
Ottawa - **Facing fallout from judges complaining of being kept in the dark over some of its activities, Canada's domestic spy agency says its officials always keep CSIS's political masters and watchdogs aware of what it is doing**. In a rare public statement, the director of the **Canadian Security Intelligence Service** says that his predecessors briefed ministers several times over the past decade about the kinds of data collection done within what CSIS calls its "Operational Data-Analysis Centre." "The creation of **ODAC** ... was presented to the Minister of Public Safety in July, 2006, explaining the requirement for advanced analytics and the ability of ODAC to retain data, including metadata, for extended periods of time," **Michel Coulombe** said in a statement released Sunday. "The minister was also briefed on the program in March, 2010." His remarks come days after the Federal Court released a scathing ruling faulting CSIS for unlawful data retention and not being forthright with judges. CSIS's current minister, Ralph Goodale, has also since complained of lax record keeping by the spy agency. Most Canadians had never heard of the ODAC intelligence facility until last week. While much remains murky, it appears to be a repository of all kinds of data that federal intelligence analysts can study in attempts to predict, or better understand, security threats.

Head of CSIS argues data was collected legally, but accepts Federal Court ruling
The Canadian Press, Joanna Smith, 2016 11 06
Ottawa - The **head of the Canadian Security Intelligence Service says he wants to make sure everyone understands the spy service did not deliberately do anything wrong when it kept potentially revealing electronic data about people who posed no security threat**. ``CSIS recognizes the importance of maintaining public trust and confidence in its activities," its director, **Michel Coulombe**, said in a statement issued Sunday. The statement was an unusual step for the head of the spy agency, which characterized it partly as a response to the media coverage that followed a Federal Court decision released publicly last week, when Justice Simon Noel ruled CSIS had violated the law by keeping the personal data over a 10-year period. Coulombe said he wanted to reiterate that the data was collected legally using warrants and that the spy agency, in consultation with the Justice Department, had interpreted the CSIS Act in a way that allowed them to retain the data in the way they did. ``The Federal Court has disagreed with this interpretation and we accept their decision. I would like to make it clear that the Service was not knowingly exceeding the scope of the CSIS Act," Coulombe wrote. The judge said that in 2006, CSIS began processing the data, using a powerful program known as the Operational Data Analysis Centre to produce intelligence that is able to reveal specific, intimate details about people.

Federal security review to examine CSIS powers in the digital age, Goodale says
Canadian Press, Jim Bronskill, 2016 11 05
Ottawa - A **federal review of national security will consider whether Canada's spy service should be able to sift through the kind of personal data it kept illegally for years, says Public Safety Minister Ralph Goodale**. Goodale said Friday the notion that the Canadian Security Intelligence Service should avoid stashing away information about innocent people is a ``fundamental principle of Canadian privacy." But the minister appeared to leave the door open to one day giving CSIS the legal authority to keep and analyze electronic data about individuals who do not pose a security threat. He indicated the federal security review already under way would be a good forum to explore the matter. ``I want to hear the professional advice on both sides," Goodale told a news conference in the foyer of the House of Commons. ``I'm not pre-empting the consultation." A Federal Court judge says CSIS violated the law over a 10-year period by keeping potentially revealing electronic data about people who were not targets of investigation. In a pointed ruling made public Thursday, Justice Simon Noel said CSIS breached its duty to inform the court of its data- collection program, since the information was gathered using judicial warrants. In a hastily assembled news conference Thursday after the decision become public, **CSIS director Michel Coulombe** said the spy service had halted all access to, and analysis of, the data in question while it thoroughly reviews the court decision. Goodale said he became aware of the ``full scope of the issue" when the court judgment was made available to him in preliminary form a couple of weeks ago.

Espionnage de journalistes - Ottawa ferme les yeux sur le passé
Le Devoir, Guillaume Bourgault-Côté, 2016 11 05
Ottawa - **Aucun journaliste n'est actuellement surveillé par la GRC et le SCRS... mais Ottawa n'a pas idée si cette situation a pu se produire dans un passé récent. Le ministre de la Sécurité publique, Ralph Goodale**, ne l'a pas demandé. Et il n'a pas l'intention de le faire : c'est le présent qui compte, dit-il. Pour M. Goodale, " la question porte sur ce qui se passe maintenant et nous pouvons offrir l'assurance que ce genre d'activité n'a pas lieu. Je ne sais rien sur les événements qui se sont produits lorsque nous [les libéraux] ne formions pas le gouvernement ", a indiqué le ministre en point de presse. Questionné à savoir s'il demanderait directement au patron du Service canadien du renseignement de sécurité (SCRS) si des mandats de surveillance ont pu être lancés dans les cinq dernières années, Ralph Goodale a

répondu que c'était précisément la " responsabilité du directeur de répondre aux questions opérationnelles ". Or, interrogé la veille à savoir si le SCRS a pu mettre des journalistes sous surveillance dans les dix dernières années, le directeur en question -- **Michel Coulombe** - - avait répondu : " Ce qui s'est passé au Québec ne se produit pas au niveau fédéral. Je ne commenterai pas plus que cela et je ne commenterai pas des questions opérationnelles. " Il avait ajouté qu'à " cause des mesures en place au niveau fédéral, une situation comme on voit présentement au Québec ne s'est pas produite et ne se produira [pas] ".

Civilian watchdog defends CSIS and embattled director over 'metadata'
Toronto Star, TondaMacCharles and Alex Boutilier, 2016 11 05
Ottawa - **Michel Coulombe, Canada's top spy, is in deep trouble with the courts and his political boss, Public Safety Minister Ralph Goodale, over revelations CSIS kept a decade's worth of data on Canadians who are no threat to national security. But Pierre Blais, head of the civilian watchdog agency over CSIS, says Coulombe "acted in good faith" and should not lose his job over the affair.** "He's doing a good job. And that's a difficult issue, that we have to act as big girls and big boys and we look at this and we should do the best for the future," said Blais, chair of the Security Intelligence Review Committee (SIRC). Blais came to Coulombe'sdefence Friday, saying CSIS and its director did not deliberately lie to the court about a practice that SIRC red-flagged in an annual report tabled in January. That was the first time the Federal Court learned that CSIS had created an Operational Data Analysis Centre in 2006. CSIS and its lawyers were hauled before a panel of all Federal Court judges who handle national security warrants and cases last spring to explain.

Animal Rights Groups, the KKK, and ISIS--the RCMP's New Guide To Extremism
Vice News Canada, Justin Ling, 2016 11 05
Ottawa - For the past few years, the Canadian government has faced accusations that it's been asleep at the switch when it comes to stopping youth from being programmed by violent extremist groups. The **Royal Canadian Mounted Police are striking back at that notion with a 140-page guide to radicalization, extremist groups operating in Canada, and terrorist groups abroad. The agency's Terrorism and Violent Extremism Awareness Guide, which was officially unveiled in October,** "is intended for first responders, parents, colleagues or friends of persons at risk alike and is meant to help the reader to better understand and recognize the growing phenomenon of radicalization to violence." A large chunk of the report is just compiling resources on radicalization, offering different models that try to explain how someone might come around to violence and extremism based on their social, religious, and political beliefs. But the report also sheds light on exactly which domestic groups the RCMP are keeping an eye on. The report's language borrows heavily from internal security and intelligence assessments prepared by groups like the **Canadian Security Intelligence Service and the Integrated Terrorism Assessment Centre**. The federal police break those organizations down by three groups: right-wing extremists, left-wing extremists, and "sole motivation" ideologies.

Quebec Mounties seek to launch discrimination lawsuit against RCMP
iPolitics.ca, Amanda Connolly, 2016 11 05
Ottawa - The **association that represents RCMP members in Quebec is seeking to certify a class action lawsuit against the force on behalf of members across the country, alleging systemic harassment and discrimination against members by superiors**. "There's some cases that have been done privately but on behalf of all members, this has never been done," said Frederic Serre, media officer for the Quebec Mounted Police Members Association. "You're looking at power trips and unfortunately there's a lot of it within the force ... That's what we're trying to point out with this action." Serre said that although it's an association

representing Quebec Mounties that's seeking to launch the suit, the class action is meant to represent all RCMP members across Canada -- not just those in Quebec or francophones.

CSIS broke law by keeping sensitive metadata, Federal Court rules
Canadian Press, Jim Bronskill, 2016 11 04
Ottawa - A **Federal Court judge says Canada's spy agency illegally kept potentially revealing electronic data about people over a 10-year period.** In a hard-hitting ruling made public Thursday, **Justice Simon Noel** said the Canadian Security Intelligence Service breached its duty to inform the court of its data-collection program, since the information was gathered using judicial warrants. CSIS should not have retained the information since it was not directly related to threats to the security of Canada, the ruling said. ``Ultimately, the rule of law must prevail," Noel wrote, adding, ``without it, the actions of people and institutions cannot be trusted to accurately reflect the purpose they were entrusted to fulfil." CSIS crunched the data beginning in 2006 using a powerful program known as the Operational Data Analysis Centre to produce intelligence that can reveal specific, intimate details about people the spy service investigates, the judge said. The improperly retained material was metadata _ information associated with a communication, such as a telephone number or email address, but not the message itself. However, it is difficult to determine the precise nature of the metadata involved due to heavy redactions to the 126-page court ruling. At a hastily arranged news conference late Thursday, **CSIS director Michel Coulombe said the spy service had halted all access to, and analysis of, the data in question while it thoroughly reviews the court decision**. ``I deeply regret the court's serious concerns with respect to meeting our duty of candour, and I commit to continuing my efforts, with the deputy minister of justice, to address this concern," Coulombe said. Mosley said CSIS breached its duty of candour by failing to disclose that **CSE's foreign counterparts in the Five Eyes intelligence network _ the United States, Britain, Australia and New Zealand _** could be called upon to assist.

In scathing ruling, Federal Court says CSIS bulk data collection illegal
Globe and Mail, Colin Freeze, 2016 11 04
Ottawa - The **Federal Court of Canada faulted Canada's domestic spy agency Thursday for unlawfully amassing data, for misusing its surveillance warrants and for not being forthright with judges who authorize its intelligence programs**. The court is also revealing that CSIS no longer needs warrants to collect Canadians' tax records because of changes wrought by Bill C-51. The matter was said to involve the decade-long collection of volumes of data within the **Canadian Security Intelligence Service's little- known Operational Data Analysis Centre,** which the judges who scrutinize CSIS are characterizing as a hidden and unlawful repository of data amassed by the spy agency. The centre and the data within it are so secret that the Federal Court - which authorizes CSIS wiretapping bids - had no idea they existed. "The Court had never before been fully informed of the existence of the program. The Court, during the hearings, learned that the program had been in existence since 2006 yet it had never heard nor seen any evidence on the matter," reads a partly redacted new ruling from Federal Court **Judge Simon Noël**.." Public Safety Minister Ralph Goodale is currently consulting with Canadians on whether he needs to change the laws under which CSIS operates. He is also pitching Parliament on a new committee of MPs who could be given powers to investigate intelligence agencies. The Federal Court has now signalled it disagrees with this assessment. In recent years, CSIS's collection capabilities are thought to have been vastly increased by co- operation warrants that exist with the **Communications Security Establishment,** a federal spy agency that dredges global telecommunications data in bulk.

Les espions canadiens ont outrepassé leur mandat
TVA Nouvelles avec l'Agence QMI, Journaliste maison, 2016 11 03

Ottawa - **Le service d'espionnage canadien a outrepassé sa mission en conservant illégalement des informations sensibles recueillies en vertu de mandats, a tranché la Cour fédérale dans un jugement rendu public**, jeudi. En point de presse, **Michel Coulombe, le patron du Service canadien du renseignement de sécurité (SCRS) a dit prendre acte du verdict**. «Le SCRS accepte la décision de la cour et a pris des mesures immédiates pour y répondre», a-t-il déclaré. Je regrette profondément les graves préoccupations de la cour à l'égard de notre manquement quant à l'obligation de franchise.» Durant plusieurs années, le SCRS a caché à la Cour fédérale - qui est chargée de lui délivrer des mandats - l'existence d'un programme de récolte de métadonnées.

Feds hold Twitter consultation on national security
CTV.CA, Laura Payton, 2016 11 04
Ottawa - **Public Safety Canada held a Twitter chat Thursday night to hear what Canadians think about national security and its responsibility to Canadians**. The department in charge of the **RCMP, the Canadian Security Intelligence Service and its oversight body, and the Canada Border Services Agency** asked people to tweet them using the hashtag #YourNatlSec starting at 8 p.m. ET to discuss accountability in national security. The social media discussion comes the same week the House public safety committee is starting its review of bill C-22, which will amend some of the laws changed under the Conservatives' highly contentious C-51. The review also comes hours after a shocking revelation that CSIS held on to 10 years of electronic data it wasn't allowed to have. The metadata, which includes information like a telephone number or email address but not the content of a communication, wasn't directly related to national security threats. The Federal Court released a decision Thursday rebuking CSIS for keeping the information. **Public Safety Minister Ralph Goodale** didn't participate in the Twitter chat. New Democrat justice critic Murray Rankin says he wanted as many people as possible to participate.

Hillary Clinton was warned in 2010 that U.S.-Canada intelligence sharing 'may be controversial for Canadians'
Postmedia News, Zane Schwartz, 2016 11 04
Ottawa - **Huma Abedin warned Hillary Clinton in 2010 that cables from the U.S. Embassy in Ottawa could cause problems for Stephen Harper's government, emails released** Thursday show. "Two cables set for release contain especially sensitive information on counterterrorism and intelligence sharing. The depth of bilateral cooperation detailed in the cables may be controversial for Canadians," said longtime Clinton-advisor Abedin. Abedin's email was sent on Nov. 27 2010. On Nov. 29 the New York Times published a story detailing a 2008 **conversation between the former head of the Canadian Security Intelligence Service Jim Judd and senior State Department counsellor Eliot Cohen**. The story details a conversation where Judd told Cohen that Canada received warning the Taliban was planning an explosion at Sarpoza Prison in Kandahar but was unable to "get a handle on the timing." 'Everything we do is reviewed': Canadian security agency defends activities amid spying allegations This seemed to contradict a statement made by former chief of defence staff General Rick Hillier that: "Obviously we would have liked to have known so we could have pre-empted or helped, more accurately, the Afghans pre-empt that kind of thing." The significance of Canada's role in the Five Eyes alliance became clearer in 2013 when leaked information from whistle blower Edward Snowden showed that **Canada's Communications Security Establishment** set up covert spy posts in about twenty countries on behalf of the United State's National Security Agency .

In wake of Quebec incidents, PM has verified no reporters under watch at federal level
Toronto Star, Bruce Campion-Smith and TondaMacCharles, 2016 11 04

Ottawa - Revelations of police surveillance of journalists are "troubling" and could spark further measures to better safeguard the rights of the press, **Prime Minister Justin Trudeau** says. Trudeau **said he has verified no journalists are under surveillance "at the federal level" by the RCMP or CSIS,** and said Canadians are following "with concern" reports that Quebec's two largest police forces had been tracking the phones of several reporters in that province in recent years. "Not only is freedom of the press important, but it's one of the foundational safeguards of a free democracy, of a free society," Trudeau told a news conference Thursday. "This government understands that and understands how important it is to respect the media and the press," he said. Asked about Quebec police justifying the intrusive technique on the basis they sought to plug leaks, Trudeau said the "troubling" revelations of police snooping will lead to "reflection" on how governments can better ensure the protection of the press and the rights of journalists.**CSIS director Michel Coulombe** later echoed Trudeau's comments but refused to directly say whether Canada's spy agency has undertaken court-warranted interception of any Canadian journalist's communications, saying he would not talk about operational matters.

La GRC et le SCRS ne surveillent pas les journalistes, dit Trudeau
La Presse+, Joel Denis Bellavance, 2016 11 03
Ottawa - Se **disant préoccupé par les révélations au sujet des activités de surveillance menées par le Service de police de la ville de Montréal et la Sûreté du Québec auprès de journalistes, le premier ministre Justin Trudeau affirme avoir obtenu l'assurance de la part des patrons de la GRC et du SCRS qu'ils ne se livrent pas à de telles activités**. En mêlée de presse, jeudi, M. Trudeau a indiqué avoir pris l'initiative de communiquer avec le commissaire de la GRC, **Bob Paulson**, et le directeur du Service canadien du renseignement de sécurité (SCRS), **Michel Coulombe**, afin de s'assurer que les règles et les lois fédérales qui s'appliquent à ces deux organisations soient respectées.

Des francophones de la GRC intentent une action collective
Journal de Montréal, Michaël Nguyen, 2016 11 04
Westmount - Des **francophones de la Gendarmerie royale du Canada (GRC) veulent intenter une action collective contre leur employeur qu'ils accusent de discrimination**. Des membres et ex-membres francophones de la GRC, dont Paul Dupuis (en mortaise), veulent intenter une action collective contre la discrimination qu'ils disent avoir vécue. La plupart des policiers concernés viennent de la Division C, basée à Westmount. «Les opportunités d'avancement sont de beaucoup diminuées pour des policiers francophones, alors que dans l'autre sens, un unilingue anglophone peut accéder à un haut grade», s'insurge Paul Dupuis, un retraité de la police fédérale, à l'origine de ce recours.

Surveillance de journalistes : mutisme à la GRC et au SCRS
La Presse+, Vincent Brousseau-Pouliot, 2016 11 02
Ottawa - Alors que la SQ et la Ville de Montréal ont confirmé avoir mis des journalistes sous surveillance, **la GRC et le Service canadien du renseignement de sécurité (SCRS), les deux corps policiers fédéraux, ne veulent pas confirmer s'ils ont déjà adopté de telles pratiques**, et le cas échéant à quelle fréquence. La GRC précise seulement que «les cas où des enquêtes de la GRC concernant des journalistes ont eu lieu sont extrêmement rares». Le commissaire de la GRC Bob Paulson a dit mercredi «ne pas être au courant que nous avons des enquêtes actives ou de la surveillance à l'égard de journalistes», mais la GRC n'a pas voulu confirmer si des journalistes ont été surveillés dans le cadre de ses enquêtes. Un cas de filature avait été rendu public il y a un an, celui du journaliste de La Presse Joël-Denis Bellavance qui a été pris en filature en 2007.

Goodale ducks question about journalists under surveillance
iPolitics.ca, Staff reporter, 2016 11 02
Public Safety Minister **Ralph Goodale won't say how many Canadian journalists might be under police surveillance.** In question period today, NDP leader Tom Mulcair raised the case of Montreal journalist Patrick Lagacé -- who learned recently that police had been monitoring his phone calls and location through GPS in his cellphone as part of an internal police probe. At least 24 warrants were issued on Lagacé's phone. "'It's disgusting', as one of my colleagues said," Mulcair told the Commons, also citing the case of La Presse journalist Joel-Denis Bellavance, who has been tailed by police. Mounties followed Bellavance for nine days in 2007 in an attempt to track down a leak of classified documents. **"Can the minister of public safety tell us whether other journalists are being spied upon either by the police, the RCMP or CSIS?" Mulcair asked Goodale. Goodale skirted the question, saying only that the issue is "entirely in the jurisdiction of Quebec,** and this morning the premier of Quebec has made a very import pronouncement in that regard.

Cybersecurity talent shortage on the radar of government, business
CBC News, Julie Ireton, 2016 11 02
Ottawa--An **international shortage of cybersecurity talent is expected to grow over the next few years, according to the Information and Communications Technology Council**. The council's vice-president of talent innovation, **Sandra Saric**, said there's an expected need for more than 1.5 million people to work in cybersecurity globally by 2020. Solving the talent shortage was one of the challenges emphasized by government and private industry executives at a cybersecurity forum at the GTEC conference in Ottawa on Tuesday. It's an annual technology event that brings together business and government. "Getting more people to take science, technology, engineering and mathematics courses and degree programs, and also training them to be cybersecurity savvy is probably the first challenge," said **Scott Jones, assistant deputy minister responsible for the information technology security program with Communications Security Establishment Canada (CSEC).**

Ottawa falls short of real oversight for C-51 powers
The Province (Vancouver), Murray Rankin, 2016 11 02
Op-ed: Last year, former prime minister Stephen Harper's **Bill C-51** brought in controversial new security powers, despite the opposition of hundreds of thousands of Canadians and the advice of legal scholars and civil liberties organizations. Resisting calls from the NDP and others to repeal the law, the Liberal government has kept C-51 on the books. Under the legislation, the sharing of personal information between government agencies was **expanded, the Canadian Security Intelligence Service was given unprecedented powers to disrupt terrorist plots and a range of perceived security threats**, the right of police to preventively arrest people was expanded, and urging others to commit terrorism became a criminal offence. Now, Parliament is debating a proposal to plug a long-standing gap in our security architecture: Canada today stands alone among our closest allies in lacking independent, elected oversight of security and intelligence agencies. Unfortunately, **the government's plan falls short of giving Canadians a real watchdog for their rights and safety. Bill C-22 would create a committee without the powers, the independence and the public trust needed to get the job done**.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

Chinese spies in a field of dreams; Seed case shows difficulty of fighting espionage
Los Angeles Times, Del Quentin Wilber, 2016 11 08
Washington - It was a chilly spring day when an Iowa farmer spotted something odd in his freshly planted cornfield: a short, bald Asian man on his knees, digging up seeds. Not just any seeds -- special inbred seeds, the product of years of secret research and millions of dollars in corporate investment, so confidential that not even the farmer knew exactly what he was growing. The farmer approached the trespasser, who grew flush and nervous, stammering something about being from a local university. When the farmer diverted his attention briefly to take a phone call, the stranger bolted to a waiting car and sped away. That curious encounter eventually led to an **exhaustive five-year federal investigation and prosecution into one of the most brazen examples of Chinese economic espionage against the U.S., a crime that annually costs American companies at least $150 billion**. The **FBI** pulled out all the stops to catch the spies. Agents obtained surveillance warrants from the nation's secret intelligence court, planted GPS-tracking devices on cars, trailed operatives from airplanes and bugged their phones. The investigation culminated last month with a three-year prison sentence for Mo Hailong, 47, a Chinese citizen and U.S. legal resident who works for a Chinese conglomerate. Even though the scheme was exposed, Chinese companies almost certainly got their hands on some of the lucrative seeds.

How the F.B.I. Reviewed Thousands of Emails in Eight Days
New York Times, Adam Goldman, Matt Apuzzo, 2016 11 08
Washington - Out of hundreds of thousands of emails seized last month from disgraced former Representative Anthony D. Weiner, a substantial number turned out to be copies of documents already reviewed by F.B.I. agents and analysts, allowing the agency to wrap up in days a review that some had feared would take weeks, if not longer. The F.B.I. discovered approximately 650,000 emails on a computer that agents had seized while investigating Mr. Weiner on allegations of sexual improprieties. Some of those emails belonged to Huma Abedin, Mr. Weiner's estranged wife and a top aide to Hillary Clinton. As **it turned out, law enforcement officials said, there was no need to review all of the emails, only Ms. Abedin's. Those emails numbered in the thousands, and even many of those were duplicates of messages that had been looked at previously, officials said. That allowed the F.B.I. to sort through the emails faster than many, including some at the agency, had expected.**

Amid Clinton Controversy, FBI Documents Show Why Americans Should Worry About Intelligence Gathering
The Intercept, Cora Currier, 2016 11 07
Washington - Two **internal policy documents obtained by The Intercept make clear that, whatever (FBI director James) Comey's motivations, his critics are right to worry about the bureau's mounting ambition and about the widening scope of its intelligence gathering**. Under Comey and the previous director Robert Mueller, the bureau has transformed its domestic intelligence operations in the name of fighting terrorism, building up an army of some 15,000 informants and deploying those informants in recent years not only for aggressive sting operations but also to collect intelligence not tied to any particular criminal case. The documents, one of which dates to August 2013, just before Comey was sworn in, clearly illustrate this transformation as they make the case that the FBI should maintain and expand its

human intelligence (or "**HUMINT**") efforts. They also show the FBI jostling for "primacy" with the CIA and other intelligence agencies. One memo, a "Domestic HUMINT Vision Proposal" from an advisory council to the FBI's Directorate of Intelligence, states that the FBI's "policies and procedures need to mirror those under which US Intelligence Community (USIC) partners operate." The advisory council stood up in 2011, according to the FBI's 9/11 Review Commission report, and the vision proposal, from references in the text, appears to date to some time after 2012.

F.B.I. Says Review Clears Clinton in Email Inquiry
New York Times, Multiple reporters, 2016 11 07
Washington - The F.B.I. director, **James B. Comey, told Congress on Sunday that he had seen no evidence in a recently discovered trove of emails to change his conclusion that Hillary Clinton should face no charges over her handling of classified information**. Mr. Comey's announcement, just two days before the election, was an effort to clear the cloud of suspicion he had publicly placed over her presidential campaign late last month when he alerted Congress that the F.B.I. would examine the emails. "Based on our review, we have not changed our conclusions that we expressed in July with respect to Secretary Clinton," Mr. Comey wrote in a letter to the leaders of several congressional committees. He said agents had reviewed all communications to and from Mrs. Clinton in the new trove from when she was secretary of state.

The Democratic National Committee Has Told the FBI It Found Evidence Its HQ Was Bugged
Motherjones, David Corn, 2016 11 05
Washington - In an episode reminiscent of Watergate, the **Democratic Party recently informed the FBI that it had collected evidence suggesting its Washington headquarters had been bugged, according to two Democratic National Committee officials who asked not to be named.** In September, according to these sources, the DNC hired a firm to conduct an electronic sweep of its offices. After Russian hackers had penetrated its email system and those of other Democratic targets, DNC officials believed it was prudent to scrutinize their offices. This examination found nothing unusual. In late October, after conservative activist James O'Keefe released a new set of hidden-camera videos targeting Democrats, interim party chairwoman Donna Brazile ordered up another sweep. There was a concern that Republican foes might have infiltrated the DNC offices, where volunteers were reporting to work on phone banks and other election activities.

The FBI looks like Trump's America
Politico.com, Josh Zeithz, 2016 11 05
Washington - The **typical Federal Bureau of Investigation special agent is white, male, and middle-aged, often with a military background -- in short, drawn from the segment of the U.S. population most likely to support GOP nominee Donald Trump**. That demographic reality explains much of the heat **FBI Director James Comey** is taking from his own work force at the moment for his handling of the Hillary Clinton email investigation and inquiries into the Clinton Foundation. Days before the presidential election, FBI finds itself at the center of a political maelstrom, with Comey being sharply criticized by Democratic presidential nominee Hillary Clinton and even President Barack Obama, who've faulted the FBI director for going public with word of new evidence in the Clinton email probe. That furor has exposed dissension in the FBI's ranks, prompting a flurry of leaks about alleged efforts to impede the Clinton-related inquiries and exposing lingering anger among agents about Comey's July decision not to recommend any charges in the email probe.

'He's got to get control of the ship again': How tensions at the FBI will persist after the election
Washington Post, Multiple reporters, 2016 11 04
Washington - **Deep divisions inside the FBI and the Justice Department over how to handle investigations dealing with Hillary Clinton will probably fester even after Tuesday's presidential election** and **pose a significant test for James B. Comey's leadership** of the nation's chief law enforcement agency. The internal dissension has exploded into public view recently with leaks to reporters about a feud over the Clinton Foundation, an extraordinary airing of the agency's infighting that comes as the bureau deals with an ongoing threat of terror at home and a newly aggressive posture from Russia. Comey, meanwhile, has come under direct fire for his decision to tell Congress that agents were resuming their investigation of Clinton's use of a private email server - a revelation that put him at odds with his Justice Department bosses and influenced the presidential campaign. **"He's got to get control of the ship again," said Robert Anderson, a former senior official in the FBI** who considers Comey a friend. "There's a lot of tension in the organization, and there's a lot of tension in Congress and the Senate right now, and all that counts toward how much people trust the FBI."

FBI examining fake documents targeting Clinton campaign: sources
Reuters, Staff report, 2016 11 04
Washington - The **FBI and U.S. intelligence agencies are examining faked documents aimed at discrediting the Hillary Clinton campaign as part of a broader investigation into what U.S. officials believe has been an attempt by Russia to disrupt the presidential election**, people with knowledge of the matter said. U.S. Senator Tom Carper, a Democrat on the Senate Homeland Security Committee, has referred one of the documents to the FBI for investigation on the grounds that his name and stationery were forged to appear authentic, some of the sources who had knowledge of that discussion said. In the letter identified as fake, Carper is quoted as writing to Clinton,

'The FBI is Trumpland': anti-Clinton atmosphere spurred leaks, sources say
The Guardian (London), Spencer Ackerman, 2016 11 03
New York - **Deep antipathy to Hillary Clinton exists within the FBI, multiple bureau sources have told the Guardian, spurring a rapid series of leaks damaging to her campaign just days before the election.** Current and former FBI officials, none of whom were willing or cleared to speak on the record, have described a chaotic internal climate that resulted from outrage over director James Comey's July decision not to recommend an indictment over Clinton's maintenance of a private email server on which classified information transited. "The FBI is Trumpland," said one current agent. The currently serving FBI agent said Clinton is "the antichrist personified to a large swath of FBI personnel," and that "the reason why they're leaking is they're pro-Trump."

Russia may be wounded, but it can still bite
Washington Post, David Ignatius, 2016 11 04
Column - **Whoever wins Tuesday's presidential election will face an assertive, aggrieved Russia whose risk-taking behavior under President Vladimir Putin is increasingly worrisome to U.S. experts**. Today's pushy, headstrong Russia presents a paradox: By most measures, it is a country in decline, with a sagging economy, an underdeveloped technology base and a shrinking population. Corruption pervades nearly every sector. The collapse of the Soviet Union is still an open wound, and many Russians blame the United States for taking advantage of them during their years of decline. Yet this inwardly weak Russia displays the cockiness of a street fighter. It is waging war in Syria, Ukraine and cyberspace with a seeming disdain for U.S. power. **According to Director of National Intelligence James R. Clapper Jr.,**

Russian hackers sought to "interfere with the U.S. election process," on authority of the highest levels of the Russian government. "Putin's definition of risk-taking has evolved in the direction of greater boldness and less attention to how it will affect the U.S.," argues Dimitri Simes, president of the Center for the National Interest. "Putin thinks that American positive inducements are next to nonexistent, and that the penalties are minimal, and will be imposed whatever he does."

U.S. officials warn of Russian mischief in election and beyond
Washington Post, Greg Miller, Adam Entous, 2016 11 04
Washington - U**.S. intelligence agencies do not see Russia as capable of using cyberespionage to alter the outcome of Tuesday's presidential election, but they have warned that Moscow may continue meddling after the voting has ended to sow doubts about the legitimacy of the result**, U.S. officials said. The assessment reflects widespread concern among U.S. spy agencies that a months-long campaign by Russia to rattle the mechanisms of American democracy will probably continue after polls close on one of the most polarizing races in recent history, extending and amplifying the political turbulence. U.S. security officials have not ruled out Russian-sponsored disruption on Election Day. In recent weeks, officials at the Department of Homeland Security have collected evidence of apparent Russian "scanning" of state-run databases and computer voting systems. "Whether they were really trying hard to get in, it's not clear," a U.S. official said. Still, the decentralized nature of U.S. polling would make it extraordinarily difficult to subvert a nationwide race.

John Brennan's attempt to lead the CIA into the age of cyberwar
Reuters, David Rhode, 2016 11 02
Washington - **When America goes to the polls on Nov. 8, according to current and former U.S. intelligence officials, it will likely experience the culmination of a new form of information war**. A months-long campaign backed by the Russian government to undermine the credibility of the U.S. presidential election - through hacking, cyber attacks and disinformation campaigns - is likely to peak on voting day, the officials said. Russian officials deny any such effort. But current and former U.S. officials warn that hackers could post fictional evidence online of widespread voter fraud, slow the Internet to a crawl through cyber attacks and release a final tranche of hacked emails, including some that could be doctored. "Don't underestimate what they can do or will do. We have to be prepared," said Leon Panetta, who served as CIA director and defense secretary in President Barack Obama's first term. "In some ways, they are succeeding at disrupting our process. Until they pay a price, they will keep doing it." **John Brennan, the current CIA director, declined to comment on the Russian efforts.** But he said Russian intelligence operatives have a long history of marrying traditional espionage with advances in technology. More broadly, Brennan said, the digital age creates enormous opportunities for espionage.

Obama Faults F.B.I. on Emails, Citing 'Incomplete Information'
New York Times, Multiple reporters, 2016 11 03
Chapel Hill - **President Obama threw the power of the White House behind Hillary Clinton on Wednesday. He faulted how the F.B.I. director, James B. Comey, handled new emails related to the investigation into Mrs. Clinton's private server**, and then shouted out to college students here in a pivotal battleground state that it was crucial that they vote because the "fate of the world is teetering." Mr. Obama's comments about Mr. Comey, broadcast early in the day as recent polls showed a tightening race, were striking for a president who has insisted he does not comment on F.B.I. investigations. But Mr. Obama appeared to be doing exactly that in implicitly criticizing Mr. Comey's decision to send a vague letter last week to Congress -- and by extension, the public -- informing lawmakers about a discovery of new emails related to Mrs.

Clinton's use of a private server as secretary of state. "We don't operate on incomplete information," Mr. Obama said in an interview with NowThis News.

The politics of espionage in the Obama-Brennan era
Reuters, David Rhode, 2016 11 03
Washington - **Supporters hail CIA director John Brennan as a devoted public servant with a strong moral core and a tenacious work ethic. He has increased the recruitment of minority intelligence officers and promoted women to senior posts. He wears a lanyard around his neck every day that celebrates LGBT diversity at the CIA**. But **some former covert operatives say Brennan is too cautious and political**. Liberals accuse Brennan of protecting the CIA instead of forcing it to become more accountable to Congress. In particular, they blame Brennan for convincing President Barack Obama to oppose the release of the full 6,000-page U.S. Senate report detailing torture by the CIA during the presidency of George W. Bush. In private hearings, they said, Brennan bristled at questions from senators regarding the report. After CIA officials searched the computer of a Senate staffer investigating torture, an outraged Sen. Dianne Feinstein accused Brennan's CIA of provoking a "constitutional crisis" by thwarting Congress' ability to perform its mandated right to oversee the executive-branch agency. Two other Democratic Senators called for Brennan's resignation.

Turmoil in the FBI
CNN.com, Multiple reporters, 2016 11 03
Washington - **Among the casualties of the 2016 presidential campaign is the mystique of the FBI. Behind the scenes over the past 15 months**, infighting among some agents and officials has exposed some parts of the storied bureau to be buffeted by some of the same bitter divisions as the rest of American society. This account is based on interviews with more than a dozen officials close to the matter who spoke anonymously because they've been ordered not to speak to the news media. Tensions have built in particular over the handling of matters related to Hillary Clinton. Some of the sharpest divides have emerged between some agents in the FBI's New York field office, the bureau's largest and highest-profile, and officials at FBI headquarters in Washington and at the Justice Department. Some rank-and-file agents interpreted cautious steps taken by the Justice Department and FBI headquarters as being done for political reasons or to protect a powerful political figure.

Clinton Emails Could Help ex-NSA Contractor Who Took Terabytes Home, Attorneys Say
US News and World Report, Steven Nelson, 2016 11 01
Washington - In **the four years Hillary Clinton sent and received State Department correspondence using a private and insecure email system, Harold T. Martin III allegedly stockpiled classified information inside his Maryland home** and an unlocked shed. Martin faces charges for alleged theft of government documents and mishandling classified information that carry up to 11 years in prison, and he's been behind bars since his August arrest, with prosecutors saying they intend to file more serious Espionage Act charges, often used by the Obama administration to go after leakers and whistleblowers. Though prosecutors have not alleged the now-fired **Booz Allen Hamilton contractor** -- who worked for the **National Security Agency** six years before a transfer to the Pentagon last year -- is a spy or that he shared the information or allowed it to be accessed by a third party, they do allege he could be responsible for one of the largest security violations ever and knowingly mishandled classified records working various jobs over two decades. Defense attorneys for prominent whistleblowers, accused leakers and careless clearance-holders say that unless more damning evidence emerges they could see Martin making a successful plea for leniency by pointing to the Justice Department's decision this summer not to prosecute Clinton.

Evan McMullin Says He Was Aware Of CIA Torture Program, Cites "Gray Areas"
BuzzFeed News, Ali Watkins, 2016 11 02
Washington - **Evan McMullin, the former CIA officer running for president, told BuzzFeed News Tuesday that he was aware of -- but never participated in -- the agency's controversial torture program and would not wholly rule out the future use of tactics like waterboarding**. "I was aware of it by virtue of where I was," McMullin said. "I was serving in a place that was the kind of place where people entered that program from that place, but I never participated in it, I never went to a black site, never met with a detainee." McMullin said he opposes the use of torture, but also declined to clearly qualify what he considered torture, and whether CIA tactics like waterboarding crossed the line.

FBI faces high bar in Clinton case; Legal scholars say charges are unlikely, partly because of Comey's past remarks.
Los Angeles Times, Del Quentin Wilber, 2016 11 02
Washington - **Even if FBI agents discover classified information on a newly seized laptop, Hillary Clinton is unlikely to face criminal charges, according to legal experts and former federal prosecutors.** That's largely because the Justice Department and FBI Director James B. Comey have already declined to prosecute based on a legal conclusion that there was no evidence that Clinton and her aides intended to violate laws governing the handling of classified information, a key element of such a criminal offense. To change the calculus, the FBI would have to find correspondence that clearly demonstrates Clinton or her aides knowingly broke the law, exchanged materials they knew to be classified or attempted to interfere with the investigation by withholding or destroying evidence, according to former federal prosecutors and legal scholars. "Such an email itself would have to be one of those things you would be saying, 'I can't believe you wrote that down,' " said Roscoe Howard Jr., a former federal prosecutor and U.S. attorney for the District of Columbia during the George W. Bush administration.

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

Now in charge of UK spies, gaffe-prone Boris Johnson surveys their domain
Reuters, Staff report, 2016 11 08
London - **Foreign Secretary Boris Johnson has ventured into the headquarters of the MI6 foreign intelligence service for the first time**, praising Britain's spies for stealing secrets in an increasingly unpredictable world. A former journalist and mayor of London known for often outlandish comments and comical behaviour, Johnson gained oversight of the spy service upon his appointment as foreign secretary in July. In a rare statement issued on Tuesday, MI6 said Johnson had paid his first visit to the agency's headquarters at Vauxhall Cross, by the River Thames in London, on Oct. 20. It did not make clear why he had not visited sooner. **MI6 Chief Alex Younger hosted Johnson, who discussed threats ranging from terrorism to the spread of nuclear weapons and cyber attacks.** He also addressed MI6 staff and had an informal question and answer session with spies, according to the statement. "Whether it's combating terrorism or keeping our nation one step ahead of our adversaries, the brave men and women who work for MI6 do a great job in gathering the crucial intelligence the government needs," Johnson was quoted as saying by MI6.
GCHQ wants internet providers to rewrite systems to block hackers
Sunday Telegraph (UK), Cara McGoogan, 2016 11 06

London - **GCHQ is urging internet providers to change long-standing protocols to help prevent computers being used to set off large-scale cyber attacks**. The Government's cyber-defence arm said it plans to work with networks such as BT and Virgin Media to rewrite internet standards to restrict "spoofing" - a technique that allows hackers to impersonate other computers and manipulate them to carry out anonymous attacks. "Distributed denial of service" (DDoS) attacks, which employ this method, have been used in numerous high-profile incidents in the past fortnight, including an unprecedented hack that brought down Netflix, eBay and hundreds more popular websites. "We think we can get to a point where we can say a UK machine can't participate in a DDoS attack," **Ian Levy, GCHQ's National Cyber Security Centre, told The Sunday Telegraph. "We think that we can fix the underpinning infrastructure of the internet through implementation changes with ISPs and CSPs [communications service providers]."** The plan would involve changes to the Border Gateway Protocol (BGP) and Signalling System 7 (SS7) standards that are widely used for routing traffic.

SAS in Iraq gets kill list of British jihadis
Sunday Times (UK), Mark Hookham, 2016 11 06
London - **British special forces operating in Iraq have been issued with a "kill or capture" list containing the names of up to 200 British terrorists fighting alongside Isis**. The Sunday Times understands that the SAS is under orders to target UK terrorist suspects **using intelligence supplied by MI6, MI5 and GCHQ**. Those captured will be handed to the Iraq authorities with the prospect of execution if they are found guilty in trials. The security services and the police have previously spoken of their fear of a so-called "Raqqa scatter" that could see British nationals abandon Isis strongholds, such as the group's de facto capital in the Syrian town of Raqqa, and return to the UK to establish terrorist cells. Senior sources say any surviving Isis terrorists will be "hardened, highly radicalised fighters" who have endured months and sometimes even years of fighting. In a reference to last year's co-ordinated attacks in France which killed 130 people, one source described the terrorists as "highly effective and extremely dangerous guerrilla fighters more than capable of conducting Parisstyle attacks".

Jihadist who fled UK in lorry to join ISIS claimed 'MI5 were making his life intolerable
Daily Mirror, James Carteledge, 2016 11 05
London - A **jihadist who fled the UK in the back of a lorry in a bid to join Islamic State, claiming MI5 had made his life "intolerable"**. **AnasAbdalla** was arrested along with **MahamuudDiini and Gabriel Rasmus** - who talked of launching a terror attack in Birmingham - when they were found hiding in a truck at the Kent port of Dover on April 3 last year. Rasmus, 30, of Sparkhill, admitted preparing for terrorist acts but Somalia-born Abdalla, 27, of Acocks Green, denied it and was found guilty after a retrial. The pair, who are in custody, will be sentenced at the Old Bailey by Judge Richard Marks QC. The retrial was heard partly in secret because the case was said to involve matters of "an extremely sensitive and confidential nature" It can now be reported that the judge's order under Section 11 of the Contempt of Court Act 1981 barred the public from being present when any evidence was called by the prosecution which "confirm or deny" allegations made in Abdalla'sdefence statement. **They were the allegation of contact or attempted contact with MI5 and his claim that "he would not be allowed by MI5 to live and progress normal expectations and achievements in life"** The court was closed during parts of Abdalla's evidence in the witness box, closing speeches by lawyers and the judge's summing up, reports the Birmingham Mail.

Kremlin pours cold water on MI5 chief's claims of Russian threat
The Guardian (London), Shaun Walker, 2016 11 01

Moscow - The **Kremlin has brushed off claims made to the Guardian by the head of MI5 that Russia is taking various hostile measures against Britain**, which together pose a threat to the country. "Those words do not correspond to reality," said Kremlin spokesman Dmitry Peskov on Tuesday. **Andrew Parker, the head of MI5**, told the Guardian that despite widespread fears of Islamic extremists, hostile state actors were a growing threat, and Russia was the main concern. Peskov said: "Until someone produces proof, we will consider those statements unfounded and groundless." Elsewhere in Moscow, there was an acerbic reaction to the Parker interview. "I would like to ask the head of MI5 if he also sees the hand of the Kremlin in the appointment of Boris Johnson as head of the Foreign Office," said Maria Zakharova, spokeswoman for Russia's foreign ministry. She declined to comment further.

MI5 has been caught on the back foot once again
London Times, Sean O'Neill, 2016 11 02
Column - **Russia, the head of MI5 warned yesterday, is using the "whole range of state organs and powers to push its foreign policy in increasingly aggressive ways".** A decade after the state-sponsored murder of the anti-Putin dissident Alexander Litvinenko in London, **Andrew Parker** used the first newspaper interview given by a serving MI5 director-general to deliver this statement of the blindingly obvious. Perhaps it would have been better if Mr Parker had admitted that the Security Service has been largely barking up the wrong tree for the past ten years and underestimated the threat from Putin's regime. Over that period, MI5 has put pretty much all of its resources into spying on Islamists. That, of course, was a threat it also discovered late. **One problem is that MI5 is perpetually led by insiders who have spent their entire career inside the organisation**. Such people have a tendency to focus on the future of the institutions they love and engage in a constant quest for more staff, money and powers.

UK must build cyber-attack capability, chancellor says
The Guardian (London), Jessica Elgot, 2016 11 01
London - The **UK must strike back at hostile states in cyberspace and be capable of mounting sophisticated cyber-attacks of its own in place of military strikes**, the chancellor has said. **Philip Hammond** said that unless the UK could match the cyber-attack abilities of foreign rogue states, the alternatives would only be to ignore digital attacks on Britain's infrastructure or use military force. Launching the government's £1.9bn national cybersecurity strategy, Hammond said the UK had to develop "fully functioning cyber-attack capability".

Return to Table of Contents/ Retour à la table des matières

Australia/ Australie

Intelligence probe
Herald Sun, Annika Smethurst, 2016 11 08
Melbourne - **Former UK spy boss Sir Iain Lobban will join a review into Australia's intelligence agencies. Prime Minister Malcolm Turnbull last night announced he had commissioned the probe, which will assess whether our current intelligence services are "best placed" to meet future security challenges**. Sir Iain, the **former director of the UK's Government Communications Headquarters, will work on the review with Australia security expert and Howard government bureaucrat Professor Michael L'Estrange and former Australian Defence Signals Directorate boss Stephen Merchant**. Mr L'Estrange has

held several senior public service positions including secretary of the Department of Foreign Affairs and Trade and was also the head of the National Security College at the Australian National University. Mr Merchant served as the deputy secretary responsible for the three Defence intelligence agencies and has extensive experience in defence strategy and capability and international policy. It will be the first major review of intelligence services since 2011 and the third report since the September 11 terrorist attacks, which led to an overhaul of intelligence efforts in Australia. Sir Iain, who headed up the UK equivalent of **Australia's Signals Directorate -- which monitors communications between people and agencies** -- was also a member of the Australian Government's expert panel on cyber security.

PM announces intelligence services review
Australian Associated Press, Max Blenkin, 2016 11 08
Canberra - **Australia's intelligence agencies are to be reviewed to ensure structures and mechanisms are able to meet current and future challenges**. **Prime Minister Malcolm Turnbull says, like earlier reviews in 2004 and 2011**, it will assess how the intelligence community serves national interests and consider the ongoing suitability of legislative and oversight provisions. "This is an opportunity to assess whether our current intelligence arrangements, structures and mechanisms are best placed to meet the security challenges we are likely to face in the years ahead," he said in a statement. Mr Turnbull said the review would be conducted by **former top government officials Professor Michael L'Estrange and Stephen Merchant, who will report in the first half of 2017**. He said they were eminently qualified. Prof L'Estrange has held senior public service positions, including secretary of the Department of Foreign Affairs and Trade and High Commissioner in London. He was the inaugural head of the National Security College. **Mr Merchant has held senior defence and intelligence positions including director of the Defence Signals Directorate and the deputy secretary responsible for the three Defence intelligence agencies**. Mr Turnbull said he had also asked the former head of the Government Communications Headquarters, the UK counterpart of the Australian Signals Directorate, to assist the reviewers. The Australian intelligence community comprises the Office of National Assessments, Australian Security intelligence Organisation, Australian Secret Intelligence Service, **Australian Signals Directorate, Defence Intelligence Organisation and Australian Geospatial-Intelligence Organisation**.

National security impact if 18C scrapped
Australian Associated Press, Staff reporter, 2016 11 08
Canberra - A **counter-terrorism expert turned federal MP has warned tinkering with race hate speech laws could have an impact on national security**. Egyptian-born Anne Aly praised former prime minister Tony Abbott for abandoning suggested changes to a contentious section of the **Racial Discrimination Act**. But the Labor MP is scathing of Malcolm Turnbull's willingness to play politics with the issue after the prime minister flagged support for a parliamentary review. "I think this latest backflip is particularly extraordinary when you consider that even Tony Abbott ... recognised the value of not alienating certain sections of the community in the interests of our national security," Dr Aly told reporters in Canberra on Tuesday. She said sections 18C and 18D of the Act - which make it an offence to offend, insult, humiliate or intimidate a group of people based on their race, and provide a defence for fair comment - had served Australians well. "

Spy fear over China link to NBN Component builder linked to Party
Canberra Times, Richard Baker and Nick McKenzie, 2016 11 06
Canberra - **More than 1 million Australian homes and businesses have been connected to the National Broadband Network by components made in a Shanghai factory controlled**

by China's Communist Party. The revelation comes at a time when **China is suspected of mounting massive cyber-espionage attacks on Australia** and after successive Labor and Coalition governments banned Chinese company Huawei from NBN involvement on security grounds.

Asio 'special intelligence operation' not reported to watchdog for 10 days
The Guardian (Australia), Paul Farrel, 2016 11 04
Canberra - **Australia's domestic intelligence agency failed to notify the intelligence watchdog of a controversial "special intelligence operation" for 10 days in what is the first official confirmation of highly secretive missions that give intelligence officers immunity from prosecution**. In 2014 the government passed controversial national security laws that allow the creation of "special intelligence operations" that must be approved by the attorney general, George Brandis. The operations grant **Australian Security Intelligence Organisation** affiliates immunity from prosecution. The new powers also contained a sweeping gag law that news organisations said would stifle legitimate public interest reporting on intelligence operations. A review by the independent national security monitor, Roger Gyles, found that the move could be unconstitutional, and recommended limited changes to the law. The government has put forward a bill to amend the scope of the offence. But a vexed question has been whether these operations had even occurred. Last year the intelligence watchdog declined to respond to Guardian Australia's queries about whether or not they had taken place. **But the inspector general of intelligence and security (Igis), Margaret Stone, has finally confirmed that at least one of the operations has been authorised by the attorney general and executed by Asio.**

Parliamentary committee backs call to keep terrorists in jail after sentences expire
ABC (Australia), Henry Belot, 2016 11 04
Canberra - A **parliamentary committee has endorsed new laws allowing convicted terrorists to be kept in jail once their sentences expire**, provided a court rules they pose a threat to society. The strengthening of Australia's counter-terrorism laws was recommended by Prime Minister Malcolm Turnbull earlier this year after high-profile terror attacks in Orlando, Nice and Paris. On Friday, the Parliamentary Joint Committee on Intelligence and Security recommended the laws be introduced along with 23 amendments. The committee, chaired by Liberal MP Michael Sukkar, called for Attorney-General George Brandis to be able to apply for an extension 12 months before a sentence expires, rather than six months as originally proposed. Other amendments include the exclusion of officers convicted of treason and those publishing recruitment material.

Cabinet warned of cyber threats
The Australian Financial Review, Fleur Anderson, 2016 11 03
Canberra - **Cabinet ministers have been told to improve the cyber security of their departments after it was found inadequate safeguards risked government agencies becoming the "honey pots" of secret information in cyber espionage**. Dan Tehan, the minister assisting Prime Minister Malcolm Turnbull on cyber security, will tell his senior colleagues they need to appoint top bureaucrats to be responsible for cyber security after a study by the Australian National University's National Security College found smaller government agencies and medium-sized business were the weakest link, or "honey pots", in Australia's cybersecurity defences because they are not vigilant enough about "low-level" threats like malware and denial of service attacks.

Government agencies the new 'honey pots' for cyber spies
The Australian Financial Review, Fleur Anderson, 2016 11 02

Canberra - **More than 40 per cent of Australia's government agencies have inadequate awareness of cyber security risks and could become the new "honey pots" of state-sponsored online espionage and cybercrime,** a new investigation by private-sector cyber security experts has found. The Australian National University's National Security College found smaller government agencies and medium-sized business were the weakest link in Australia's cyber security defences because they are not vigilant enough about "low-level" threats like malware and denial of service attacks. Lead researcher Dr Tim Legrand, working in partnership with Macquarie Telecom Group, found it was very likely many attacks were not being reported to the federal government's Computer Emergency Response Team.

Terrorist lockup laws get go ahead
Adelaide Advertiser, Simon Benson, 2016 11 02
Adelaide - The **Turnbull Government has been given the green light for controversial national security laws that would keep convicted terrorists detained after their jail sentences expire if they were deemed to pose an ongoing risk**. The Advertiser understands that the Parliamentary Joint Committee on Intelligence and Security yesterday agreed to back the laws but with the condition that it include a 10-year sunset clause on the legislation. Its final report will go to the government by the end of the week. The committee heard evidence from the Australian Federal Police that more than 180 suspected terrorists across the country were now under investigation by the AFP. But of equal concern was the potential post- sentence risk posed by 14 jailed terrorists already currently in Australian prisons, the first being due for parole next year. Labor had originally sought to delay the committee's final report on the High Risk Terrorist Offenders' legislation until next year.However, it is believed that the Opposition caved in to pressure following a heated exchange last week between the committee Chair Liberal MP Michael Sukkar and Labor's shadow Attorney general Mark Dreyfus. (Full report)

Return to Table of Contents/ Retour à la table des matières

New Zealand/Nouvelle-Zélande

Evidence of terror-attack plan
The Daily Post (New Zealand), David Fisher, 2016 11 04
Wellington - **Concrete evidence has emerged that there has been an actual attempt to carry out a terrorist attack on New Zealand soil**. The security services will release no details of how the plot was foiled or when it emerged, although the system which was activated to deal with it has only been in existence for two years. The existence of the threat came from the newly released **National Security System** handbook. It stated the system - which triggers a special set of protocols - had been activated for a "threat of a domestic terrorist incident". The National Security System is New Zealand's highest-level response to the most serious threats against our country. It is led by a committee chaired by the prime minister and brings together key officials from intelligence services, police, the military and other departments - depending on the threat - to co-ordinate a response. No further information on the nature of the threat was forthcoming from **Prime Minister John Key and Security Intelligence Service (SIS) director Rebecca Kitteridge**. The Department of Prime Minister and Cabinet, which co-ordinates responses, also would not supply details. A spokesman for Mr Key's office said: "As the prime minister has said, New Zealand is not immune from the threat of terrorism, although the threat to New Zealand remains low.

Watchdog raises concern over SIS
New Zealand Herald, Nicholas Jones, 2016 11 04
Wellington - The **intelligence agency watchdog has flagged "significant concern" about how long the Security Intelligence Service (SIS) has taken to respond to her about whether some of its activities were lawful. Inspector-General of Intelligence and Security (IGIS) Cheryl Gwyn** has revealed her displeasure in her office's annual report. In June last year, Gwyn queried whether certain SIS activity was lawful and, if not, how it could be remedied. "The **NZSIS provided its first substantive response to the questions raised in March-April 2016**," Gwyn wrote in the annual report, out today. While she appreciated the issue was complex, Gwyn said the "time taken to engage with and resolve this significant issue is in itself a matter of concern". "To ensure it operates lawfully, the NZSIS must be able to deal with such issues in a more timely way. I will report fully on this issue as soon as possible." Minister Responsible for SIS Chris Finlayson said he was satisfied with the agency's response. "It was largely a result of my instruction. I said, if we are going to change long-standing practice, I want to be absolutely certain that things are done properly.

New Zealand, Australia cooperate on Asia-Pacific cyber security
Xinhua News Agency, John Macdonald, 2016 11 03
Wellington - **New Zealand and Australia have begun working together on initiatives to strengthen trans-Tasman cyber security**, New Zealand Communications Minister Amy Adams said Thursday. Adams said she had recently held talks in Sydney with Australian Minister Assisting the Prime Minister for Cyber Security Dan Tehan, and they had agreed to work together on a range of initiatives that would benefit both countries. Areas of interest included boosting cyber skills, building the cyber capability of small and medium-sized businesses, and cooperating on joint awareness-raising campaigns. The initiatives would bolster the government's approach to cyber security issues, and further align Australia and New Zealand's public- private awareness initiatives and workforce readiness to reduce the cyber threat in the Asia-Pacific region.

The Government won't confirm whether there's been one or two terrorist threats
Radio New Zealand News, Staff reporter, 2016 11 03
Wellington - The **Government won't confirm whether there's been one or two terrorist threats in New Zealand.** In her annual report, the Inspector-**General of Security and Intelligence** confirms the SIS responded to a suspected terrorist act in the second half of last year. They got an urgent authorisation to carry out surveillance without a warrant. At the same time, the Prime Minister's department has released the National Security System handbook which says there was a domestic terrorist threat but it gives no further details. Chris Finlayson, the minister responsible for the SIS, will not confirm whether this threat is the same as the one SIS responded to last year. (full report)

The Prime Minister is dismissing calls to make it harder for the GCSB and SIS to access personal information held by other organisations.
Radio New Zealand News, Staff reporter, 2016 11 03
Wellington - The **Prime Minister is dismissing calls to make it harder for the GCSB and SIS to access personal information held by other organisations**. New legislation requires them to abide by Privacy Act principles, but not have a warrant, when seeking or accessing information from government departments and private companies. The telecommunications company Spark and the Privacy Commissioner have told MPs the bill should have stronger safeguards, including a warrant for sensitive information. John Key says there are bigger privacy concerns than the spy agencies.

Return to Table of Contents/ Retour à la table des matières

International

China/Chine

Asia financial body says China cyber security law could make risk management harder
Reuters, Michelle Price, 2016 11 08
Hong Kong - **The chief of one of Asia's most prominent financial trade bodies on Tuesday said new cyber security rules in China could make it harder for foreign companies operating in the country to manage risk as cyber threats become increasingly cross-border**. Speaking at the Thomson Reuters Pan-Asian Regulatory Summit in Hong Kong, Mark Austen, chief executive of the Asia Securities Industry and Financial Markets Association (ASIFMA), said the rules marked a "worrying" development because regulators globally have to work together to address cyber risks rather than attempt to isolate their jurisdictions. China adopted a **cyber security law** on Monday to counter what the government said were growing threats such as hacking and terrorism. Foreign business and rights groups expressed concern that the law could, for instance, bar foreign companies from certain sectors. The legislation, set to take effect in June 2017, includes requirements for security reviews and for data to be stored on servers in China.

Citing Security, China Will Add Internet Limits
New York Times, Paul Mozur, 2016 11 08
Hong Kong - In August, business groups around the world petitioned China to rethink a proposed **cybersecurity law** that they said would hurt foreign companies and further separate the country from the internet. On Monday, China passed that law -- a sign that when it comes to the internet, China will go its own way. The new rules, which were approved by the country's rubber-stamp Parliament and will go into effect next summer, are part of a broader effort to better define how the internet is managed inside China's borders. Officials say the **rules will help stop cyberattacks and help prevent acts of terrorism, while critics say they will further erode internet freedom.** Business groups worry that parts of the law -- such as required security checks on companies in industries like finance and communications, and mandatory in-country data storage -- will make foreign operations more expensive or lock them out altogether. Individual users will have to register their real names to use messaging services in China.

CY makes pitch for another security law push
South China Morning Post, Jeffie Lam and Gary Cheung, 2016 11 08
Beijing - **Chief Executive Leung Chun-ying made his strongest stand yet on the need to put controversial national security legislation back on the government agenda**. Leung had previously pledged not to touch on the contentious subject during his five-year term. But yesterday, speaking an hour after Beijing had handed down its interpretation, he said the city **would enact the national security law** on its own based on Article 23 of the Basic Law, which would prohibit any act of treason, secession, sedition or subversion. "I believe the central government would no longer regard the legislation of Article 23 as an unfinished constitutional responsibility in the wake of the pro-independence and separatist drive, but instead a [matter of] practical significance," Leung said. "Hongkongers have not seen anyone in the city advocating Hong Kong independence in the past, but now they see it. This indeed deserves our attention."

Government attempts to enact the law in 2003 saw 500,000 people, fearful for their rights and freedoms, take to the streets.

NPC passes cybersecurity law
Global Times, Leng Shumei, 2016 11 08
Beijing - **China's first Cybersecurity Law, which allows authorities to take action against overseas individuals or organizations that will harm China's national interests, will not affect foreign firms' development in China,** experts said. Authorities in China are allowed to take action against overseas individuals or organizations that "attack, intrude, interfere with or sabotage the nation's key information infrastructure," read the **Cybersecurity Law**, which was adopted at the bimonthly session of the National People's Congress Standing Committee on Monday. Operators of key information infrastructure should store important business data and personal data they collect during their operation in China, read the law. In response to questions on whether the law would affect foreign companies's development in China, Foreign Ministry spokesperson Lu Kang said at a regular news briefing on Monday that the law was essentially the same as similar laws in other countries and it treated involved companies, no matter Chinese or foreign, equally without discrimination.

Beijing Tightens Its Control Over Internet With New Law
Wall Street Journal, Josh Chin, Eva Dou, 2016 11 07
Beijing - **China's government approved a broad new cybersecurity law aimed at further tightening and centralizing state control over the internet**, including the role foreign companies play in Chinese cyberspace. The law, passed by the standing committee of China's legislature and issued publicly on Monday, tasks agencies and enterprises with improving their ability to defend against network intrusions while demanding security reviews for equipment and data in strategic sectors.

China adopts law on cybersecurity
Xinhua News Agency, Staff reporter, 2016 11 07
Beijing - **China's top legislature on Monday adopted a Cybersecurity Law to safeguard sovereignty on cyber space, national security and the rights of citizens**. The government will take measures to "monitor, defend and handle cybersecurity risks and threats originating from within the country or overseas sources, protecting key information infrastructure from attack,intrusion, disturbance and damage," the law reads. Efforts will also be made to punish criminal activities online and safeguard the order and security of cyberspace. Individual users and organizations are not allowed to jeopardize security on the Internet or use it to "damage national security, honor and interests," according to the provisions.

Senior graft-buster appointed Chinas new spy chief amid leadership reshuffle
South China Morning Post, Nectar Gan, 2016 11 07
Beijing— A **key ally of Wang Qishan, the Chinese Communist Party's anti-corruption tsar, has been appointed China's top spy master, taking over one of the most secretive ministries** that is undergoing a shakeup after senior officials were accused of graft. **Chen Wenqing** started his career as a policeman in Sichuan province and was Wang's deputy at the Central Commission for Discipline Inspection when it investigated Zhou Yongkang, the former national security chief who oversaw the country's police force, courts and part of its spy operations. He is serving a life sentence for corruption and abuse of power. Chen, 56, who became the Communist Party chief at the Ministry of State Security last year, was officially named as minister of the department by the nation's legislature on Monday. He **will replace his retired predecessor Geng Huichang.**

China Replaces Finance Minister Lou Jiwei in Surprise Reshuffle
Dow Jones Newswire, 2016 11 07
Beijing— China replaced its finance minister and two other top officials in a major reshuffle that comes ahead of a Communist Party congress next year. Finance Minister Lou Jiwei, who was widely seen as a voice for reform of China's fiscal system, was abruptly removed from his position and, according to party officials briefed on the matter, is expected to become head of China's national pension fund. **In another high-profile move, Minister of State Security Geng Huichang was also replaced. He will be succeeded by Chen Wenqing**, an appointment that was widely expected as Mr. Chen was made party secretary of the ministry last year in what was seen as a move by President Xi to strengthen his control over the country's security services.The **Ministry of State Security, or MSS**, is responsible for foreign intelligence and counterespionage. Mr. Geng had been in the post since 2007 and headed the ministry during a period in which the police and intelligence agencies were seen to have become excessively powerful under the leadership of the party's then security czar, Zhou Yongkang.

China approves law to tighten control on internet use
Associated Press, Staff reporters, 2016 11 07
Beijing - **China's legislature approved a cybersecurity law on Monday that human rights activists warn will tighten political controls and foreign companies say might hamper access to Chinese technology markets.** Chinese authorities say the law is required to prevent crime and terrorism. It also prohibits activity aimed at "overthrowing the socialist system," a reference to challenges to the ruling Communist Party's monopoly on power. Chinese leaders promote internet use for business and education but try to block access to material deemed subversive or obscene. The country has the biggest population of Internet users at 710 million, according to government data. The latest measure approved by the National People's Congress requires companies to enforce censorship and aid in investigations and imposes standards for security technology. It tightens controls on where Chinese citizens' data can be stored. Human rights groups complain it will extend controls on a society in which media are controlled by the ruling party and the internet has provided a rare forum for individuals to express themselves to a large audience.

Information sharing key to capturing corrupt officials (Canada)
China Daily, Zhou Wenting, 2016 11 04
Shanghai - **Information sharing has played a key role in bringing back corrupt officials who fled abroad to avoid trial, Ding Guping, director of the anti-corruption bureau at the Shanghai People's Procuratorate**, said on Thursday. Anti-graft officers have analyzed big data collected from various sources to learn about the movements of suspects, Ding said during a media briefing on the hunt for such fugitives since the launch of operation "Sky Net" in March last year. Sky Net was launched by the Chinese government, aimed at tracking down corrupt officials hiding abroad and confiscating their ill-gotten assets. A total of eight corrupt officials have been brought back to face trial from six countries - the **United States, Canada, Australia, Thailand, Japan and Singapore** - and more than 15 million yuan ($2.22 million) in illegal funds has been seized, according to the bureau. Ding said it cooperated with the police department, the state security bureau and the immigration inspection authority to obtain information, such as conversation and transaction records from popular messaging app WeChat and mobile payment service Alipay.

China, Australia sign MOU on anti-money laundering information sharing
Xinhua News Agency, Staff reporter, 2016 11 03
Beijing - **China and Australia have signed a Memorandum of Understanding on sharing information on money laundering, terrorist financing and other crimes**, said the Chinese

Foreign Ministry on Thursday. The MOU was signed on Tuesday in Beijing between Chinese Anti-Money Laundering Monitoring and Analysis Center (CAMLMAC) and Australian Transaction Reports and Analysis Center, said Foreign Ministry spokesperson Hua Chunying at a routine press briefing. The MOU will enable cooperation between the two countries on the collection, analysis and exchange of crime- related financial information. This is the 41st cooperation agreement CAMLMAC signed with counterparts overseas,

Cybersecurity law to enhance State security
Global Times, Deng Xiaoci, 2016 11 03
Beijing - **China's draft cybersecurity law, which stipulates that foreign technology firms should store important business data and personal data related to their operation within China, is aimed at effectively safeguarding State security as well as protecting people's privacy**, an expert said. The comment came after Reuters reported that short-term rental company Airbnb told Chinese users that it will store their personal data locally "as foreign tech companies operating in China respond to increasing regulatory pressure." A spokesperson with the Airbnb China confirmed with the Global Times on Wednesday on condition of anonymity that its parent company is moving Chinese mainland-based users' information including the guest bookings in China and Airbnb listings to local servers for greater localization.

Spy chief to take up advisory role on Hong Kong
South China Morning Post, Li Jing, 2016 11 03
Beijing - The **county's security chief is expected to stand down soon after being appointed to a senior role on an advisory panel for Hong Kong and Taiwan affairs**. Geng Huichang, the minister of state security, was on Tuesday named deputy director of the Chinese People's Political Consultative Conference (CPPCC) national committee's panel on Hong Kong, Macau, Taiwan and Overseas Chinese affairs, state-run Xinhua reported yesterday. The CPPCC is the country's top political advisory body. The advisory role for Geng, who has reached the mandatory retirement age of 65, was announced alongside new appointments for two other top officials. CaiFuchao, former head of the State Administration of Press, Publication, Radio, Film and Television, was named deputy director of the CPPCC committee for education, science, culture and health; and Liu Peng, former director of the State General Administration of Sports, was named deputy director of the CPPCC foreign affairs committee..

Return to Table of Contents/ Retour à la table des matières

Russia/Russie

New Report Lifts Curtain On Russia's Construction Of Powerful "Cyberarmy"
BuzzFeed News, Sheera Frenkel, 2016 11 07
San Francisco - An **investigation published early Monday on the eve of the US election details how Russia built one of the largest and most aggressive "cyberarmies" in the world.** As Russia's cyberoperations have risen in global prominence (and notoriety), the independent Russian news site Meduza has detailed how Russia built its current cyberabilities. While US officials recently took the unprecedented step of accusing Russia of trying to influence the upcoming vote in the US by hacking and leaking emails in an effort to damage the campaign of Democratic presidential nominee Hillary Clinton, cybersecurity experts claim that Russia has been meddling in the affairs of European states for years. The report reveals a system in which Russia's top political leadership is tasked with recruiting hackers and blackmailing criminals to

do their bidding, all the while testing the limits of their cyberabilities on eastern European states before, ultimately, turning their attention to the US this year. BuzzFeed News was given an early look at the report, authored by journalist Daniil Turovsky, and is publishing some of its findings here. Meduza found that: - **Russia's Ministry of Defense focused some of its earliest efforts on recruiting both from academic institutions and from hackers who may have arisen from the criminal underground. -** The teams were organized into groups known as "research squadrons," many of which lay within various Russian ministries and military units.

Hackers Release More E-Mails They Say Tie Putin Aide To Ukraine Crisis
Radio Free Europe, Staff report, 2016 11 03
Kyiv - **Ukrainian hackers claim to have broken into a second e-mail account linked to VladislavSurkov, a senior aide to Russian President Vladimir Putin**, releasing documents they say add to mounting evidence of the Kremlin meddling in Kyiv's affairs. The new e-mails were obtained by RFE/RL from the hackers in advance of their public release on November 3. If authentic, they provide detail about the extent to which Surkov's office worked to set up separatist enclaves in eastern Ukraine in 2014. The e-mails include plans that ostensibly show how associates of Surkov plotted to destabilize Ukraine's eastern Kharkiv region, researched Ukrainian politicians who openly supported weakening central power in a bid to exploit the country's political divisions, and helped establish the leadership of separatist groups in the Donetsk and Luhansk regions.

Moscow's Aggression, Source of Concern for the West
Asharq Al-Awsat, Taha Abed alWahed, 2016 11 04
Moscow, London - **Relations between London and Moscow have deteriorated after Russia's rising role in hot spots like Ukraine and Syria. but the tension began with the case of Alexander Litvinenko, the former KGB officer who was killed in London in 2006**. According to **Andrew Parker, head of Britain's internal intelligence agency MI5**, Russia had been a covert threat for decades, but what differs now from the Cold War era is that more sophisticated tools are at its disposal to pursue its anti-Western agenda. Speaking to the Guardian newspaper, Parker said that Russia "is using its whole range of state organs and powers to push its foreign policy abroad in increasingly aggressive ways, involving propaganda, espionage, subversion and cyber-attacks.

Hackers leak Putin plan to carve up Ukraine
London Times, Maxim Tucker, 2016 11 03
Kyiv - **Leaked Kremlin emails reveal how Russian operatives botched an attempt last year to foment an uprising in Kharkiv, the second largest city in Ukraine**. The emails, obtained by The Times, were apparently hacked from the inbox of Maria Vinogradova, an adviser to VladislavSurkov, President Putin's point man on Ukraine. The civilian intelligence analysis group Inform Napalm said that it had traced the adviser to an office in central Moscow used by the **FSB spy agency**. Three of the Ukrainian hackers involved in the leak met The Times on condition of anonymity, carrying concealed weapons but rejecting suggeserntions that the hack had been carried out with the help of Ukrainian or US intelligence services. Last month NBC News reported that the **CIA** had vowed to retaliate against Russia for a series of intrusions targeting American political institutions.

Le logo des renseignements ukrainiens a de quoi déplaire à Moscou
La Tribune (France), Jean-Christophe Catalon, 2016 11 03
Berlin - Ce blason multiplie les symboles anti-russes et entretient la rivalité entre les deux pays, alors qu'aucune porte de sortie n'a été trouvée lors du dernier sommet, à Berlin, le 19 octobre. Les relations entre l'Ukraine et la Russie ne sont pas près de se réchauffer. La semaine

passée, le président **Petro Porochenko a présenté le nouveau chef de la direction des renseignements du ministère de la Défense (GUR-MOU), VasylBurba**. Si l'événement a fait parler de lui, c'est moins pour la nomination que pour le logo des services de renseignements, affiché en grand derrière le chef de l'État. De la **CIA américaine à la DGSE française, en passant par le GRU russe, tous affichent un symbole international neutre**. - Le hibou : le choix du volatile n'est pas anodin. Le blason du GRU russe arbore une chauve-souris, animal dont l'un des prédateurs naturels est... le hibou.

Former director of Russian foreign intelligence to chair board of directors at Almaz-Antei
TASS News Agency, 2016 11 02
Moscow— **Mikhail Fradkov, a former Prime Minister and director of the Russian foreign intelligence service SVR, will chair the board of directors at the air defense systems manufacturing company Almaz Antei** and will simultaneously stand at the head of the **Russian Institute for Strategic Studies (RISS)**. President Putin took a decision of Fradkov"s appointment there after a meeting with the latter man and with the president of Rostech state corporation Sergei Chemezov. Earlier, Fradkov was supposed to become chairman of the board of trustees at the Russian state railway corporation RZD.

Return to Table of Contents/ Retour à la table des matières

Europe

Last-Intance Court Revokes Sentence of Bulgaria Ex-Spy Chief
Sofia News Agency, Staff report, 2016 11 08
Sofia - The **Supreme Court of Cassation (VKS) on Tuesday overturned a 10-year imprisonment sentence ruled for former intelligence head Kircho Kirov, BGNES wire service reports. Kirov, who headed the National Intelligence Service** (renamed last year to **State Intelligence Agency**) between 2002 and 2012, became the first high-profile official to be sentenced to jail time in Bulgaria's most recent history. He was found guilty of embezzlement over the misappropriation of BGN 4.7 M in public money. The VKS, however, handed the case to a lower-instance court on Tuesday, arguing a number of procedures in evidence assessment had been violated.

Pas de surveillance généralisée des mosquées
Le Matin (Suisse), Journaliste maison, 2016 11 08
Berne - Pas **question de surveiller préventivement les mosquées et les imams en Suisse, dit le patron du Service de renseignement (SRC) dans un entretien**. La base légale n'existe pas, même avec la nouvelle loi sur le renseignement. Et il ne voit aucune raison de le faire. « Il n'y a pas de base légale qui permette au SRC d'opérer une surveillance généralisée des mosquées et des imams en Suisse » , affirme le **directeur du SRC Markus Seiler** dans une interview au quotidien Aargauer Zeitungpubliée hier. De plus, « les mosquées, leurs imams et les organisations ne sont pas en eux- mêmes le problème » . La menace viendrait « le plus souvent de l'entourage » , poursuit M. Seiler. Le SRC peut agir préventivement lorsque des indices concrets d'une telle menace sont établis.

Germany fears UK may quit spy programme because of Brexit
The Guardian (London), Phillip Oltermann, 2016 11 07
Berlin - **Germany fears Britain may pull out of a key intelligence- sharing programme in May next year, a move that it says would create a "moment of weakness" in the fight against terrorism and jeopardise security across the EU**. As the continent remains on alert

for terrorist attacks, Berlin is understood to view intelligence as Britain's primary contribution to European collaboration, and fears it could use future cooperation as a bargaining chip in Brexit negotiations. According to documents seen by the Guardian, Germany is already lobbying the British government to renew its role in Europe's law enforcement agency, Europol, before its current collaboration runs out on 1 May 2017. In a response to a parliamentary question submitted by Germany's Left party, Angela Merkel's government confirmed that it believed the European commission should encourage the UK to remain in Europol.

Renseignement: comment Squarcini a utilisé la DCRI au bénéfice du camp Sarkozy
Radio France Internationale, 2016 11 05
Paris - En **France, l'enquête sur Bernard Squarcini, ex-patron de la Direction centrale du renseignement intérieur (DCRI) sous la mandature de Nicolas Sarkozy, révèle que l'ancien maître espion a gardé de nombreuses entrées dans la police**. Nos confrères du journal «Le Monde» ont eu accès au dossier de l'instruction. Il apparaît que Bernard Squarcini a privatisé la DCRI au bénéfice du camp Sarkozy. Bernard Squarcini fait partie de ces hauts fonctionnaires ouvertement sarkozystes mis sur la touche en 2012. Pourtant après ce départ forcé, Bernard Squarcini, dit le « squale », a continué à s'activer dans l'ombre du renseignement intérieur. L'enquête des juges Tournaire et Buresi jette une lumière cru sur ses agissements peu orthodoxes.

Bernard Squarcini, l'ange noir de la Sarkozy
Marianne, Marc Endeweld, 2016 11 04
Paris - Ancien grand patron du renseignement intérieur et homme de l'ombre de Nicolas Sarkozy, **Bernard Squarcini est désormais sous le coup d'une kyrielle de mises en examen.** Comme nombre d'autres proches de l'ex- président... Portrait du "Squale". La scène se déroule début octobre, une semaine après sa garde à vue conclue par une mise en examen pour «violation du secret de l'enquête», «trafic d'influence» et «détournement de fonds publics». Ce soir-là, Bernard Squarcini, le patron de la **Direction centrale du renseignement intérieur (DCRI)** sous Nicolas Sarkozy, s'affiche sans complexes dans les salons des Invalides où Valeurs actuelles, le magazine de la droite de la droite, fête son 50e anniversaire. La réception a lieu précisément au musée de la Chasse, ce qui n'est pas pour déplaire à ce flic, chasseur dans l'âme.

Former spy chief to head DFB ethics commission
Associated Press, 2016 11 04
Frankfurt— **Klaus Kinkel, a former spy chief and later Germany's justice and foreign minister, has been named the president of the newly created ethics commission of the German soccer federation**. Kinkel was elected at a federation congress in the eastern city of Erfurt. The commission is part of the DFB's declared drive for more transparency and integrity in an organization still reeling from the fallout of a financial scandal around the 2006 World Cup it hosted. The congress also extended the mandate of DFB president Reinhard Grindel until 2019. **Kinkel served as the head of West Germany's intelligence agency from 1978-82** and became the justice minister of a newly reunited Germany in 1991.

Malware used to spy on Iran talks in Geneva
The Local (Switzerland), Staff report, 2016 11 04
Geneva - A **large number of computers at a Geneva hotel that hosted delicate Iranian nuclear talks last year were infected with malware used for espionage**, Swiss prosecutors said on Thursday. The **Swiss Attorney General's office** (OAG) however said it had closed its investigation, since it had failed to determine who was behind the spying. Swiss investigators launched a probe in May last year based on "suspicion of illegal intelligence services operating

in Switzerland," searching a hotel that hosted the nuclear talks and seizing computer equipment. Those talks, which were held at a range of luxury hotels in Switzerland and Austria, concluded on July 14th 2015 with a landmark deal to rein in Iran's nuclear programme in exchange for the lifting of international sanctions.

Security police lobbies Parliament to defend funding
Yle (Finland), Staff report, 2016 11 04
Helsinki - **Parliament's Administration Committee is considering a statement tabled by Finland's security and intelligence police Supo**, in which the agency warns of dramatic consequences if its funding is not secured. The statement references the government's draft budget for next year, in which projected spending cuts targeting the police force are expected to have the effect of **reversing planned additional funding for Supo**, amounting to two million euros annually from 20017 to 2020. The statement was signed by Supo chief Antti Pelttari, and conformed to years of budget tactics as practiced by the Defence Forces. However instead of asking the question, "What part of the country should we not defend?" Supo laid out specific individual programmes that could face the chopping block if the agency were under-funded.

Former spy chiefs call for EU-US intelligence hub (Canada)
EU Observer, Andrew Rettman, 2016 11 03
Bratislava - **Europe and the US need an "intelligence hub" to fight terrorism**, with French and German ideas on EU military integration unlikely to bear fruit, Germany's former spy chief has said. The counter-terrorism hub, to be based in The Hague, would start out like the Schengen zone, the EU's passport-free travel area. It would involve a core group of trusted states such as **Canada, France, Germany, Switzerland, the UK, and the US**. Their intelligence services would form "operational task forces" and, as with Schengen's IT security system, would have access to each other's data. They would also create a "centre of excellence" to reform other EU states' services, which could join down the line. "I was one of the fathers of the Schengen agreement in the 1990s.

Les petites combines d'un maître espion
L'Obs, Violette Lazard avec Caroline Michel, 2016 11 03
Paris - Le **dessous des cartes L'enquête sur l'ex-patron du renseignement révèle que Bernard Squarcini n'a jamais coupé les ponts avec son ancienne maison**, tout en travaillant pour LVMH Juste avant d'être présenté aux juges, Bernard Squarcini a tenté de s'expliquer. « Je suis parti contraint et forcé, a déclaré l'ex-patron de la DCRI (le renseignement intérieur, devenu la DGSI en 2014). J'ai changé d'activité, mais j'ai gardé un état d'esprit identique à celui qui m'accompagnait en ma qualité de haut fonctionnaire. » Une défense bien maladroite. Entendu comme témoin (une situation inédite), **Patrick Calvar** reconnaît avoir accepté de faire la démarche, mais à titre exceptionnel. Qui sont ces deux Russes, résidant à Nice ? Des proches d'Alexandre Djouhri, un homme d'affaires lié aux plus gros contrats de la République, et qui se trouve aujourd'hui au centre d'une enquête sur le supposé financement libyen de la campagne de Sarkozy en 2007. Pourquoi protéger ces deux femmes, membres de la belle-famille de Djouhri ?

Didier Le Bret : « Daech va probablement retourner à la clandestinité »
Le Figaro, Marie-Amélie Lombard-Latune, 2016 11 02
Paris - **L'ex-coordonnateur national du renseignement livre son analyse sur les prochains défis de la lutte antiterroriste**. De juin 2015 à septembre 2016, en pleine période terroriste, **Didier Le Bret a été chargé par l'Élysée de veiller à la bonne coopération des services de renseignement français**. Un poste qu'il a choisi de quitter pour se présenter, en 2017, à la députation dans la 9e circonscription des Français établis hors de France (Afrique de l'Ouest,

Maghreb). Auparavant, ce diplomate, largement apprécié, a notamment travaillé à la Mission permanente de la France à l'ONU, a été ambassadeur en Haïti et a dirigé le Centre de crise du Quai d'Orsay. LE FIGARO. - Vous avez côtoyé les grands spécialistes du renseignement pendant un an. Quel principal enseignement en avez-vous retiré ? Didier LE BRET. - Il est frappant de voir à quel point nos services de renseignement - **DGSE, DGSI, Tracfin, DNRED** (1) - ont évolué. Ils ont pris le virage technologique. La DGSE a une longueur d'avance sur la DGSI qui est en phase de rattrapage. Ils se sont ouverts à tous les talents, ont su recruter des ingénieurs, des linguistes, des gens qui viennent du privé.

Tabloid: Supo suspects Russia of buying up Finnish property for military personnel
Yle (Finland), Staff report, 2016 11 02
Helsinki - **Finnish Security and Intelligence Police Supo has speculated that Russia could use property it has purchased in Finland as accommodation for its military**, according to the tabloid Iltalehti. In a report to presented to Parliament in September on threats facing Finland, Supo noted that a foreign power could make use of property purchased without any commercial or conventional real estate value. Supo speculated in the report that such real estate could be used for preparations to wield influence in a crisis situation. In practice, as a landowner, a foreign state could shut down road access or provide accommodation for troops, the agency said in the report.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Senior intelligence official: There's a basis for a deal with the Palestinians
Jerusalem Post, Herb Keinon, 2016 11 02
Jerusalem - A **senior Israeli military intelligence officer said that Palestinian Authority President Mahmoud Abbas is a legitimate peace partner, and that he has "consistently kept the peace and quiet,"** according to channel 10. Speaking to MKs and ministers recently, Brig.- Gen. Dror Shalom said "I know some of you might not like to hear this, but since 2004, there is a leader, Abu-Mazen (Abbas), who has generated quiet and opposed terrorism." He added that "there is a basis for a solution to the conflict." Shalom added that "it is true that we are not the world's problem, but we are an easy target." In early September, there was talk of a Russian- arranged meeting between Abbas and Prime Minister Benjamin Netanyahu, either in Moscow or in Luxembourg. "We'll see, either one - or any other place," Netanyahu had said, reiterating that Israel is "always ready for direct negotiations without preconditions." However, the meeting did not come to fruition.

Shin Bet denies torturing UK citizen over Hamas ties
The Jerusalem Post, Yonah Jeremy Bob, 2016 11 02
Jerusalem— The **Judea Military Court recently ordered the release of a British citizen facing charges of assisting terrorists, due to issues with Shin Bet (Israel Security Agency) interrogation methods leading to a confession,** Walla News reported Tuesday. **Faiz Mahmoud Ahmad Sharawi** will still face charges for helping terrorists smuggle funds and cellphones for Hamas in the West Bank as well as charges dating back to 2005. But if the court decision stands, he will be freed from custody throughout the trial procedure....Subsequently, The Jerusalem Post acquired a copy of the October 27 decision by Judge Lt.-Col. Azriel Levi and learned that the IDF prosecution has appealed the decision to the West Bank Military Appeals Court, which is set to hear the appeal Sunday. Painful handcuffing and threats are a

common method used in Shin Bet interrogations with the purpose of causing a detainee grave pain and suffering and to break his spirit." In contrast, the **Shin Bet denied any wrongdoing and emphasized the still pending allegations against Sharawi** for terrorism were "grave" as well as the IDF prosecution's pending appeal. It said, "the claims that torture were used during the interrogation... are baseless and groundless.

Syria Intelligence Chief: Aleppo Conflict will End in 10 Days if West Stops Supporting Militants
Fars News Agency, 2016 11 02
Tehran - **Syrian Air Force Intelligence Directorate head said that violence in the war-torn Syrian city of Aleppo could be ended within 10 days if the United States and the European Union end their practice of applying double standards to Syria** and supporting militants in the country. "It is solely US and European double standards, which are the reason behind terrorist activity in Aleppo. If they stop financing the militants for 10 days in a row, the Aleppo problem will be resolved and the militants will take their weapons and depart to join their friends in Turkey," Said **Syrian Air Force Intelligence Directorate head Jamil Hassan**, RIA Novosti reported. The intelligence officer, who is also a close aide to Syrian President Bashar Assad, stressed that international politics should not determine the course of the battle for Aleppo and that the United States continued to back terrorists at the highest diplomatic levels.

Return to Table of Contents/ Retour à la table des matières

Asia/Asie

Three Indian 'undercover agents' leave Pakistan
Pakistan Dawn, Syed Sammer Abbas, 2016 11 08
Islamabad - **Three out of eight Indian High Commission officials suspected of involvement in terrorist and subversive activities in Pakistan left for India on Tuesday**. Anurag Singh, Vijay Kumar Verma and Madhavan Nanda Kumar, allegedly members of the **Research and Analysis Wing (RAW)**, left for India earlier today on flight EK613 via Dubai. Rajesh Kumar, Amerdeep Singh Bhatti, Dharmendra Sodhi, who are also alleged members of RAW, are still in Pakistan, along with Balbir Singh and Jayabalan Senthil, who are said to be **Indian Intelligence Bureau** (IB) operatives. The FO during a press briefing last week revealed details of the eight Indian 'diplomats' in Pakistan, saying that a number of "Indian diplomats and staff belonging to **Indian intelligence agencies RAW and IB** have been found involved in coordinating terrorist and subversive activities in Pakistan under the garb of diplomatic assignments."

India, UK need to cooperate more on counter-terrorism: President
Press Trust of India, 2016 11 08
New Delhi - **India and the United Kingdom need to cooperate more on countering terrorism** which is the "biggest menace" to world peace and tranquillity, President Pranab Mukherjee has said. Talking to British Prime Minister Theresa May, who called on him last evening, the President said India sees the UK as a key partner in its growth and economy. "India would encourage more companies from the UK to partner in its national programmes like Make in India, Skill India, Digital India etc," the President was quoted as saying by the Rashtrapati Bhawan spokesman in a statement today.

S. Korea, Japan to hold talks on intelligence-sharing
Yonhap News Agency, Staff reporter, 2016 11 08

Seoul - **South Korea and Japan will hold their second round of talks in Seoul on Wednesday to discuss the signing of an intelligence- sharing pact that could allow the neighbors to better counter North Korea's growing threats**, the defense ministry said. "The two sides are expected to reach an agreement soon as the talks are under way based on the terms they tentatively agreed to in 2012," Moon Sang-gyun, spokesman for the Ministry of National Defense, said in a regular press briefing. In late October, the two agreed to reopen talks on a bilateral General Security of Military Information Agreement (GSOMIA), with the goal of concluding the pact by the end of the year. The United States welcomed the decision, saying the potential deal between its two Asian allies would bolster cooperation amid evolving nuclear and missile threats posed by Pyongyang. The first talks were held in Tokyo on Nov. 1. This year alone, the communist regime carried out two underground nuclear tests and some two dozen ballistic missile tests. Such developments have escalated global fears that the North is approaching its stated goal of developing a nuclear-tipped long-range ballistic missile that can hit parts of the U.S. mainland. Related to the GSOMIA, the two neighbors almost inked a deal, but the negotiations fell through due to negative public sentiment in South Korea about signing such a pact with its former colonial master. Korea was a colony of Japan from 1910 to 1945.

Indonesia calls for greater intelligence cooperation against terrorism at Interpol forum
Straits Times, Arlina Arshad, 2016 11 07
Jakarta - **Indonesian Vice-President Jusuf Kalla on Monday (Nov 7) urged top international security officials to increase intelligence sharing between nations to fight the threat of terrorism**. "Terrorism is an extraordinary crime, and countering it requires Interpol member countries to cooperate and focus on intelligence," he said. "Without same and accurate information in every member state, we will have difficulty in tapping the Interpol network nationally and globally." Mr Kalla was speaking at the opening of the 85th International Police (Interpol) General Assembly, which runs to Thursday in Nusa Dua, Bali. The forum, attended by **Interpol president Mireille Ballestrazzi**, secretary general Jürgen Stock, and some 1,360 police chiefs and other delegates from 167 Interpol member countries, is expected to discuss terrorism, cybercrime and drug and people smuggling.

Indian diplomats have contacts with Taliban
The International News, 2016 11 04
Islamabad - **Pakistan on Thursday took a step forward to internationalise and reached out to foreign capitals regarding the activities of Indian state-sponsored subversive and terrorist activities inside Pakistan** -- having contacts with Taliban and aiming at sabotaging the China Pakistan Economic Corridor -- which has led to nine Indian officials including diplomats at the Islamabad Mission found involved in promoting terrorist activities and terror financing. The government says it has pursued a policy of restraint, patience and sobriety which has been appreciated the world over.

India, China likely to sign anti-terror pact
Times of India, Dipanjan Roy Chaudhury& Rahul Tripathi, 2016 11 04
New Delhi - **India and China are likely to sign a major security cooperation agreement, which would enhance their efforts to jointly fight terrorism and international crime**, when New Delhi hosts Chinese Communist Party's influential politburo member MengJianzhu next week. Meng is likely to visit India on November 8, when the two sides are expected to seal the umbrella security cooperation pact. The terms, which are currently being negotiated, will also include a mutual legal assistance treaty mechanism, according to people familiar with the matter.

Indian diplomats in Pakistan handled TTP factions: Foreign Office
Pakistan Dawn, Syed Sammer Abbas, 2016 11 03
Islamabad - The **Foreign Office (FO) on Thursday said eight Indian diplomats in Pakistan - allegedly members of the Research and Analysis Wing (RAW) and Indian Intelligence Bureau (IB) - are suspected of involvement in terrorist and subversive activities including the handling of Tehreek-i- Taliban Pakistan (TTP) factions in Pakistan**. FO Spokesman NafeesZakaria during a weekly press briefing in Islamabad said, "As you are aware, a number of Indian diplomats and staff belonging to Indian intelligence agencies RAW and IB have been found involved in coordinating terrorist and subversive activities in Pakistan under the garb of diplomatic assignments." Zakaria provided details of the activities of the 'undercover agents', alleging that the suspected RAW and IB operatives handled TTP factions, fueled secatarianism in Pakistan and created unrest in Balochistan, Sindh, and Gilgit-Balistan (GB).

Pakistan may expel two Indian diplomats in Islamabad for spying
The Express Tribune, Kamran Yousaf, 2016 11 03
Islamabad - **Two Indian diplomats in Islamabad have been caught spying for India's premier spy agency, Research and Analysis Wing (RAW), and may be expelled**, sources told The Express Tribune on Wednesday. According to sources, Rajesh Kumar Agnihotri has been identified as RAW station chief, while Balbir Singh has been identified as an officer of the Indian Intelligence Bureau (IB). Both officers were working at the Indian High Commission office in Islamabad. A source said both Agnihotri and Balbir were involved in terrorist activities in the country.

Pakistan accuses eight Indian diplomats of espionage, terrorism
Reuters, 2016 11 03
Islamabad— **Pakistan on Thursday named eight Indian diplomats it accuses of espionage and terrorism**, as tension mounted between the nuclear-armed rivals following days of artillery duels and skirmishes on the border dividing the disputed Kashmir region. The foreign ministry said six Indian embassy staff worked for **New Delhi's Research & Analysis Wing (RAW) intelligence agency**, while two were operatives for the Intelligence Bureau agency. Their names were leaked to Pakistani media overnight. In response, India said it "completely rejected the baseless and unsubstantiated allegations" leveled by Pakistan against officials at its high commission in Islamabad. The foreign ministry statement gave an eight-point list of the diplomats' espionage activities.

Four officers likely to be called back from India
Pakistan Dawn, BaqirSajjad Syed, 2016 11 02
Islamabad - **The government is considering pulling out from India four of its officers posted in Pakistan's High Commission in New Delhi, days after Indian authorities declared one official persona non grata.** "This is under consideration. A final decision would be taken shortly," a source at the Foreign Office said on Monday. The names of the officers -- commercial counsellor Syed Furrukh Habib and first secretaries Khadim Hussain, Mudassir Cheema and Shahid Iqbal -- were made public after Indian officials released to media a recorded statement of a high commission staffer Mehmood Akhtar, who was expelled from India after being declared persona non grata.

New leak shows Pakistani ISPs may have been hacked by the NSA
The Express Tribune, Tech Desk, 2016 11 02
Islamabad - A **group called the Shadow Brokers has released a new cache of data purporting to be taken from the NSA in a Medium post titled "Trick or Treat" -- revealing hundreds of IP addresses apparently compromised by the NSA as part of its operations**.

Interestingly, the majority of the nodes are located overseas, including compromises in China, Russia, India, or Pakistan, presumably to make it difficult for targets to attribute any attack launched through the network. At least four Pakistani Internet Service Providers (ISPs) are also part of the leaked list.

Dawn report suggests bigger spy ring, names 4 diplomats
The Hindu, Kallol Bhattacherjee, 2016 11 02
New Delhi - The **diplomatic battle between neighbours heated up on Tuesday after a media report from Pakistan said Islamabad was considering withdrawal of four of its diplomats from India**. The report suggesting that the diplomats were allegedly engaged in espionage in India drew a strong response from Pakistani diplomatic sources, who dismissed the charges as baseless. Government sources termed the episode an "internal" matter of Pakistan. Citing sources in the Ministry of Foreign Affairs in Islamabad, the Karachi-based Dawn reported that Mehmood Akhtar, the diplomat who was expelled by India on October 29 for spying, had named the four officials in a recorded statement in Delhi.

Return to Table of Contents/ Retour à la table des matières

Africa/Afrique

Sudan arrests more opposition activists over fuel prices
Agence France-Presse, 2016 11 06
Khartoum— **Sudanese security agents have arrested several opposition politicians over the past two days** to prevent protests against Khartoum's decision to hike fuel prices, their parties said on Sunday. **Sudan's all-powerful National Intelligence and Security Service (NISS)** arrested on Friday the deputy chief of the opposition Sudanese Congress Party, Khaled Omar, from his home in Khartoum. Omar was arrested after he delivered a speech criticising the hike in prices of petrol and diesel by about 30 percent. Since then threee other members of Omar's party were also arrested, a senior member of their party, Bakri Youssef told AFP.

Ten people on top spook shortlist
Pretoria News, 2016 11 02
Pretoria— The **joint standing committee on intelligence wants to speedily appoint the new inspector-general of intelligence in the coming weeks after it shortlisted 10 people for the position**. The committee wants to conclude all processes before the end of the year with Parliament left with effectively four weeks to finish its business for the year. The appointment of the IG for Intelligence has been delayed for several months after fights in the National Assembly on the candidate to be backed by all parties. Former ANC MP Cecil Burgess was initially picked for the job in March but his appointment fell through after he did not secure the support of all parties. He was not on the list of the 10 people shortlisted for the job. The **new inspector-general will keep a watch on the conduct of intelligence agencies, including State Security Agency spooks.**

Return to Table of Contents/ Retour à la table des matières

Americas/Amériques

Journalists reporting on Venezuelan crisis risk temporary and prolonged detentions
Journalism in the Americas blog, 2016 11 04

Unidentified Placeline— **Covering protests, photographing food lines or taking video inside a hospital can be risky for journalists working in Venezuela** today. Various reporters and photojournalists working in the country have been subjected to temporary and prolonged detentions in the process of carrying out their jobs in recent months. Recently, **agents with Venezuela's Bolivarian Intelligence Service (Sebin) detained Matt Gutman, a correspondent for U.S. network ABC News,** on Oct. 24 while he was reporting on conditions at a hospital in the state of Carabobo. Gutman, and a cameraman and a Venezuelan doctor who were also detained with him, was kept in custody until the night of Oct. 26. ABC News confirmed the detention on Oct. 27 and said Gutman "was released without incident. The Press and Society Institute (IPYS for its acronym in Spanish) of Venezuela told the Knight Center that it recorded 22 instances of arbitrary detentions of directors, journalists and photojournalists between Jan. 1 and Sept. 30 of this year. According to the organization, a majority of the detentions were carried out by state police (8). The other entities behind the detentions have been: National Armed Forces (7), the **Bolivarian National Intelligence Service** (Sebin) (3), courts (2) and airport authorities (2).

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

09-11-2016 to/au 15-11-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Police, Power and Privacy
Toronto Star and CBC News, Staff reporters, 2016 11 15
Ottawa - The **RCMP has provided unprecedented access to the Toronto Star and the CBC in an effort to make its case that antiquated law**s and diminished police powers in the digital age are allowing suspected terrorists, drug gangs and child abusers to operate beyond the law. Journalists from the two media outlets have reviewed the details of 10 high- priority cases after clearing RCMP security checks for access to "top- secret" information. In each case, investigators were stonewalled by legal and technical obstacles in accessing digital evidence, the Mounties say. Most of the suspects remain at large. These cases stand at the centre of an emerging national debate. Police argue they are on the losing side of a digital divide, while on the other side are tech-savvy criminals who are shielded by impenetrable encryption, telecommunication companies and technology manufacturers. **Privacy advocates argue that police have never before had such powers of surveillance** and that they have failed to provide evidence that the public's safety is in jeopardy. **They are equally alarmed by the recent Federal Court ruling that denounced the national spy agency, CSIS, for illegally gathering the private information of Canadians**, and by news that Quebec police forces intercepted and tracked the cellphones of as many as 10 journalists to discover their sources. "We need a public debate," said RCMP Chief Supt. Harold O'Connell, the force's director general of national security investigations. "We can influence, we can tell you what we think the lay of the land is, and then you, as Canadians and legislators, decide where you want us to be."

Inside RCMP's file room
Toronto Star, Robert Cribb, 2016 11 15
Ottawa - The **RCMP shared details of 10 ongoing "high-priority" investigations with the Toronto Star and CBC News to begin a public debate on expanding police capabilities while investigating crimes involving digital and online evidence**. This coincides with a federal review of **Canada's Anti-Terrorism Act (Bill C-51)** and a public consultation on the government's **Green Paper on National Security**, which includes proposals to enhance police digital capabilities. To allow access to the investigations, the RCMP conducted security screening and granted top-secret clearances to Robert Cribb of the Toronto Star and Dave Seglins of CBC News. The RCMP provided summaries and interviews on the cases but withheld names, locations and key details that could compromise ongoing investigations, prosecutions and secretive police techniques.

Canada's energy sector braces for rising threat from activists
Globe and Mail, Shawn McCarthy, 2016 11 14
Ottawa - **Canadian security experts are increasing their vigilance against activists' threats to the country's energy infrastructure**, as civil- liberties advocates worry about the use of improper surveillance on peaceful opponents to major projects. In what is billed as a training workshop, **Carleton University's Infrastructure Resilience Research Group** is playing host to a closed-door conference on Monday and Tuesday for lawyers, police, regulators and industry representatives on "the challenges of dealing with natural resource development projects and activism." One of the organizers, professor emeritus Martin Rudner, said there are significant threats from "domestic extremists" to Canada's energy infrastructure, including pipelines, generating stations and transmission lines. Prof. Rudner is active on several industry-

government-academic networks that consult on protection of critical infrastructure, including the energy and utilities- sector network managed by Natural Resources Canada. But critics argue police and intelligence agencies are armed with overly broad definitions of national security and critical infrastructure, which include projects that are in the planning and construction phase, in addition to assets that are operational and delivering energy across the country. "A lot of these concerns are overblown," Ottawa lawyer **Paul Champ** said. He is **a board member of the British Columbia Civil Liberties Association that has alleged RCMP and the Canadian Security Intelligence Service (CSIS) engaged in illegal surveillance of Canadians protesting against Enbridge Inc.'s proposed Northern Gateway pipeline.** Mr. Champ said the RCMP and CSIS became more active in natural-resources development under the former Conservative government, which defined national-security threats to include actions that could affect the economic stability of the country, and then defined resource development as essential to the health of the Canadian economy.

RCMP tracked 89 indigenous activists considered 'threats' for participating in protests
National Post, Sarah Craig, 2016 11 14
Toronto - The **Trudeau government says Canada's national police force respects the right to peaceful demonstrations by indigenous activists**, after it was revealed the **RCMP compiled a list and distributed profiles of indigenous protesters** it deemed "threats" who it determined were potentially willing and capable of criminal activities. Dubbed Project SITKA, the RCMP began soliciting information on indigenous activists who could be perceived "to have committed or commit" crimes from all of its divisions and local police departments across the country in March 2014. Using the information it received and data collected from social media, the Mounties identified 313 activists -- attendees of protests on issues ranging from natural resource development to missing and murdered indigenous women -- who potentially posed a "criminal threat to Aboriginal public order events." The RCMP did not reply to a request for comment.

How much data retention is reasonable in counter terrorism?
Hill Times, Phil Gurski, 2016 11 14
Column - A new salvo has been fired in the continual contest that pits national security vs. privacy rights in Canada. A **Federal Court judge has ruled that the Canadian Security Intelligence Service illegally held on to data that was not threat-related for an unnecessary period of time**. The judicial decision was announced the same week that news broke of several Quebec journalists whose call logs had been monitored by police. All in all a bad week for those we expect to protect us and our freedoms. Not surprisingly, the CSIS story is getting a lot of attention. Also not surprisingly, some of the facts are being twisted and the story is being manipulated to fit various agendas. This issue is an important one and needs a fuller explanation. I would like to try to provide that explanation. Where the controversy lies is in the retention of the data collected, more accurately the "metadata" (essentially data about data, i.e. phone numbers or email addresses but not content). The law states that CSIS should only collect what is strictly necessary for its investigations and that information that does not meet this definition must be destroyed. **Judge Simon Noel** ruled that CSIS acted illegally by retaining the metadata that was not threat-related in a section called **ODAC--the Operational Data Analysis Centre. Why would CSIS do this?** The answer is very simple. Today's threat, at least as far as terrorism goes, is constantly shifting and requires more tools and more resources to counter. Terrorists use the panoply of social media and communications technology available to them and security services are having a hard time keeping up. Most importantly, terrorists are social animals, much the opposite of the current mythological "lone wolves" paradigm that unfortunately now dominates the discourse.

Spies in new glass houses: Ottawa's electronic espionage agency budget blows past CSIS, tops $600 million
Ottawa Citizen, Ian MacLeod, 2016 11 12
Ottawa - The **federal government is spending more than half a billion dollars on its electronic spying service this year, six times its pre-9/11 budget and a reflection of how the Internet has morphed into a juicy intelligence target**. The **Communications Security Establishment, or CSE, is to receive $605.6 million, according to supplementary estimates tabled in Parliament.** That's $22 million more than originally planned, much of it carried over from CSE's 2015-16 budget. In 2000, by comparison, the agency's annual spending stood at $97 million. What's more, the looming U.S. presidency of Donald Trump is already prompting leading national security experts Wesley Wark and Craig Forcese to suggest Canada consider enhancing its foreign intelligence capacity to be better able to resist "the gravitational pull of the U.S. alliance relationship" should it move in "an unpalatable direction," says Forcese. Their main preoccupation is counter-terrorism, though Russian expansionism is rekindling targeting not seen since the end of the Cold War. Though the CSE received no new powers under the **2015 Anti-terrorism Act** (formerly Bill C-51), its mandate includes providing electronic spying assistance to other security agencies and law enforcement. Security intelligence experts suspect much of whatever assistance **CSE renders is for the Canadian Security Intelligence Service, or CSIS, Canada's human spy service. (CSIS funding is pegged at $593.9 million for 2016-17.)** Earlier this year, the independent watchdog agency monitoring the legality of CSE activities disclosed the agency had for years been unlawfully sharing with the Five Eyes metadata associated with Canadians' private communications. The practice was halted in 2014. The 11-member Office of the Communications Security Establishment Commissioner operates on $2.2 million in annual funding and is headed by Jean-Pierre Plouffe, a former military and Quebec court judge. William Galbraith, its executive director, said current funding is sufficient and that the office is considering adding another full-time review expert to the eight now employed.

Surveillance: Mulcair veut que Goodale et Wilson-Raybould s'expliquent
La Presse canadienne, Pierre Saint-Arnaud, 2016 11 09
Ottawa - Le **chef néo-démocrate, Thomas Mulcair, demande aux ministres de la Sécurité publique, Ralph Goodale, et de la Justice, Jody Wilson-Raybould, de rendre des comptes devant le Comité permanent de la sécurité publique sur la surveillance des citoyens et des journalistes**. De passage à Montréal, mercredi, M. Mulcair a exigé que les deux ministres s'expliquent sur la **tentative du ministère de la Justice d'empêcher que ne soit rendue publique l'information voulant que le Service canadien de renseignement de sécurité (SCRS)** ait illégalement recueilli et conservé des données personnelles de citoyens canadiens pendant une décennie. «Comment se fait-il que le ministère de la Justice se soit battu en Cour très récemment à Ottawa pour empêcher qu'on dise la vérité aux Canadiens sur le fait que le SCRS a maintenu et gardé pendant des années, complètement illégalement, un ensemble de renseignements sur des particuliers au Canada, sur des citoyens canadiens?», a demandé M. Mulcair.

Want to move to Canada? Well, their spy agency is involved in mass surveillance too
International Business Times (UK), Mary-Ann Russon, 2016 11 09
London - The US is not the only country to have grave problems relating to government mass surveillance - the **Federal Court of Canada recently ruled that the Canadian Security Intelligence Service (CSIS)'s practice of collecting and retaining data on citizens for over a decade is unlawful.** US citizens who voted for Hillary Clinton in the US presidential elections have been taking to Twitter to announce that they intend to move to Canada in the wake of business entrepreneur Donald Trump's victory, but it might be worth noting that although

Canada has Justin Trudeau as prime minister, it doesn't mean the country doesn't have some similar problems. Intriguingly, the Canadian federal court found that the judiciary had no idea that bulk surveillance was being carried out at all, despite the fact that judges are required to sign off on warrants and intelligence programmes.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

'Knife fight' as Trump builds an unconventional national security cabinet
CNN.com, Multiple reporters, 2016 11 15
Washington - **Donald Trump's transition is being marked by sharp internal disagreements over key cabinet appointments and direction, both for internal West Wing positions and key national security posts**, sources involved in the transition team tell CNN. One source with knowledge of the transition described it as a "knife fight." The divisions are being played out as Trump considers key appointments in the national security and diplomatic sectors, including secretary of state, with mainstream conservatives supporting John Bolton against Rudy Giuliani, who is seen as a loyalist to Trump. On other key national security appointments, there is more agreement. Sen. Jeff Sessions is now the leading contender for attorney general, and is in the mix for secretary of defense as well, say multiple sources with knowledge of the transition. **Retired Lt. General Ron Burgess, former director of the DIA, is a leading contender for director of national intelligence.** Retired General Michael Flynn is leading candidate for national security adviser. Pete Hoekstra, a long-serving former congressman from Michigan who chaired the House Intelligence Committee from 2004-2007 is thought to be in the running for the same role or director of the CIA.

How Trump Can Gut Obama's National Security Policies on Day One
NBC News, Ken Dilanian, 2016 11 15
New York - **President Obama made aggressive use of the CIA and Special Operations Forces to hunt and kill al Qaeda, ISIS and other terror groups**. But he also imposed a set of rules designed to regulate the conduct of U.S operatives -- banning torture, for example, and minimizing the risk of civilian casualties in drone strikes. President-elect Trump, who campaigned against those rules, would be able to undo most of those rules in his first hour in office. In fact, if he chooses to do so, Trump can quickly reshape large swaths of American national security policy, much of which is governed by executive orders and presidential policy guidance that can be overridden by the president's signature. That includes U.S. sanctions on Russia, and its recent rapprochement with Cuba. "The range of unilateral presidential authority is astonishingly broad," said **Steven Aftergood, who directs the project on government secrecy at the Federation of American Scientists**. "If you look at the presidential policy directives issued by Obama, they cover topics as diverse as biological weapons, nuclear weapons policy, intelligence surveillance policy, cyber operations, maritime security, arms-transfer policy, and on and on. And because it is based on presidential authority, it can also be revised and reshaped by a new president."

Snowden warns of increase in U.S. domestic spying after Trump victory
Reuters, Staff report, 2016 11 15
Buenos Aires - **Donald Trump's election as U.S. president raises concern that Washington may increase the intrusiveness of domestic intelligence gathering, former U.S. spy agency contractor Edward Snowden said** on Monday, warning that democratic checks and

balances were losing ground to authoritarianism. Snowden lives in Moscow under an asylum deal after he leaked classified information in 2013 that triggered an international furor over the reach of **U.S. spy operations**. He spoke at a teleconference hosted by Buenos Aires University's law school. "We are starting to substitute open government for sheer authoritarianism, a government based not upon the principle of informed consent granted by people who understand its activities but rather a trust in personalities, a trust in claims, a trust in the hope that they will do the right thing," Snowden said.

Trump's most important new partner: The intelligence community
Washington Post, Michael Hayden, 2016 11 14
Op-ed **- I don't envy the president-elect's intelligence briefers. Candidate Donald Trump stormed through the election as a primal force of dystopia, anger and accusation. More often than not, there was little effort to back up accusations with fact. Many of them were, in fact, not true. With that record, a fair question is: What role will facts and fact-bearers play in the Trump administration.** What happens when he is told that Syrian refugees are already extremely vetted? Or when his intel briefer dishes up that the Russians really aren't targeting the Islamic State? What controls - - new data or preexisting mythology? For many authoritarian populists (think the leaders of Turkey, Venezuela and Russia), it's the latter. The intelligence community sometimes makes mistakes, but it strives to create a fact-based, inductive view of the world. From as much data as it can acquire, it works to create general conclusions. Not surprisingly, there are often tensions with policy makers who tend to be deductive, trying to apply their vision to specific situations. For its part, the intelligence community needs to understand how the president-elect learns and how contrarian ideas are best served up to him. Not an easy task. And the intelligence community needs to stand its ground, even, or especially, when it is irritating the client in chief. Simply writing down an unwelcome assessment or saying it once is not enough.

Trump Backer Pushes for New CIA 'Enhanced Interrogation'
The Daily Beast, Kimberly Dozier, 2016 11 14
Column - The **former senior CIA officer who championed waterboarding hopes President-elect Donald Trump will bring harsh interrogation methods--and bring the CIA back into the business of interrogating terrorist suspects**. "We have to be able to capture terrorists. We have to be able to interrogate them. We don't do that anymore," said **Jose Rodriguez**, who led the CIA's clandestine service during the Bush administration. A Trump supporter, Rodriguez said he didn't want to lead the CIA, though he has been named as a possible pick. But he does want to bring back some form of now-illegal interrogation measures, like waterboarding, sleep deprivation, and other so-called "enhanced interrogation methods" approved by the Bush White House to question terrorist suspects in the wake of the al-Qaeda attacks of 9/11.

3 slain troops worked for CIA in Jordan
Washington Post, Thomas Gibbons-Neff & Joby Warrick, 2016 11 13
Washington - The **three Army Special Forces soldiers killed at a Jordanian military base this month were working for a CIA program to train moderate Syrian fighters when they were shot at a checkpoint under still- unclear circumstances**, U.S. officials said. The Nov. 4 attack is thought to be the deadliest single incident involving a CIA team since December 2009, when seven officers and contractors were killed in a suicide bombing in Khost, Afghanistan. The three soldiers - all members of the 5th Special Forces Group based at Fort Campbell, Ky. - were killed by a Jordanian soldier at an entry control point to Prince Faisal Air Base near Jafr, in the southern desert about 150 miles south of the capital, Amman, according to the officials. The shooter also was wounded in what was described by U.S. and Middle Eastern sources as an exchange of gunfire. The soldiers, identified as Staff Sgt. Matthew Lewellen, Staff Sgt. Kevin

McEnroe and Staff Sgt. James Moriarty, were among about 2,000 U.S. troops working in Jordan while participating in the U.S.-led campaign fighting the Islamic State.. The **CIA declined to comment on the shooting incident or on the soldiers' possible role in agency programs**.

Hillary Clinton Blames F.B.I. Director for Election Loss
New York Times, Amy Chozick, 2016 11 13
Washington - **Hillary Clinton on Saturday cast blame for her surprise election loss on the announcement by the F.B.I. director, James B. Comey, days before the election that he had revived the inquiry into her use of a private email server**. In her most extensive remarks since she conceded the race to Donald J. Trump early Wednesday, Mrs. Clinton told donors on a 30-minute conference call that Mr. Comey's decision to send a letter to Congress about the inquiry 11 days before Election Day had thrust the controversy back into the news and had prevented her from ending the campaign with an optimistic closing argument. "There are lots of reasons why an election like this is not successful," Mrs. Clinton said, according to a donor who relayed the remarks.

Inside the mind of Trump's national security guru
CNN.com, Peter Bergen, 2016 11 13
Analysis: One is the son of a multimillionaire real estate developer from New York City who avoided service in Vietnam and whose experience and knowledge of the military and the national security realm are close to zero. The other is a retired three-star general -- one of nine children who grew up in a small house in Middletown, Rhode Island. He went on to run intelligence for the US Joint Special Operations Command, which includes SEAL Team 6 and Delta Force. Later he commanded the Defense Intelligence Agency, the US military's overall intelligence organization. But **riding on a wave of ultranationalistic rhetoric, Donald Trump and his top adviser on national security, retired US Army Lt. Gen. Michael Flynn, have now catapulted from political outsiders to the White House. On Friday, Trump appointed Flynn as one of five vice chairs of his transition team**. NBC reports that Flynn is being considered as either Trump's national security advisor or secretary of defense. The latter position would require a waiver to allow a former military officer to assume a Cabinet position. Understandably, a request for a comment from Flynn about what his future role in the Trump presidency might be did not yield a response. **Flynn's advice to the President-elect is all the more important because he is the only person on Trump's team with any significant experience in America's post-9/11 wars that continue to grind on in Afghanistan, Iraq, Libya, Pakistan, Somalia, Syria and Yemen.**

President-elect Donald Trump is about to learn the nation's 'deep secrets'
Washington Post, Bob Woodward, 2016 11 13
Washington - **One of the most important phases of the transition to power for President-elect Donald Trump includes briefings on U.S. intelligence capabilities and secret operations as well as separate descriptions of the extraordinary powers he will have over the military**, especially contingency plans to use nuclear weapons, according to officials. Though Trump has been given some intelligence briefings on threats and capabilities, there are a series of separate briefs scheduled for the president-elect into what Obama has called "our deep secrets." First is a detailed look at technical and human intelligence sources and methods that provide critical information on **Special Access Programs** -- the most sensitive top-secret undertakings -- for drone strikes and other intelligence operations. This would include the disclosure, if Trump wants the names, of the dozens of officials abroad paid by the **CIA**, to the tune of millions of dollars. Though entitled, presidents normally have not asked for names unless the secret relationship involves a particularly important CIA asset. A second briefing will

be on the covert actions undertaken by the CIA that are designed to change events abroad without the hand of the United States being revealed publicly..

Trump now has access to nation's most valuable intelligence
Fox News, Catherine Herridge, 2016 11 12
Washington - **President-elect Donald Trump will now have access to the most authoritative and highly classified intelligence produced by the U.S. government**, Fox News has learned. Two intelligence sources confirmed that the President's Daily Brief, or PDB, is now available to Trump - after the White House, before Tuesday's election, had directed that the winner have full access to the material, to ensure a smooth transition. The sources told Fox News they do not anticipate the briefings will begin until next week at the earliest. The PDB is like a highly classified newspaper for the president, and now the president-elect. It is significantly different than the information provided in briefings for candidates; those briefings act as primers to help bring candidates up to speed on topics like China, Iran and the Islamic State.. Fox News has also learned that, **because the briefing itself must be done in a secure facility, the White House has a dedicated transition space nearby that can be used by the president-elect to receive the PDB**. If Trump were to receive the brief in New York City, the president-elect would need to travel to a secure federal facility, such as the FBI office.

Concerns raised over Trump accessing global surveillance network
The Guardian (London), Ewen MacAskill, 2016 11 12
London - **Privacy supporters criticise Obama for failing to change legislation following Edward Snowden's NSA revelations**. Privacy and human rights campaigners have expressed fears over the prospect of Donald Trump gaining access to the vast global US and UK surveillance network.They criticised Barack Obama's administration for being too complacent in the wake of the 2013 revelations by the NSA whistleblower, Edward Snowden, and making only modest concessions to privacy concerns rather than carrying out major legislative changes. The concern comes after Snowden dismissed fears for his own safety if Trump, who called him "a spy who has caused great damage in the US", was to strike a deal with Vladimir Putin to have him extradited.. The UK surveillance agency **GCHQ is so tied up with America's NSA, often doing work on its behalf,** it could find itself facing a series of ethical dilemmas. On the campaign trail, Trump made an ambiguous remark about wishing he had access to surveillance powers.

Donald Trump May Select an Architect of Bush's Torture Program to Run CIA
The Intercept, Lee Fang, 2016 11 12
Washington - **Donald Trump may select Jose Rodriguez, one of the primary architects of the George W. Bush torture program, to run the Central Intelligence Agency**, according to a law firm with close ties to Trump. Rodriguez, the **former director of the National Clandestine Service, helped developed the CIA black sites, secret prisons operated in foreign countries where interrogators used a range of torture tactics**, including the use of "waterboarding," the simulated drowning technique once used by the Khmer Rouge and Nazi agents to glean information from detainees. At least 136 individuals were detained and tortured by the CIA. Interrogation tactics also included forced nudity, sleep deprivation while being vertically shackled, and confinement in a small box. Rodriguez is unapologetic about his role in the program, telling 60 Minutes that "we did the right thing for the right reason," even if it meant "going to the border of legality." The **suggestion that Rodriguez may head the CIA was made in a post-election prediction document published by Dentons**, a law and lobbying firm where Trump confidant Newt Gingrich serves as a senior advisor.

'Black Swan' Exercise to Give Trump's Team Practice for Security Crisis
ABC News, Alexander Mallin, 2016 11 12
Washington - **Donald Trump's transition team is getting a helping hand from the Obama administration on national security matters**. The **administration is giving the president-elect and a select few of his top advisers sensitive intelligence briefings**. And, in addition, Trump and his team will take part in two so-called 'black swan' exercises that simulate a domestic or national security emergency. The exercises are intended to help an incoming administration learn how to manage a crisis in real time in case there is some kind of global or domestic emergency in the first days of a Trump presidency. A **black swan exercise would, for example, ensure that a fledgling Trump administration knows how to activate the proper federal agencies to maintain stability.**

'Fearful' national security officials prepare for major shift in US policy
The Guardian (London), Spencer Ackerman, 2016 11 12
Washington - A **US intelligence officer operating in a dangerous part of the world prepared this week for Donald Trump's presidency by making a pact with a colleague: they resolved to disobey any order to commit torture**. The two officers' pledge reflects a wider debate within the national security bureaucracy, as some officials - concerned by Trump's authoritarian inclinations - debate whether to quit in protest at his electoral victory or to remain at their post in the hope of checking impulses they consider dangerous. Officials in the US military, **intelligence services**, diplomatic corps and federal law enforcement have told the Guardian that Trump's suggestions represent such a departure from the norms of American governance that they are contemplating internal resistance or a career change.

Comey faces complicated path under Trump administration
Associated Press, Staff report, 2016 11 10
Washington - **FBI Director James Comey faces a complicated path under a Donald Trump administration.** Does he try to serve out the remaining seven years of his term under a president who has publicly questioned the FBI's integrity? Or does he stay on as a safeguard against executive power and a guide for a novice president on complex national security matters? The term of the FBI director is set at 10 years as an affirmation of the bureau's political independence, and some other chiefs including Robert Mueller, Comey's predecessor, have served presidents of both parties. But Comey would be in the delicate position of working with a president who lobbed occasional criticisms from the campaign trail against the nation's premier law enforcement agency. Though attention had centered on whether Comey could have co-existed with a Hillary Clinton presidency, given the FBI's investigation into her email practices and his own public statements about the probe, that question applies at least equally to a Trump administration.

Team Trump Struggling to Fill National Security Jobs
The Daily Beast, Kimberly Dozier, Shane Harris, 2016 11 10
Washington - **President-elect Trump is scrambling to line up senior officials to run the government's sprawling intelligence and homeland security bureaucracy**. Team Trump is struggling to fill numerous key slots or even attract many candidates because hundreds have either sworn they'd never work in a Trump administration or have directly turned down requests to join, multiple current and former U.S. officials with direct knowledge of the transition efforts told The Daily Beast. Team Trump didn't expect to win until the campaign's internal polling a month before the election signaled a possible victory.

Trump will soon be working with an FBI director he attacked
Washington Post, Sari Horwitz, Ellen Nakashima, 2016 11 10

Washington - **Donald Trump will enter the White House with an awkward relationship with the FBI director after attacking the bureau over its handling of the investigation into former secretary of state Hillary Clinton's private email server**. **James Comey**, who is in the third year of a 10-year term, is unlikely to go anywhere. Unlike the attorney general, the FBI director does not change with the administration. And officials close to Comey say he has no plans to leave, despite the political turmoil around the bureau since his surprise announcement last month on the Clinton investigation. Comey's handling of the Clinton matter drew withering criticism from current and former Justice Department officials, including former attorney general Eric H. Holder Jr. Nearly 100 former senior law enforcement officials from both parties censured Comey for sending his letter, which they said amounted to influencing the election in violation of long-standing Justice Department policy.

U.S spy agencies to begin top secret Trump briefings within days
Reuters, Mark Hosenball, 2016 11 10
Washington - U.S**. intelligence agencies will soon begin giving President-elect Donald Trump the same top secret national security briefings they give President Barack Obama, current and former intelligence officials said Wednesday**. The briefings by veteran career intelligence analysts, which will begin in the next few days, will include some of the government's most closely-guarded secrets, including details of undercover espionage operations and classified intelligence collection methods, including the National Security Agency's controversial eavesdropping operations, the officials said. The **Office of the Director of National Intelligence (ODNI), which will be in charge of Trump's briefings, had no immediate comment.**

CIA launches Signature School Program at UNM
Albuquerque Business First Online, 2016 11 11
Albuquerque --The **Central Intelligence Agency announced Thursday it will launch its Signature School Program at the University of New Mexico. CIA Director John Brennan spoke about the future intelligence and security challenges and previewed the new program** during a speech and visit to the UNM campus. "The CIA-UNM Signature School Program, the first of its kind in the nation, rests on two important factors: the rich academic programs at UNM across disciplines and fields of study, and the diversity of UNM students," said Emile Nakhleh, director of UNM's **Global and National Security Policy Institute**, in a news release. "It's win-win for our students and faculty because the program will strengthen the students' competitive edge in their search for careers in the federal government and in global and national companies and organizations." The program will deepen cooperation between the CIA and UNM and provide opportunities for students and faculty to engage CIA officers and learn about employment opportunities.

CIA announces student recruitment at UNM
Albuquerque Journal, Maggie Shephard, 2016 11 11
Albuquerque—The **CIA has taken a special interest in the University of New Mexico, announcing Thursday that the school is its first of five American colleges and universities that will be targeted for student recruitment into the intelligence agency. CIA Director John Brennan** made the announcement in person to about 300 people on campus before fielding questions from Emile Nakhleh, head of the school's new **Global and National Security Policy Institute**, and members of the audience. The other four schools have yet to be announced, making UNM the testing ground for the CIA's recruiting effort intended to "cultivate an applicant pool" that is as diverse as America is. "Improving diversity at CIA is not just a moral imperative, but a mission imperative ... to collect on a target anywhere around the world." Brennan told the crowd. Nakhleh said after the announcement that the school is not paying or

providing the CIA with an office or any funds, only working with it to allow the CIA to offer experiences and recruiting information to students to make them more hireable for federal security jobs.

Trump's torture support could mean the end of GCHQ-NSA relationship
The Register (UK), Alexander J. Martin, 2016 11 09
Column - If **comments made on the campaign trail by Donald Trump were sincere, then today's British government will need to do some serious soul-searching very soon**. Trump, who was today announced as the president- elect of the United States of America, has been controversially outspoken while seeking to be nominated as the Republican Party's presidential candidate, and while campaigning to be elected as President. The constitution may ostensibly be amended, and a UN convention might be derogated from, but a US decision to legalize torture would very probably prohibit the greater part of the intelligence-sharing aspects of the UK and US's special relationship - a relationship that already is substantively about the **collaboration between GCHQ and the NSA (US National Security Agency).**

Gen. Michael Hayden: Trump Won on Anger and May Act on Beliefs
Newsmax (US), Sandy Fitzgerald, 2016 11 09
Washington - **Donald Trump became the president-elect by "showing anger and being accusatory," and unless he has a meaningful conversation with the "fact-based" world's people, former CIA and National Security Agency Director Michael Hayden fears the worst**. "I fear he will act on the other set of beliefs, and that is going to be very bad for America and the world," Hayden, who was among a group of security experts opposing Trump's campaign, told CBS News anchor Charlie Rose on the "CBS This Morning" program early Wednesday. Trump won by "not being all that fact-based and scapegoating real and imagined enemies," said Hayden, and "none of that fits into the intelligence picture.

US official: Security controls 'working' despite NSA theft
Associated Press, Staff report, 2016 11 09
Washington - The **top U.S. counterintelligence official announced that secret government data is vulnerable to thieves, such as the National Security Agency insider accused of working undetected for more than 20 years to steal a large trove of classified material**, even as he defended the security controls put in place after the Edward Snowden theft. "I believe the reforms are working very well. I think we've done an amazing job in the intelligence community and across the government in executing our reforms," said Bill Evanina, the chief counterintelligence and security adviser to the national intelligence director. "However, I will say that if someone wakes up tomorrow and they make a decision that they're going to steal data from the government, they will be successful at it." Evanina told The Associated Press in a recent interview that no matter how good security controls are, they will never catch every insider or hacker -- and they must be continually improved because of technological advances. His extensive comments followed the August **arrest of former NSA contractor Harold Thomas Martin III, 51,** of Glen Burnie, Maryland. Martin remains in custody after a judge deemed him to be a flight risk.

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

UK opts in to new Europol intelligence-sharing programme
Financial Times, Helen Warrell, 2016 11 14
London - The **UK will opt in to a new intelligence-sharing programme with EU law enforcement agency Europol, in an effort to boost cross-border action against terrorism and cyber crime ahead of Brexit. Brandon Lewis, policing minister, said** on Monday that while it was still "too early to speculate" on whether security co-operation would continue after Britain leaves the EU, the government had decided to join the updated Europol framework in the short term. It is UK's first significant opt-in decision since the June referendum. Britain's collaboration in Europol was due to expire in May 2017 because the last government initially rejected the new programme, fearing it would reduce the operational independence of UK policing and increase the obligation to **share intelligence data**. Ministers have now secured concessions that do not extend the agency's powers over member states. Historically, Europol has been able to gather and disseminate intelligence, but its officers have no executive powers such as the right to make arrests. Following the terrorist attacks in Paris last year, some European interior ministers have called for more power for the agency. **Charles Michel, Belgium's prime minister, even suggested the EU should set up a "European CIA".** The new agreement falls far short of this, giving a "clear mandate" only to the EU's internet referrals unit, which tackles online terrorist propaganda, and allowing Europol to initiate investigations together with member states.

Britain's plan to tame Trump
London Times, Tim Shipman, 2016 11 13
London - A **secret memo from the British ambassador to the United States has laid bare how the UK plans to shape Donald Trump's presidency so he helps to boost Britain's national interests**. In a leaked telegram, written just as Trump was surging to victory last week, Sir Kim Darroch boasted that the UK is the best placed of any nation to steer the new president's foreign policy and encourage his more extreme ideas to "evolve". Darroch describes Trump as "open to outside influence" from Britain if Theresa May launches a diplomatic offensive to win him over. Whitehall sources say ministers, generals and intelligence chiefs are drawing up plans to influence Trump on such issues as Nato, Iran, Russia and immigration in an effort to help the UK exploit his victory and curb his more extreme views.

McCartney asks police to probe MI5 'bugging'
Sunday Times (UK), John Mooney, 2016 11 13
London - **Raymond McCartney a Sinn Fein MLA, has asked the Police Service of Northern Ireland to investigate the alleged bugging of his home in 2002 by the army and MI5**. McCartney, who lives in Derry, has been unable to locate an eavesdropping device which he believed was planted in his home. Its existence was exposed when an operations log book was accidentally left on the kitchen table by a "ghost team" comprised of army surveillance officers and an MI5 technician, who is said to have disarmed the alarm system on McCartney's house. The request by the former IRA hunger striker follows the publication of Charlie One, a book by a former army intelligence officer who used the pseudonym Sean Hartnett and revealed details about classified surveillance operations in Northern Ireland.

EX MI6 Boss: Nuclean War More Likely Under Trump
Daily Mail (UK), Dan Martin, 2016 11 12
London - **Donald Trump's unpredictable temperament has made nuclear war more likely, the former head of MI6 warned last night. John Sawers** said the president-elect's 'fierce' reactions when he feels he has been insulted could prove dangerous. The world has become far more perilous over the past few years, he said, with an increased threat of a nuclear clash between the US and China or Russia. Sir John told BBC Radio 4 that Barack Obama must take

some blame for the increased nuclear threat because his administration did not bolster relations with Russia. But he added: 'I don't think Donald Trump quite yet knows what the pressures will be on him when he becomes president.

Brazilians suspected as GCHQ investigates Tesco cyberattack
London Times, Multiple reporters, 2016 11 09
London - The **cyberattack on 40,000 Tesco Bank accounts "looks unprecedented", the chief City watchdog said yesterday, as it emerged that GCHQ is helping to investigate the crime**. Reports from victims pointed to Brazil as the origin of the biggest hack to strike a British bank, but the country's authorities have not yet been contacted by their British counterparts. Tesco said that it had been hit by "a systematic, sophisticated attack" with 20,000 customers having an estimated £17 million drained from their accounts. The bank has frozen all online transactions and many customers have had their debit cards blocked. Andrew Bailey, chief executive of the Financial Conduct Authority, told MPs that he was worried about weaknesses in banks' IT systems. He said: "The heart of the concern is what is the root cause of this and what does it tell us about broader threats." The **National Cyber Security Centre, a new part of GCHQ that tackles online crime, confirmed that it was providing "on-site assistance" to Tesco**. It is working alongside the National Crime Agency to investigate. Several customers said that fraudulent transactions were made in Rio de Janeiro.

No 10 source dismisses emergency MI5 meeting 'nonsense' as Jeremy Corbyn says Donald Trump win is 'unmistakable rejection of establishment'
London Daily Telegraph, Michael Wilkinson, 2016 11 09
London - **Theresa May has congratulated Donald Trump on being elected as the 45th president of the USA**, promising to remain "strong and close partners". In a statement she said: "I would like to congratulate Donald Trump on being elected the next President of the United States, following a hard-fought campaign. "Britain and the United States have an enduring and special relationship based on the values of freedom, democracy and enterprise. "We are, and will remain, strong and close partners on trade, security and defence. "I look forward to working with President-elect Donald Trump, building on these ties to ensure the security and prosperity of our nations in the years ahead." The **statement came as Number 10 sources described as "nonsense" claims that the head of MI5 has gone in for an emergency meeting,** insisting it was a long-scheduled meeting and that he always uses the back door.

Return to Table of Contents/ Retour à la table des matières

Australia / Australie

Govt appoints new cyber affairs ambassador
Australian Associated Press, Staff reporter, 2016 11 10
Canberra - **Australia has appointed its first-ever ambassador for cyber affairs. Dr Tobias Feakin** will fill the inaugural position from January as part of the federal government's $230 million cyber security strategy. The academic, who has been the director of national security programs at the Australian Strategic Policy Institute since 2012, will work with other countries to strengthen the region's response to cybercrime and advocate against state censorship of the internet. (Full report)

Don't believe anything you hear, Canberra was no nest of spies
The Australian Financial Review, Brian Toohey, 2016 11 09
Column: John **Blaxland's enthusiastic sales pitch for his new book suggests Canberra residents must have found it hard not to trip over Russian spies doing battle with Australian spy catchers in the 1970s and '80s.** Blaxland, co-author of the latest volume of the **official history of the Australian Security Intelligence Organisation** told The Canberra Times last week, "It was on for young and old" in shops, restaurants, cafes and bars in Manuka, Kingston, Deakin, Yarralumla, Red Hill and parks near the Soviet and Chinese embassies. Blaxland said Russian spies were waiting for "a pre- arranged contact to turn up to drop something off or have a 'brush-past' [jargon for quick handover]". But not everyone is convinced it occurred, not least because it is not in the official history itself, The Secret Cold War. When asked to confirm that the Russian spies met their Australian contacts in shops, cafes etc in each of the locations Blaxland named, a **spokesman for ASIO referred this column to the official history - a book it knows doesn't confirm these details**. On the contrary, it says ASIO hadn't managed to detect a KGB officer meeting an agent. This might explain the gently sceptical comment from a former senior defence official, Patrick Gourley, who told this column, "Millers of Manuka was a hotbed for the spy trade.

Return to Table of Contents/ Retour à la table des matières

New Zealand / Nouvelle-Zélande

The spy agencies watchdog is calling for the proposed warrants regime in new spy legislation to be tightened.
Radio New Zealand News, Staff reporter, 2016 11 10
Wellington - The **spy agencies watchdog is calling for the proposed warrants regime in new spy legislation to be tightened. MPs are considering a new law for the GCSB and the SIS setting up a common warranting and compliance regime**. The Inspector-General of Intelligence and Security, Cheryl Gwyn, says some of the new provisions are too broad, lack safeguards, or weaken conditions in the current law. She told a select committee this morning she supports more ministerial policy statements on what agencies can do without warrants. (Full report)

Return to Table of Contents/ Retour à la table des matières

International

China / Chine

Cybersecurity bill to rank agencies by data sensitivity
Taipei Times, Lee Hsin-fang, 2016 11 13
Beijing - A **new draft cybersecurity bill that aims to protect sensitive government information is to rank government agencies on a three- tier system according to the data they handle**, sources said. A total of 123 key government institutions, including the Presidential Office, **the National Security Council**, the Executive Yuan, the Ministry of National Defense and the National Security Bureau, have been identified by the Executive Yuan as tier-A organizations in terms of information security interests, a source who declined to be named said. The institutions would be required to conform to semiannual inspections, as well as

conduct cyberattack response drills at least once a year. While relations between China and Taiwan seemingly thawed during former president Ma Ying-jeous tenure, former premier Simon Chang had previously acknowledged that attacks on Taiwans computer systems by Chinese hackers were still frequent at that time.

More talks needed with Japan on military intelligence pact: S. Korea
Kyodo News, Staff reporter, 2016 11 10
Seoul - **South Korea and Japan will hold further discussions before reaching a final agreement on signing a pact to share military intelligence**, South Korea's Defense Ministry spokesman said Thursday. "We are not in the (stage) for final agreement yet. Additional discussions are being arranged," the spokesman told a regular press conference, a day after officials from the two sides held a second round of talks in Seoul with an eye on concluding the General Security of Military Information Agreement by the end of the year. Meanwhile, South Korea's opposition camp, which holds majority in the National Assembly, is demanding the suspension of the talks and submitted a resolution to the parliament on Wednesday to that end.

Chinese official named head of Interpol, drawing criticism
Associated Press, Christopher Bodeen, 2016 11 10
Beijing - A **top Chinese police official was elected president of Interpol on Thursday, setting off alarm bells among rights advocates over abuses and a lack of transparency within China's legal system,** as well as the potential misuse of the police organization to attack Beijing's political opponents. **Vice Public Security Minister Meng Hongwei was named as the first Chinese to hold the post** at the organization's general assembly on the Indonesian island of Bali, Interpol announced in a press release. The Lyon, France-based International Criminal Police Organization has 190 member nations and has the power to issue "red notices." It's the closest instrument to an international arrest warrant in use today. Interpol circulates those notices to member countries listing people who are wanted for extradition.

China says "no grace period" for foreign NGOs under tough new law
Reuters, Staff reporter, 2016 11 09
Beijing - **There will be no "grace period" for the implementation of new regulations limiting the activities of foreign non-governmental organisations (NGOs) in China that are slated to come into effect in 2017, according to the Ministry of Public Security**. Western governments have lambasted the foreign NGO law passed in April, saying it treats the groups as a criminal threat and would effectively force many out of the country. "China is a country with the rule of law - no law has a 'transition period' or 'grace period' after it takes effect," a representative from the Ministry of Public Security's Foreign NGO Management Bureau told consular officials from 11 countries at a briefing in Shanghai on Tuesday.

Return to Table of Contents/ Retour à la table des matières

Russia / Russie

Former SVR chief Fradkov heads up Almaz-Antey board of directors
Interfax News Service, 2016 11 14
Moscow—**Mikhail Fradkov, former head of the Russian Foreign Intelligence Service (SVR)**, has headed up the board of directors of Concern VKO Almaz-Antey, the concern said on its website.It was reported on November 9 that Fradkov had been nominated by Prime Minister Dmitry Medvedev for the post of board member of Concern VKO Almaz-Antey. Until recently,

the board of Concern VKO Almaz-Antey was headed by Sergey Chemezov, the head of the state corporation Rostec.

How Two Russian Defectors Helped the FBI Nab European Mobsters Then Wound up Stranded in Oregon
Newsweek, Bryan Denson, 2016 11 12
Analysis: As an **intelligence officer in Russia's Federal Security Service, Jan Neumann** knew the weight of a loaded Makarov 9 mm. When he later worked for a Moscow bank that laundered money for the mob, he also knew the weight of $1 million packed into bricks. But on a spring night in 2008, as he headed home to his wife, he could scarcely comprehend the weight of his impending troubles.,,Jan also downloaded an electronic file on several government-affiliated banks, a rare glimpse inside the criminal Cerberus of financial big shots, mobsters and **FSB officers**. The Neumanns drove half the night to see a friend, then switched cars and headed back to Moscow. Victorya booked three flights set to depart from airports around the city--decoys to confuse pursuers. In the final hours before their departure, Victorya purchased tickets for the flight they intended to board, bound for Frankfurt, with a connecting flight to the Dominican Republic, a Caribbean nation that requires no visas.

Russian State Duma ratifies China-Russia anti-terrorism agreement
Xinhua News Agency, 2016 11 12
Moscow - The **Russian State Duma, or the lower house of parliament, ratified an agreement on Friday between China and Russia on cooperation in fighting against terrorism, separatism and extremism**. Russian President Vladimir Putin submitted the agreement to the State Duma for parliamentary ratification on Sept. 28. The agreement, signed in Beijing on Sept. 27, 2010, is aimed at developing bilateral cooperation in combating terrorism, separatism and extremism by taking joint measures to prevent and stop terrorist attacks. The two countries will exchange information in fighting criminal activities of terrorists and extremists, hold regular meetings and consultations, and work together to prevent and suppress crimes in the border regions between China and Russia.

Return to Table of Contents/ Retour à la table des matières

Europe

Germany does not have to hand over NSA list of spying targets
DPA News Agency, 2016 11 15
Berlin—A **list of spying targets given to German intelligence by the United States does not have to be made available to a parliamentary committee investigating the affair**, the country's Constitutional Court ruled Tuesday. The list of so-called "selectors" - telephone numbers, email and IP addresses - was handed to **Germany's foreign intelligence agency BND by the National Security Agency (NSA)** with the aim of spying on German and other European targets. Making the sensitive information public could threaten national security and the work of Germany's intelligence agencies, the court in Karlsruhe said in a decision issued last month but made public on Tuesday.
Quand Israël tentait d'espionner la sécurité intérieure
Le Monde, Jacques Follorou, 2016 11 15
Paris - En **2011-2012, le Mossad a essayé de faire acheter au renseignement intérieur et à la direction de la police des moyens techniques piégés** Les affaires d'espionnage entre les Etats ne se règlent quasi jamais au grand jour. L'évocation dans une procédure judiciaire visant Bernard Squarcini, ex-patron de la sécurité intérieure, d'une tentative d'espionnage de la

Direction générale de la police nationale (DGPN) et de la **Direction centrale du renseignement intérieur (DCRI) par le Mossad**, les services secrets israéliens, est une première. Soupçonné de plusieurs faits, dont certains relevant du trafic d'influence, l'ancien chef de la DCRI, de 2008 à 2012, a en effet révélé, fin septembre, l'existence d'une opération du Mossad contre des intérêts français, après avoir été sommé de s'expliquer sur le placement sur écoute d'un policier en 2011. Suspecté d'avoir pu détourner les moyens de la DCRI pour régler des comptes personnels, M. Squarcini s'est défendu en dévoilant l'enquête de contre-espionnage ciblant les services secrets israéliens dans laquelle ce fonctionnaire a été écouté.

Court rejects case to reveal more on US spies in Germany
The Local (Germany), Staff report, 2016 11 15
Berlin - A **case brought by opposition parties to shed light on the spying collaboration between Germany and the American NSA was rejected by Germany's highest court in a decision made public on Tuesday**. Die Linke (Left Party) and the Green party politicians from a parliamentary committee currently investigating German-American spying activities had launched the case in an effort to have **intelligence agency BND release a so-called "selectors list" of targets provided by the US National Security Agency (NSA) to Germany**. The list contains identifiers such as IP addresses, phone numbers and email addresses used to search for specific people. The committee members had wanted to view the list, but the German government refused, instead appointing a "trusted person" to evaluate the list and then inform the committee. The **Constitutional Court** ruled on Tuesday that the BND could keep the list classified, arguing that the government's interest in confidentiality was more important than the interests of the parliamentary committee to receive more information. The court further explained that publishing the list of selectors without the consent of the US could affect the **functioning of intelligence agencies and therefore Germany's security capacity**.

Enquête Squarcini, ex-chef de la DCRI, aurait mis ses réseaux au service de LVMH
L'Humanité, P. Du., 2016 11 15
Paris - On en sait un peu plus sur les **activités troubles de Bernard Squarcini, chef du renseignement intérieur (DCRI)** jusqu'en mai 2012. Mis en examen le 4 novembre pour « violation du secret de l'enquête », « trafic d'influence » et « compromission du secret-défense », ce proche de **Nicolas Sarkozy** est soupçonné d'avoir utilisé ses contacts au sein de la justice et de la police pour servir des intérêts privés, au sein de l'officine Kyros. De nouvelles informations, publiées hier par Mediapart, **montrent comment il a contribué à l'espionnage, pour le compte de LVMH, des héritiers de la famille Hermès** après avoir sollicité un magistrat encore en poste dans le but d'obtenir des informations sur une procédure opposant les deux groupes du luxe. Bernard Squarcini aurait aussi fait appel à un agent de la DGSI pour glaner des informations sur un opposant kazakh.

EU Struggles With Security Gaps
Wall Street Journal, Matthew Dalton, 2016 11 14
Paris - Shortly after the terror attacks here a year ago, **European leaders pledged to close a legal loophole that militants could exploit to pass through border crossings without security checks**. A year later, negotiators in Brussels are still quarreling over how to change the problematic law, which forbids border guards from conducting systematic security checks on European citizens. France and some other governments, fearing the return of European-born jihadists from Syria, have grown increasingly exasperated. "We have been quite irritated at the pace," said one European diplomat involved in the talks. Faced with repeated attacks by Islamic State and its sympathizers, the European Union is struggling to find decisive fixes for its myriad security vulnerabilities. Efforts have been hamstrung by the bloc's complex decision-making

procedures, **privacy concerns and a cumbersome counterterrorism apparatus** that relies on coordination among theregion's 28 governments.

Attack on Dutch elections possible warns counter-terror boss
NL Times, Taylor Moore, 2016 11 14
The Hague - **With European citizens becoming more polarized when it comes to integration, Islam and asylum, the Netherlands must prepare for a possible attack during the parliamentary elections in March, cautions Dick Schoof, the National Coordinator for Counterterrorism and Security.** Radicalized loners, both ultra nationalists and religious fanatics, could be particularly dangerous, he told radio station BNR. He added that the ISIS propaganda machine is relentlessly targeting "vulnerable, impressionable people who are not on the radar screens of security authorities." These online messages are calling on disillusioned people to carry out attacks on behalf of the militant group. But the primary danger is from the alleged jihadists who return to the Netherlands from Iraq and Syria. It is one reason why the Dutch threat level is at its second-highest level. There are European arrest warrants out for about 190 Dutch people who fought in the Syrian Civil War, and whose whereabouts are not known.

Renseignements 3.000 à 5.000 potentiels « returnees »
Le Soir, Journaliste maison, 2016 11 14
Bruxelles - Les **services de renseignement européens travaillent sur l'hypothèse d'une « vague » de milliers de combattants de Daech qui pourraient rentrer en Europe**, a indiqué dimanche le ministre de l'Intérieur. « On voit que l'État islamique est sous pression avec les attaques à Raqqa et Mossoul. Soit les combattants belges restent là-bas pour aider à la défense de l'État islamique. L'autre hypothèse, c'est que l'État Islamique renvoie ces combattants. Et pas seulement les 200 Belges sur place, mais les 3.000 à 5.000 Européens qui s'y trouvent » , a affirmé M. Jambon (N-VA) sur la RTBF.

Renseignement, prison, police... Ce qui a été fait depuis ces attaques
Le Figaro, Paule Gonzalès et Christophe Cornevin, 2016 11 12
Paris - Le **gouvernement s'y est repris à plusieurs fois avant de proposer, avec l'aide du Sénat, un dispositif légal renforcé. La loi du 13 novembre 2014 a introduit l'interdiction de sortie du territoire et créé le délit de préparation individuelle d'une entreprise terroriste**. La répression des faits d'apologie et de provocation au terrorisme a été durcie et de nouveaux outils administratifs permettent de bloquer ou de déréférencer des sites Internet. La loi du 3 juin 2016 entérine le renforcement de la lutte contre le trafic d'armes, la lutte contre le blanchiment d'argent, le renforcement du renseignement pénitentiaire et des pouvoirs d'enquête pour les magistrats, ainsi que l'usage des armes facilité pour les forces de l'ordre. Les enquêteurs pourront aussi utiliser les Imsi-catchers, permettant le recueil des données sur de larges zones d'écoutes.. Dans le cadre du **renforcement des services de renseignement, 500 agents supplémentaires sont appelés à étoffer la Direction générale de la sécurité intérieure (DGSI) d'ici à fin 2017,** en plus des 432 déjà prévus. « Des analystes techniques, des informaticiens, des linguistes sont notamment recrutés pour renforcer ses capacités d'analyse, de détection et de prévention des risques terroristes » , a annoncé Bernard Cazeneuve, qui a par ailleurs alloué 500 postes de plus - 350 policiers et 150 gendarmes - au **Service central du renseignement territorial (SCRT)**, tandis que 100 recrues vont rejoindre la Direction du renseignement de la Préfecture de police.

Poland honours CIA spy with posthumous award
Agence France-Presse, 2016 11 11

Warsaw— **Poland gave a posthumous honour Friday to a former Polish army colonel who for years gave the CIA precious information on the Warsaw Pact**, the Soviet military alliance. **Colonel Ryszard Kuklinski**, who died in Florida in 2004 and is buried in Warsaw, was declared by President Andrzej Duda to be a "knight of our independence," and promoted to the rank of general. Kuklinski, a brilliant officer in the Soviet-era Polish army, decided to change sides after the Communist regime brutally crushed a workers' revolt in 1971 and he learned of Kremlin plans for military aggression. Between 1972 and 1981, he handed some 35,000 secret documents to the US Central Intelligence Agency (CIA).

Aleksandre Tabatadze appointed as Deputy Head of State Security Service
Prime News, 2016 11 11
Tbilisi— **Aleksandre Tabatadze has been appointed as Deputy Head of the State Security Service of Georgia. Vakhtang Gomelauri is the head of the service**. As Prime-News has been informed from the State Security Service the PM has already signed the corresponding decree. Aleksandre Tabatadze worked as the Deputy Minister of Justice. Earlier he was the Deputy Interior Minister of Georgia.

Cabinet Endorses Order Of Application Of Funds By Foreign Intelligence Service
Ukrainian News, 2016 11 11
Kiev— The **Cabinet of Ministers has endorsed the order of application of state budget funds assigned for the Foreign Intelligence Service** to implement measures to enhance the nation's defensive capacity and security. Ukrainian News Agency learned this from Government Resolution 798 of November 9. The Foreign Intelligence Service is the chief controller of the budget funds and the executive manager of the budgetary program. This order regulates budget spending on the purchase and upgrades of weapons and military hardware, technical reconnaissance equipment, information protection equipment and for the development of information systems.

La DGSE s'inquiète d'une enquête sur l'accident d'avion à Malte
Le Monde, Jacques Follorou, 2016 11 10
Paris - Une **information judiciaire pourrait dévoiler des activités clandestines**. Le parquet de Paris a ouvert, dans la plus grande discrétion, une procédure après l'accident ayant coûté, le 24octobre, à Malte, la vie à cinq Français dans la chute d'un avion loué par la **Direction générale de la sécurité extérieure (DGSE).** Mise en oeuvre quand des nationaux perdent la vie dans des conditions inexpliquées, elle est jointe à celle ouverte, sur place, par les autorités maltaises. Elle est conduite en parallèle des investigations du Bureau enquêtes et accident rattaché au ministère de la défense (BEA-D). **La DGSE a, par ailleurs, diligenté, avec ses propres moyens, des recherches, par principe**, sur une éventuelle implication étrangère parmi les causes de l'accident.

Les espionnes sortent de l'ombre
L'Obs., Vincent Jauvert, 2016 11 10
Non identifié - **Espionnes, doubles vies sous haute tension, par Dalila Kerkouche**, Flammarion, 300 p., 21 euros. Il ne faut pas se fier au titre de cet ouvrage beaucoup plus important qu'il n'y paraît. Certes, il y est question de la vie difficile des femmes qui occupent des postes élevés dans les sept services de renseignement français, dont la **mythique DGSE** : le machisme insupportable, la séparation d'avec la famille et les amis, la lourdeur d'une tâche devenue hautement stratégique en ces temps de terrorisme Mais le livre de Dalila Kerchouche (photo), grand reporter à « Madame Figaro », est avant tout un document exceptionnel sur l'espionnage français. Jamais autant d'officiers en activité, des dizaines, n'avaient témoigné

(anonymement) sur leurs façons de travailler, de recruter et de manipuler les sources, remonter des filières, les démanteler.

Quand Hollande se renseigne sur le Renseignement
Le Point, A.Z., 2016 11 10
Levallois-Perret, France - **Le 2 novembre, François Hollande s'est rendu discrètement, en fin d'après-midi, à Levallois-Perret, au siège de la Direction générale de la sécurité intérieure (DGSI)**. Une visite non mentionnée sur l'agenda présidentiel. **Patrick Calvar , le patron du renseignement intérieur, a rendu compte au chef de l'Etat des opérations secrètes en cours** - avec le président, on n'est jamais sûr qu'elles le restent longtemps... Calvar lui a également exposé les défauts du système de lutte antiterroriste à l'échelon de l'Union européenne. Dans le but de lutter contre le terrorisme, l'accord Swift 2 donne en effet aux autorités américaines l'accès aux données bancaires stockées sur le réseau Swift, qui gère les transactions financières internationales de près de 200 pays... mais pas à la France.

Germany tries civil servant accused of spying for Indian intelligence
DPA News Agency, 2016 11 10
Berlin— A 59**-year-old former civil servant was set to go to trial in Germany Thursday on charges of espionage on behalf of India's foreign intelligence agency**. The German national is suspected of "occupation as a secret service agent and disclosure of official secrets in 45 cases," according to the federal prosecutor's office in Karlsruhe. The man is accused of spying on Indian nationals in Germany - mainly political dissidents and Sikh extremists - while working at a foreigners' registration office in the western state of North Rhine-Westphalia.

German cabinet approves cyber security strategy
Deutsche Welle, 2016 11 09
Berlin— **Germany's cabinet has approved a new cyber security strategy** amid a growing number of attacks. Many of the cyber attacks are directed from China and Russia. The German cabinet on Wednesday adopted a new cyber security strategy to counter a rising number of threats targeting government institutions, critical infrastructure, businesses and citizens. The strategy calls for the creation of a mobile **Quick Reaction Force housed within the Federal Office for Information Security (BSI**), as well as similar teams within the federal police and domestic intelligence agency that are able to respond to cyber threats against government institutions and critical infrastructure. **Germany's Cyber Defense Center** will fall under the authority of the Interior Ministry, which will seek to foster inter-agency coordination and cooperation.

Gülenists sabotaged reconciliation process with the PKK, former Turkish intelligence official says
Daily Sabah, Staff report, 2016 11 09
Istanbul - **Former National Intelligence Organization (MIT) official Emre Taner said Wednesday that the government's 2009 talks with the PKK terrorist organization had aimed for reconciliation and put a halt to 40 years of bloodshed**, but the whole peace process was sabotaged by foreign powers and the Gülenist terror cult (FETÖ). In a meeting with the Turkish Parliament's commission investigating the July 15 Gülenist coup attempt, he said that the talks with the terrorist group was not "treason" but only an effort to stop PKK terrorists. "We started the Oslo talks to prevent foreign powers from using the PKK as a tool. Many of them are in affiliation with the terrorist group," he said.

Quand Ceausescu espionnait les Français
L'Express, Charles Haqyet et Iulia Badea-Gueritée, 2016 11 09

Paris - **Pendant plus de quarante ans, les agents roumains en poste dans l'Hexagone ont surveillé des hommes politiques**.Et les ont parfois recrutés.Plongée dans des archives tout juste déclassifiées de la Securitate. « Stanica » : cet alias a caché, durant quatre ans, un membre du premier cercle de François Mitterrand. Son nom? **Claude Estier. Ancien résistant, député, président de la commission des Affaires étrangères, ce politicien habile a joué un rôle clef dans l'appareil socialiste jusqu'au début des années 2000.** Mais il avait un autre visage. De 1982 à 1986, Claude Estier a entretenu des relations suivies avec la Securitate, la police secrète de Nicolae Ceausescu, comme le révèlent des documents inédits (voir page 66), récemment déclassifiés, que L'Express a pu consulter. Depuis la chute du communisme, à la fin des années 1980, des centaines de chercheurs ont décortiqué les archives de ce service d'espionnage naguère omni - présent. Durant plus de quarante ans, la Securitate a tout vu, tout entendu, en Roumanie et parfois au-delà. **Ses espions ont écrit des millions de rapports, dont une grande partie dort aujourd'hui sur des étagères**, témoins poussiéreux d'une époque de terreur et de chantage.

Terrorisme: Interpol dénonce le manque de partages de données biométriques entre Etats
Agence France-Presse, Journaliste maison, 2016 11 09
Lyon - Le **secrétaire général d'Interpol Jürgen Stock a dénoncé mercredi l'insuffisant partage entre Etats de données biométriques susceptibles de permettre d'identifier plus efficacement les terroristes.** L'organisation de coopération policière estime qu'"environ 15.000 combattants se trouvent dans les zones de conflit et qu'un nombre indéterminé d'entre eux pourrait rentrer dans leur pays d'origine pour (...) s'engager dans des opérations clandestines". L'assemblée générale d'Interpol, qui était réunie à Bali (Indonésie), a souligné "l'urgence à traiter cette menace", écrit-elle dans un communiqué. "Bien que le partage d'information via Interpol ait permis aux organisations nationales de maintien de l'ordre d'empêcher des terroristes et des candidats terroristes de voyager, le manque de données biométriques reste un maillon faible", déclare M. Stock, cité dans un communiqué de l'organisation.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Intelligence Minister: Iran Most Secure Country in Middle East Despite Massive Terrorist Attempts
Fars News Agency, 2016 11 09
Tehran - **Iranian Intelligence Minister Seyed Mahmoud Alavi underlined that despite all attempts made by various terrorist groups, Iran is the most secure country in the region due to its powerful defensive and military forces**. "The security index in Iran shows improvement on a daily basis," Alavi said. He reiterated that security in most of the countries is deteriorating, but it is improving day by day in Iran. The Iranian intelligence minister said that Iran owes its stable security conditions to the efforts made by the country's intelligence forces who nip any plot in the bud and carefully watch any suspicious move right from the beginning.

Iran's security index rising on daily basis: Intelligence minister
Press TV, 2016 11 09
Tehran - **Iran's Intelligence Minister Mahmoud Alavi says the country's security index is increasing on a daily basis**, while most parts of the world are witnessing a downward trend in

the same field. “The level of security governing our country is, as in the words of Leader of the Islamic Revolution [Ayatollah Seyyed Ali Khamenei], unparalleled,” Alavi said on Monday. “The increase in our country’s security index comes as we are witnessing the deaths of people in countries here and there, which shows how the security index is low in most countries of the world,” the Iranian intelligence minister said..

Return to Table of Contents/ Retour à la table des matières

Asia / Asie

Failure of deradicalization blamed on poor coordination
Jakarta Post, Haeril Halim and Nurul Fitri Ramadhani, 2016 11 15
Jakarta - The **effectiveness of the country's deradicalization program has been put under scrutiny** in the wake of the attack at a church in Samarinda, East Kalimantan, on Sunday, the chief suspect in which is a former terrorism convict. The **National Counterterrorism Agency (BNPT) has blamed poor coordination among related institutions for the failure to monitor terrorism convicts in society** after they have finished their prison sentences. The BNPT has become the subject of criticism since it became known that Johanda, the suspected perpetrator of the Samarinda attack, which claimed the life of a toddler and left three others injured, had returned to join radical groups after he was released on parole in July 2014.

India, Israel to intensify defence, anti-terror cooperation
Press Trust of India, 2016 11 15
New Delhi - Reflecting their growing proximity, **India and Israel on Tuesday decided to further "broad-base" their already close defence partnership and intensify cooperation in combating radicalisation and extremism, while calling upon global community to act tough against terror networks and States harbouring them**. The two countries also agreed to deepen their cooperation in a variety of areas including trade and investment, agriculture, water resources and cyber crime during extensive talks between Prime Minister Narendra Modi and Israeli President Reuven Rivlin, who is on his first visit to India.

S. Korea to put intel-sharing pact with Japan up for Cabinet approval
Yonhap News Agency, Staff reporter, 2016 11 15
Seoul - **South Korea will put the military intelligence-sharing pact it reached with Japan up for final Cabinet approval this week**, the foreign ministry said Tuesday, as Seoul is moving to finalize the controversial deal despite local objections. South Korea and Japan tentatively signed the **General Security of Military Information Agreement (GSOMIA)** on Monday, which would allow the South to share its sensitive military intelligence on North Korea with Japan. The Ministry of Government Legislation has checked the deal and "upon the completion of screening, the deal may get introduced to the next vice ministerial meeting on Thursday," ministry spokesman Cho June-hyuck said in a press briefing. Approval at the vice ministerial session will allow it to be forwarded to a Cabinet meeting, the spokesman said. The next Cabinet meeting after Thursday is set for Nov. 22.

Japan, South Korea agree to sign military intelligence pact
Kyodo News, Staff reporter, 2016 11 14
Tokyo - **Japan and South Korea agreed Monday to sign a pact to share military intelligence, Japan's Foreign Ministry said**, as the two neighbors seek to strengthen security ties in the face of a growing threat from North Korea. The two governments aim to sign the

General Security of Military Information Agreement as soon as this month after completing domestic procedures, Japanese government sources said. Earlier Monday, South Korea's main opposition parties threatened to dismiss the country's defense minister if the government signs the intelligence sharing agreement. The agreement to sign the pact was reached following the third round of working- level talks between foreign and defense ministry officials in Tokyo on Monday. The two countries resumed the talks on Nov. 1 after a lapse of four years.

Pakistan won't be able to copy new notes: Intelligence agencies
Times of India, Neeraj Chauhan, 2016 11 10
New Delhi - **Intelligence agencies vetted the new denominations of Rs 2,000 and Rs 500 notes asserting that its security features will be next to impossible to replicate** for Pakistan and organised criminal networks for some time to come. A top government official without going into the details, told TOI that external intelligence agency Research and Analysis Wing, Intelligence Bureau and the DRI examined the features on the notes being secretly printed for the past six months. The official refused to reveal the number of security features on the notes but said they were difficult to forge.

Two more Indian 'undercover operatives' leave Pakistan
Pakistan Dawn, Syed Sammer Abbas, 2016 11 10
Islamabad - **Two more Indian 'undercover operatives' among eight 'diplomats' suspected of involvement in terrorism and subversive activities in Pakistan left the country on Thursday**, Foreign Office officials confirmed. Indian High Commission First Secretary Press Balbir Singh and Staff Officer Jayabalan Senthil, allegedly members of the **Indian Intelligence Bureau**, left Pakistan for Dubai via flight EK 615, the FO officials said. Three Indian High Commission officials left Pakistan earlier this week. Anurag Singh, Vijay Kumar Verma and Madhavan Nanda Kumar, were suspected of being member of **Indian spy agency Research and Analysis Wing (RAW).** The FO during a press briefing last week revealed details of the eight Indian 'diplomats' in Pakistan, saying that a number of "Indian diplomats and staff belonging to Indian intelligence agencies RAW and IB have been found involved in coordinating terrorist and subversive activities in Pakistan under the garb of diplomatic assignments."

Three of eight Indian diplomats accused of spying leave Pakistan
Gulf News, Mohsin Ali, 2016 11 09
Islamabad - **Pakistani officials say three of eight Indian diplomats accused by Islamabad of spying have left the country for New Delhi**. A security official and a government official insisted the three were part of an alleged network of spies. The two officials said the three Indians left Pakistan on Tuesday and another five "undercover agents" will also leave Islamabad soon. The officials spoke on condition of anonymity because they were not authorised to talk to the media. Pakistan has withdrawn six diplomats from its embassy in New Delhi after their names were released to Indian media. **Islamabad reciprocated by revealing names of eight Indian diplomats, claiming they were spies.**

Return to Table of Contents/ Retour à la table des matières

Africa / Afrique

FG Reads Riot Act to Defence, Intelligence Agencies on National Security
This Day (Nigeria), 2016 11 15

Abuja—The **federal government has charged the defence, security and intelligence agencies to either come up with novel, actionable and effective strategies on sustainable solution to the burgeoning security challenges in the country or be sanctioned**. The Minister of Defence, Brig-Gen. Muhammad Mansur Dan-Ali (rtd), gave the riot act yesterday while declaring open the 2016 Defence Advisers/Attaches (DAs) Annual Conference tagged: Harnessing the Potentials of Defence Attache System for improved **National Security in Nigeria", at the Defence Intelligence Agency (DIA)** Headquarters, Abuja. To this end, Dan-Ali warned the DAs and concerned authorities that the federal government would no longer tolerate any form of shoddiness and lack of creativity in handling of national security matters. He called for innovation, noting that given the complexity and uncertainty of today's security environment, our defence architecture and thought process would have to significantly to provide sustainable military and political outcomes.

Terrorisme: ouverture à Grand-Bassam de la 8è réunion des chefs des services de renseignement
Agence de Presse Africaine, Journaliste maison, 2016 11 14
Grand-Bassam, Côte d'Ivoire - La **huitième réunion des chefs des services de renseignement des pays Sahélo-sahariens s'est ouverte, lundi, à Grand-Bassam**, ville balnéaire ivoirienne située àquelque 20 km au Sud d'Abidjan et ayant subi une attaque terroriste en mars dernier, a constaté APA sur place. L'ouverture s'est déroulée en présence du ministre ivoirien de l'intégration africaine et des Ivoiriens de l'extérieur Ally Coulibaly et de l'ancien président du Burundi, Pierre Buyoya, chef de la Mission africaine pour le Mali et le Sahel (Misahel). Cette rencontre, la huitième du genre, s'inscrit dans le cadre du processus de Nouakchott mis en marche en mars 2013. Selon le Commissaire Paix et sécurité de l'Union Africaine, Chergui Smaïl, elle permettra de passer en revue la situation sécuritaire de la région, à faire l'état de la mise en oeuvre du processus de Nouakchott et à faire un point des activités de l'Unité et de liaison de l'UA.

South African spy chief linked to rhino horn trade
London Times, Stuart Graham, 2016 11 14
Johannesburg - **South Africa's intelligence minister has been linked to the illegal trade in rhinoceros horn after being photographed at a massage parlour with a Chinese crime boss who claims to be a smuggler**. The allegations are contained in a documentary, broadcast yesterday, that was filmed by the television station Al Jazeera over six months. Footage secretly recorded by an undercover investigator shows a man identified as Mr Guang, the massage parlour owner, swiping through photographs on his phone that appear to show him and the minister, **David Mahlobo**. "He came to my massage parlour every week, or at least twice a month," Mr Guang says in the documentary. "I know him well." One of the photographs appears to show Mr Mahlobo with a young woman, whom Mr Guang refers to as "one of my manicure girls". The State Security Agency, headed by Mr Mahlobo, is mandated to provide the government with intelligence on security threats, including organised crime.

Interviews heat up for top intelligence post
Cape Times, 2016 11 10
Capetown, SA—**Interviews for the new inspector-general of intelligence continued yesterday** as members of the joint standing committee grilled one candidate, to such an extent he was almost brought to tears. **Andile Kilifele** said he studied at UCT and Wits, where he obtained his LLB before he started working, but the ANC's Dumisani Gamede wanted him to account for a gap in his CV between November 2003 and April 2004, and his frequent "job-hopping". "The longest you have served was in your last job, where you worked from 2008 to 2014, but with the rest it was hardly a year?" asked Gamede. Kilifele quit his job as a **divisional**

head within the National Intelligence Agency to seek pupillage with a law firm and return to legal practice, but was now a stay-at-home dad after his application was rejected.

Spooks 'without guidance'
The Times, 2016 11 09
Cape Town—For the past 20 months, **the office of the inspector-general (IG) of intelligence has been unable to conduct any oversight**. Interviews to fill the senior **State Security Agency** position yesterday painted a bleak picture of an organisation hamstrung by a lack of leadership. Three of the five candidates interviewed are employees in the IG office and also sit on the executive committee. The interviews further revealed that, while the agency was limping along administratively, it faced court actions and had been barred from conducting any oversight work of certain services. It is also unable to fill any vacant posts. The IG position has been vacant for 20 months after opposition parties blocked the appointment of ANC favourite Cecil Burgess. The successful candidate needs to be confirmed by a two-thirds majority of parliamentarians.

Mauritanie : Nouakchott appelé à relancer la coopération sécuritaire
El Moudjahid, Journaliste maison, 2016 11 09
Nouakchott, Mauritanie - **Les experts sécuritaires des pays du G5 du Sahel ont appelé, mardi soir à Nouakchott, à la relance du système de coopération dans le domaine sécuritaire entre les pays de cette région** et à l'élaboration d'une stratégie globale qui prenne en compte les défis transfrontaliers. Les experts des pays du G5 du Sahel (Mauritanie, Mali, Niger, Burkina Faso et Tchad) ont indiqué, lors d'une réunion tenue mardi au Tchad, que les défis sécuritaires auxquels la région est confrontée «impliquent la relance du système de coopération sécuritaire entre les pays du Sahel», soulignant les répercussions dangereuses de l'insécurité dans cette région sur le plan international. Un système de coopération sécuritaire a été développé par le G5 depuis sa création à Nouakchott en mai 2014, lors de la première réunion des ministres de l'Intérieur de ces pays, avec l'aide technique de **l'Office des Nations unies contre la drogue et le crime (ONUDC)**, a précisé un expert auprès du secrétariat permanent du G5 du Sahel, précisant que ce système avait été ratifié par le sommet du G5 en novembre 2015 à N'djamena au Tchad.

Return to Table of Contents/ Retour à la table des matières

Americas / Amériques

Anaya counters critics, publishes own 3 of 3
Mexico News Daily, 2016 11 08
Mexico City— In response to the accusations for leading what some have described as a "luxury lifestyle," the leader of the National Action Party (PAN), Ricardo Anaya Cortés, has published on his personal website his own "3 of 3" report, detailing his income, expenses and savings. The party boss said if there were any irregularities in his financial situation he would not be able to denounce "so strongly and bluntly the corruption of the Institutional Revolutionary Party [PRI]." "**They have control over the Attorney General's office, the Financial Intelligence Unit, the federal taxation administration SAT, the Center for Investigation and National Security (CISEN)**. If I had committed any irregularity, I can assure you it would be public knowledge by now," said Anaya during an interview.

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

16-11-2016 to/au 22-11-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Public Safety agencies, CRA lead pack for revoking security clearances
iPolitics.ca, Staff reporter, 2016 11 22
Ottawa—**Most of the government employees who have seen their security clearances revoked for bad behaviour since January 1 work at the Canada Revenue Agency and agencies under the purview of Public Safety Canada -- including the RCMP, Correctional Services Canada and CSIS.** An order paper question filed by Conservative MP Jim Eglinski on October 3 asked the government to provide a breakdown by department of all employees who have had their security clearances cancelled or revoked, excluding retiring employees or employees whose terms of employment had ended. It also asked how many of those employees with revoked clearances were terminated as a result and what the reasons for the revocations were. While **Public Safety Canada** itself hasn't had to revoke or cancel the security clearances of any department- specific employees, the same can't be said for several agencies that fall under its purview. Two employees at the **Canadian Security Intelligence Service** (CSIS) had their security clearances revoked and were terminated as a result. The documents tabled by the government don't give reasons for those revocations. "For reasons of national security and to protect employee safety, CSIS does not disclose the reasons or rationales as to why security clearances were cancelled or revoked," the documents say.

Un nouveau métier au sein des forces armées pour se protéger des cybermenaces
Radio-Canada (Nouvelles), Raphaël Bouvier-Auclair, 2016 11 21
Ottawa - La **menace de cyberattaques est de plus en plus présente et les Forces canadiennes veulent mieux y répondre.** Radio-Canada a appris qu'à partir de l'année prochaine, un nouveau corps de métier totalement consacré à la cyberdéfense sera créé au sein de l'armée. Le risque de cyberattaques a de nouveau été exposé au grand jour la semaine dernière. Même si l'origine du problème demeure inconnue, le site de recrutement des Forces canadiennes a été ciblé jeudi. **L'ancien directeur du Service canadien du renseignement de sécurité (SCRS) Richard Fadden** y est favorable, mais croit qu'il faut avoir une discussion nationale sur le sujet puisque, selon lui, mener des cyberattaques vient avec son lot de risques. Au Canada, il n'y a pas que la Défense nationale qui est responsable d'assurer la cybersécurité. Le ministère de la Sécurité publique et des agences comme le Centre de la sécurité des télécommunications ont aussi un rôle important à jouer.

Moscow, Beijing targeting Canada's secret info and technology, spy agency warns
Canadian Press, Jim Bronskill, 2016 11 21
Ottawa - **Canada's spy agency is openly warning that Russia and China are out to steal the country's most prized secrets. The Canadian Security Intelligence Service**, which rarely identifies security threats by name, makes the frank statement in briefing notes prepared for service director **Michel Coulombe**. While Canada grapples with the problem of jihadi-inspired extremists, the long-standing threat of espionage is also a worrisome preoccupation, the spy agency says in the notes. ``Russia and China, in particular, continue to target Canada's classified information and advanced technology, as well as government officials and systems.'' The Canadian Press used the Access to Information law to recently obtain the briefing materials, intended for use by Coulombe at a March meeting of the Senate committee on national security and defence. CSIS spokeswoman **Tahera Mufti** declined to elaborate on specific aspects of investigations, but she emphasized the spy service's broad concerns. ``Canada remains a target for the traditional espionage activities of a number of foreign states,

which continue to gather political, economic, and military information in Canada through clandestine means," she said. `

Government gamers warned of Pokemon security threat
Toronto Star, Alex Boutilier, 2016 11 21
Ottawa - **Canada's spies are guarding against a new threat to operational security: Pokemon**. Canada's electronic spy agency issued guidelines for spooks and employees playing **Pokemon Go,** a popular augmented reality game for mobile devices based on the hit 1996 Nintendo game. The game uses a phone's GPS and camera to catch and battle Pokemon in the real world; players collect, train and fight Pokemon at "Poke-stops" and "gyms" attached to locations such as churches and parks. But because the game requires location and camera data to play, it poses a risk to people who would rather not be tracked: like employees of the **Communications Security Establishment (CSE),** Canada's powerful electronic spying agency. The guidelines, obtained by the Star through an access to information request, were circulated by CSE's American counterpart, the National Security Administration (NSA). They recommend a number of steps for spooks to avoid detection while training to be the very best Pokemon master. " When asked for comment, a spokesperson for CSE said the agency takes the "operational and personal security" of its employees seriously. "With this is mind, CSE takes advantage of every opportunity, including the rise in popularity of Pokemon Go, to share security information and reminders to help ensure that our employees conduct their activities in a manner that does not put themselves or CSE at risk," **Ryan Foreman** wrote in an email last week. "We would also like to point out that we are confident that Team Rocket would never pass a CSE security clearance process."

Canadian Forces recruitment data not accessed during website hack: DND
Global News, 2016 11 19
Ottawa - The **Department of National Defence (DND) says it has re- established "positive control" over its recruitment website**, which was apparently hacked Thursday, redirecting users to the official Chinese state portal. People trying to get on forces.ca were instead directed to gov.cn, the landing page of the Chinese central government's website. Forces.ca was taken down soon after the problem was discovered. There were concerns that the personal information of military recruits may have been stolen or compromised, but authorities say that there is no evidence that this occurred.

Can you keep a secret? Going to ComicCon might help you break into Canada's spy business
National Post, Marie-Danielle Smith, 2016 11 19
Ottawa - Do you enjoy going to ComicCon? What about giveaway sunglasses or free popcorn? More importantly: can you keep a secret? Then a job as a digital spy might just be for you. Or, at least, that's what the **Communications Security Establishment (CSE)** has in mind as it **seeks the best and brightest techies**. An old-fashioned popcorn machine and free pairs of CSE-branded shades were part of the display at a government job fair Thursday at Ottawa's Shaw Centre. At the event, where the hashtag #secureyourfuture was prominently displayed, **other agencies -- including Public Safety Canada, the Canadian Security Intelligence Service (CSIS), the Canadian Forces, the Correctional Service of Canada and the Canada Border Security Agency -- competed to woo curious job-hunters**, more than one of whom was spotted eating a banana. Though the Royal Canadian Mounted Police displayed Batman-like combat gear on a mannequin, it was, subjectively, hard to compete with CSE's popcorn and shades. A CSE rep explained the agency had tried recruiting at a ComicCon event for the first time in Montreal this summer -- you know, because a lot of, uh, tech-savvy people attend ComicCon. The recruiters weren't allowed to dress up like the other cosplayers, she said, so

that's why they ordered a bunch of pairs of sunglasses. (Wearing sunglasses indoors is a good way to look like you're the Men in Black, so that's kind of like dressing up.) Applying for a job at CSE takes nine to 12 months, according to a recruiter who gave prospective applicants a PowerPoint presentation.

De nombreux candidats attirés par l'espionnage et la sécurité
TVA Nouvelles, Michelle Lamarche, 2016 11 18
Ottawa - Les **organismes de sécurité publique au Canada doivent recruter des milliers de personnes et ils semblent exercer un certain pouvoir d'attraction, comme on a pu le constater à un événement qui avait lieu ce jeudi à Ottawa**. Ils **étaient nombreux à attendre au kiosque du Service canadien de renseignement de sécurité (SCRS).** Le SCRS a besoin d'espions canadiens. Il utilise d'ailleurs les médias sociaux pour attirer les candidats. «Il y a un grand futur en sécurité», estime Hugo Caza-Levert, qui assistait au salon. «Je préfère quand ça bouge et qu'il y a de l'action dans le fond, dit pour sa part Hicham Essoltani. J'aime ça quand ça change chaque jour.» La **Gendarmerie royale du Canada doit recruter un peu moins de 1500 personnes**. «C'est dur, mais ça dépend de votre volonté, estime Audrey Jacob, étudiante en techniques policières. Nous, on veut vraiment, donc on se pousse et on le fait.» «Et à l'école, en plus, ils nous préparent super bien avec nos cours de droit, on fait aussi du conditionnement physique», soulève Alexandra Boivin, qui étudie dans le même domaine.

Hackers target Canadian government's energy and resource departments
Globe and Mail, Colin Freeze, 2016 11 18
Ottawa - **Hackers hit the Canadian government's "natural-resources, energy and environment" sector almost as much as they do all other sectors combined**, newly released numbers show. Statistics released to Parliament this week show that government systems in this sector suffered 2,078 "system compromises" in 2016. This compares with 2,493 such compromises against all other federal government sectors during the same period. These first-of- their-kind numbers were publicly released this week by a federal intelligence agency, the **Communications Security Establishment (CSE),** after a question asked in the House of Commons this fall. The **release of the statistics coincided with a mysterious, and mischievous, breach at the Department of National Defence**. On Thursday afternoon, traffic from the "Forces.ca" recruiting site was routed to one of the Chinese government's main Web pages. "It is a serious situation on the surface of it," **Public Safety Minister Ralph Goodale told reporters in Ottawa, adding that he didn't yet know precisely how it happened**.

Surveillance watchdog says C-22 not likely to be abused
iPolitics.ca, Amanda Connolly, 2016 11 17
Ottawa - The **man in charge of overseeing Canada's electronics surveillance agency says there is no reason to believe the government would abuse controversial provisions in its national security committee legislation** that give ministers the power to refuse to disclose requested information. "I don't see why they would do that unless they are in bad faith, and I assume that everybody is in good faith unless the contrary is proven to me," said **Jean-Pierre Plouffe, commissioner of the Canadian Security Establishment.** "The fears we have are seldom realized to the same extent we had thought. Yes, it is a restriction, but it is a reasonable one." Bill C-22, currently being studied at the House of Commons public safety committee, would create a nine-member committee of parliamentarians tasked with monitoring and scrutinizing the activities of all government departments and agencies that engage in national security activities. While it would bring Canada up to speed among the Five Eyes intelligence allies (we are currently the only one without such a committee), opposition critics have raised red flags over several key components of the bill. The creation of a committee tasked with national security oversight was a key campaign promise by the Liberals and also part of their

plan to reform national security in light of the controversial bill C-51, passed by the former government. That bill sparked a huge public backlash after it was perceived as going too far in allowing for expanded information sharing among government departments, enhancing the powers of the **Canadian Security Intelligence Service**, and lowering the legal threshold for who can be surveilled by law enforcement.

Spy agency kept court in the dark about data
Toronto Star, Alex Boutilier, 2016 11 16
Ottawa - **Canada's electronic spies were asked to brief the Federal Court on their intelligence-gathering activities, the Star has learned. But the Communications Security Establishment (CSE) declined to meet with federal judges earlier this year**, saying an ongoing constitutional challenge prevented them from doing so. The request came from the same judge that found CSE's partner agency, the **Canadian Security Intelligence Service (CSIS), illegally kept information on innocent people for almost a decade.** In a strongly worded ruling released this month, **Justice Simon Noël found CSIS kept the court in the dark about a program to retain and analyze data about innocent people between 2006 and 2016**. The ruling gave an unprecedented look at CSIS's Operational Data Analysis Centre, which for years had been storing data about "non-threat" individuals. While the information was intercepted legally, the court ruled it was illegal for CSIS to keep and analyze it indefinitely. The ruling came out of a briefing on the program by Noël for judges who approve CSIS warrants. In documents obtained by the Star, **CSE chief Greta Bossenmaier** was told that Noël requested a general educational briefing from her agency around the same time. But because of a constitutional challenge launched by the B.C. Civil Liberties Association (BCCLA) against CSE's intelligence activities, currently before the court, the agency declined Noël's invitation.

The RCMP Is Using the Media to 'Create Moral Panic' About Encryption
Motherboard, Jordan Pearson, 2016 11 16
The Royal Canadian Mounted Police has turned to two of the country's top media outlets to make their case for new surveillance capabilities in what critics say is a PR play orchestrated to sow public worry about privacy-boosting technology. Police in Canada have long pushed for broadened surveillance powers that would force people to unlock their phones, for example, or force telecommunication companies to provide real- time access to subscriber information. No such laws currently exist, but to show why the police believe they need them to do their jobs, the country's federal force worked with two of Canada's most respected media entities. The RCMP gave the CBC's David Seglins and the Toronto Star's Robert Cribb security clearance to review the details of 10 "high priority" investigations--some of which are ongoing--that show how the police is running into investigative roadblocks on everything from locked devices to encrypted chat rooms to long waits for information. The Toronto Star's headline describes the documents as "top-secret RCMP files."

ISIS, ISIL or something else? Declassified documents reveal struggle over what to call terrorists
National Post Online, Stewart Bell, 2016 11 16
Toronto--**When a federal bureaucrat circulated a map depicting "the Islamic State's regional spread," an email soon followed from the Foreign Affairs Department saying the document had to be changed**. "We do not recognize the group as 'The Islamic State' and it is important it not be suggested that we do," read the email, which proposed amending the wording to " 'the global ambitions of ISIL' or something similar." Declassified documents released under the Access to Information Act show how Canadian officials struggled with language as they drafted a key report on terrorism in the age of the Islamic State of Iraq and the Levant. Planning for the latest annual Public Report on the Terrorist Threat to Canada began in

April 2015, during the final months of the Conservative government. But the process dragged on for so long it was not released until August 2016. An RCMP analyst said the report failed to recognize the "wide-ranging nature" of the terrorist threat, particularly the danger posed by " 'lower-risk' activities such as the perpetuation of violent ideologies, recruiters, facilitators and fundraising." **Michel Coulombe, director of the Canadian Security Intelligence Service**, was concerned about the report's reference to the roughly 180 Canadians overseas taking part in terrorist activities - including about 100 in Syria and Iraq.

Mounties lobbying for more power
Toronto Star and CBC News, Robert Cribb and CBC staff, 2016 11 16
Ottawa - The **RCMP is lobbying Prime Minister Justin Trudeau for more powers - including access to digital information without warrants** - to investigate suspects who are hiding behind uncrackable encryption on their digital devices, a Toronto Star/CBC investigation has found. "I can safely say that there's criminal activity going on every day that's facilitated by technology that we aren't acting on," RCMP Commissioner Bob Paulson told the Toronto Star and CBC in an exclusive interview. "We're losing our ability, if we haven't lost it entirely, to bring the traditional investigative response to technologically facilitated crime because of the misunderstanding, in my view, of the privacy threat." The RCMP has reached a point, Paulson said, that Canadians should "think about where you go with that complaint because I don't know that we can help you." Two weeks ago, a **Federal Court judge denounced the Canadian Security Intelligence Service's monitoring and retention of information on thousands of Canadians'** and, in Quebec, police forces admitted to intercepting and tracking cellphones belonging to at least 10 journalists. "I can't sit here and say that it's going to be a perfect," Paulson said.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

Hackers get leeway to report Pentagon bugs
Washington Post, Ellen Nakashima, 2016 11 22
Washington - The **Defense Department on Monday became the first U.S. government agency to launch a policy enabling researchers to report bugs or flaws they discover in its websites without fear of prosecution**. Calling it a "see something, say something" policy for the digital domain, Defense Secretary Ashton B. Carter said the program is aimed at improving the security of the Pentagon's unclassified, public-facing networks. The Army also opened registration Monday for Hack the Army, a challenge in which researchers and hackers scour Army sites for software flaws and compete for thousands of dollars in bounty rewards. The Army contest explicitly authorizes researchers to try to hack a limited set of Army systems to find weaknesses.

Muslims at the Pentagon Brace for Trump Administration
The Daily Beast, Nancy A. Youssef, 2016 11 22
Washington - **Donald Trump's inauguration may be 58 days away, but for the Muslim officials once welcomed into the U.S. government's war on terrorism, the change already has** begun. Four U.S. officials who spoke to The Daily Beast said **fear is pervasive among Muslims inside the halls of the Pentagon, the CIA, and the Department of Homeland Security** in anticipation of a Trump administration. Already, the officials said, they are seeing

colleagues who are less willing to share their thoughts about national security. They fear they will no longer be seen as an asset to confronting terrorism but rather suspect members of the government they serve. It is, one U.S. official explained, a climate of "anticipatory freakout." Will Muslim CIA agents be asked to register? Will the next commander in chief ban the family of Muslim troops from visiting this country? Will Muslim members of the Department of Homeland Security face increased scrutiny based on their faith?

Trump's CIA pick would reinstate US collection of phone data
San Francisco Chronicle, Bob Egelko, 2016 11 22
San Francisco - The **federal government's long-hidden authority to sweep up records of all phone calls made in the U.S. was repealed last year in a bipartisan vote of Congress**. But **President-elect Donald Trump's choice to head the CIA has called for reinstatement of the data haul and said its elimination was part of "Edward Snowden's vision of America."** Snowden, a former National Security Agency contractor, revealed in 2013 that the NSA had been collecting bulk data on U.S. phone calls without a warrant for more than a decade. President George W. Bush's administration had ordered the collection unilaterally after the terrorist attacks of Sept. 11, 2001, then obtained approval from a secret intelligence court in 2006. The records contain so-called metadata, showing the numbers called and duration of the calls, but not the content of the messages. The law that President Obama signed in June 2015, called the USA Freedom Act, leaves the records with the phone companies but allows the National Security Agency to request data on individual customers without a court order. Rep. **Mike Pompeo**, R-Kan., whom Trump named Friday as his choice for CIA director, was among a minority of House Republicans who opposed the change. In a December 2015 column in the National Review magazine, he attacked Republican presidential candidates who supported the new law.

Trump spokesman declines to back FBI Director James Comey
Washington Post, Multiple reporters, 2016 11 21
Washington - A **spokesman for President-elect Donald Trump pointedly declined to back embattled FBI Director James Comey on Monday**, saying Trump would meet with the nation's top law enforcement officer "at some point." "There hasn't been any official statement with regard to Director Comey," Trump spokesman Jason Miller said during the transition team's daily briefing. Asked if Trump would seek the resignation of Comey, who played a controversial role in the presidential campaign's final days, Miller said only: "I would imagine that at some point, the two will meet." Trump, who at times assailed the FBI and called Comey corrupt during the campaign, told "60 Minutes" after his election victory that he had not decided whether to ask Comey to step down.

Panetta: At CIA, Pompeo will have to deliver the bad news to Trump as well as the good
McClatchy News Service, Curtis Tate, 2016 11 21
Washington - **Former CIA Director Leon Panetta said that Donald Trump's choice to lead the agency will have the task of telling the president things he doesn't want to hear**. If he's confirmed by the Senate, **Kansas Republican Rep. Mike Pompeo** will lead the agency's 21,500 employees worldwide. Panetta, who led the CIA from 2009 to 2011 under President Barack Obama, said Pompeo should get to know and trust the professionals who work for the agency. "The most important thing is to respect those who are doing the job at the CIA," Panetta said in a phone interview with McClatchy. "They're not Democrats. They're not Republicans. They're good Americans who are trying to do a very tough job." Panetta said good intelligence was "absolutely critical" when the country is facing a number of flashpoints around the world. Overall, Panetta said Pompeo is "a pretty good choice" to lead the CIA.

NSA chief defends record at Halifax forum amid rumoured calls for his ouster
Canadian Press, Staff report, 2016 11 21
Halifax - The **director of the U.S. National Security Agency defended his record at the Halifax International Security Forum as rumours swirl about calls for him to be ousted from his current post** and a potential promotion in president-elect Donald Trump's administration. At a panel Sunday, **Admiral Mike Rogers** refused to address media reports saying America's top defence and intelligence officials recommended his dismissal. "Just let me cut to the chase, because I'm interested in saving us all some time," Rogers said in response to a question from the audience. "I am just not going to go down this road."

NSA Head Rogers on His Recommended Firing: 'I'm Accountable for My Actions'
US News and World Report, Paul D. Shinkman, 2016 11 21
Halifax - **Navy Adm. Mike Rogers, chief of U.S. Cyber Command and the National Security Agency, said he was "accountable for his actions"** following a report published during a security conference he attended here this weekend that senior administration officials have recommended President Barack Obama remove him amid concerns with his performance and the possible splitting of command duties for the two secretive organizations he leads. "I'm not going to go down that road," Rogers said, interrupting a journalist who asked about The Washington Post story during a forum where the admiral was speaking. Meanwhile, the 57-year-old admiral's recent trip to New York to meet with President-elect Donald Trump on Thursday also caused "consternation" for the Obama administration, the Post said, in part because it appears unprecedented for an officer like Rogers to conduct such a meeting and not inform his superiors.

Obama Is Considering Removing N.S.A. Leader
New York Times, Julie Hirschfeld Davis, David E. Sanger & Eric Schmitt, 2016 11 20
Washington - **President Obama is considering removing Adm. Michael S. Rogers from his posts as leader of the National Security Agency and United States Cyber Command after top officials expressed frustration over the speed at which Admiral Rogers had moved to combat the Islamic State and over the agency's repeated loss of closely guarded secrets**, administration and intelligence officials said Saturday. President-elect Donald J. Trump is considering Admiral Rogers, who is responsible for surveillance and the growing arsenal of cyberweapons, for a top post in his administration, including director of national intelligence overseeing all 16 intelligence agencies. Admiral Rogers met with Mr. Trump on Thursday, apparently without the White House's knowledge. The recommendation to remove Admiral Rogers, a career intelligence officer who was promoted to his posts by the Obama administration two years ago, came last month from **Defense Secretary Ashton B. Carter and the current director of national intelligence, James R. Clapper Jr. Administration and intelligence officials, who insisted on anonymity to detail the private discussions**, said the recommendation that Admiral Rogers be removed was not related to Mr. Trump's interest in hiring him.

Pompeo's reputation is as a partisan student of national security issues
Washington Post, Greg Miller, 2016 11 19
Washington - **President-elect Donald Trump's pick to lead the CIA is a Kansas congressman who is widely respected for his intelligence but also seen as a fierce partisan on polarizing issues including the deaths of U.S. personnel in Benghazi, the leaks of Edward Snowden and the email controversy that engulfed Hillary Clinton. Rep. Mike Pompeo** (R-Kan.) has used his perch on the House Intelligence Committee to attack major pillars of President Obama's foreign policy agenda, including the nuclear deal with Iran. Just hours before his name surfaced as Trump's CIA nominee, Pompeo tweeted that he looked

forward to "rolling back this disastrous deal with the world's largest state sponsor of terrorism." In closed-door briefings on Capitol Hill, Pompeo, who had previously supported efforts to oust Syrian president Bashar al-Assad, has been an intense critic of a covert CIA program to train and arm moderate rebel forces in Syria, according to U.S. officials. They said that dismantling the program - or at least subjecting it to a major reevaluation - would likely be at the top of his agenda if he is confirmed. Pompeo, 52, has no meaningful experience in espionage issues beyond his relatively brief stint as a member of the House Intelligence Committee. But he **has earned a reputation as a serious student of national security issues** who finished first in his class at the U.S. Military Academy at West Point, served as a cavalry officer in the Army and earned a law degree from Harvard.

Trump Turns to His Right Flank to Fill National Security Posts
New York Times, Julie Hirschfeld Davis, 2016 11 19
Washington - **President-elect Donald J. Trump moved quickly on Friday to begin filling national security posts at the top echelons of his administration**, selecting a group of hawks and campaign loyalists who reflect the hard-line views that defined his run for president. Mr. Trump said he would nominate as **attorney general Senator Jeff Sessions** of Alabama, who has been a fierce supporter of a crackdown on undocumented immigrants. The president-elect also **moved to install Michael T. Flynn, a retired lieutenant general who has said that Islamist militancy poses a global existential threat, as his national security adviser**. And as **director of the C.I.A., Mr. Trump selected Representative Mike Pompeo** of Kansas, who harshly criticized Hillary Clinton during the House investigation of the 2012 attack on the United States diplomatic compound in Benghazi, Libya. All three are regarded, in some ways, as outliers from conventional Republican thinking, shunned at times for strident statements, controversial positions or highly partisan moves. The flurry of announcements indicated that Mr. Trump was gaining control over a transition operation that had been entangled in infighting during its early stages.

America's Top Spy Talks Snowden Leaks and Our Ominous Future
Wired, Garrett M. Graff, 2016 11 19
Analysis: Public appearances don't come easily to **James Clapper, the United States director of national intelligence**. America's top spy is a 75-year-old self-described geezer who speaks in a low, guttural growl; his physical appearance--muscular and bald--recalls an aging biker who has reluctantly accepted life in a suit. Clapper especially hates appearing on Capitol Hill, where members of Congress wait to ambush him and play what he calls "stump the chump." As he says, "I rank testimony--particularly in the open--right up there with root canals and folding fitted sheets." One of the things Clapper does profess to enjoy about his job is meeting with the men and women who make up his covert empire of 17 agencies, which range from brand names like the **CIA, NSA, DEA, and FBI to lesser-known units like the Treasury Department's Office of Intelligence and Analysis.** As he has traveled the country and the world over his six years in office, he has hosted scores of town hall meetings with intelligence officers, analysts, and operatives. The events are typically low-key, focusing less on what's in the news than on the byzantine and, to Clapper, almost soothing minutiae of the military-intelligence bureaucracy. And so it was that he found himself in late August in an auditorium at US Strategic Command near Omaha, Nebraska, headquarters of the nation's nuclear forces, taking questions from a group of 180 civilian and military personnel.

Donald Trump hopes to abolish intelligence chief position, CIA reforms
The Intercept, Matthew Cole & Jenna McLaughlin, 2016 11 19
Washington - **Donald Trump's National security team is discussing plans to dismantle the Office of the Director of National Intelligence**, the organization that was created in response

to the 9/11 attacks, according to an adviser to the president-elect and a former senior intelligence official. The news comes as the current director of national intelligence, James Clapper, announced his resignation Thursday. The **Trump national security team has been meeting in recent days, planning the removal of the cabinet- level position and assessing how to fold parts of the organization into the 16 federal intelligence agencies it oversees, according to both people with knowledge of the plans**. If the restructuring is accomplished, it would undo legislation passed by Congress in 2004, dismantle the biggest American intelligence bureaucracy created since the end of World War II, and roll back a key recommendation of the 9/11 Commission. The national security team believes the effort will be "long and messy" but is confident it will be successful, according to the former senior U.S. intelligence official who is consulting with those involved in the transition. Both sources asked for anonymity because they are not authorized to speak publicly about confidential plans. The former senior intelligence official, who supports the proposal, said the DNI was never a solution to the 9/11 attacks. "It was always a naive idea that American intelligence can be 'fixed.' You'll never get it all correct," the former official said. "You can never have 100 percent intelligence, never stop every terror plot or penetrate every terrorist cell. There will always be gaps." **The Office of the Director of National Intelligence declined to comment,** but a source close to Clapper said the director was not aware of the Trump transition team's plans.

Clapper: US collects and analyzes more intelligence on jihadi groups now than ever
Long War Journal, Thomas Joscelyn, 2016 11 18
Washington - **Director of National Intelligence (DNI) James Clapper announced his retirement during a hearing held by the House Permanent Select Committee on Intelligence (HPSCI)** earlier today. In his written testimony, Clapper offered this assessment: "Violent extremism, which has been on an upward trajectory since the late 1970s, has generated more IC collection and analysis against groups, members, and safe havens than at any other point in history. These include: the Islamic State of Iraq and the Levant; al-Qa'ida with its nodes in Syria, Pakistan, Afghanistan, and Yemen; al-Shabaab, al- Qa'ida's affiliate in East Africa; and Iran, the foremost state sponsor of terrorism, which continues to exert its influence in regional crises in the Middle East through the Islamic Revolutionary Guard Corps - Qods Force, its terrorist partner Lebanese Hizbollah, and proxy groups."

NI Clapper: Russia has 'curtailed' cyber attacks
USA Today, Eliza Collins, Kevin Johnson, 2016 11 17
Washington - **Russian government hackers "curtailed" their cyber espionage against U.S., political institutions after the Obama administration formally blamed the nation last month for breaching the computer systems of the Democratic National Committee and other entities, Director of National Intelligence James Clapper told a House panel** Thursday. "That activity seemed to have curtailed," Clapper told the House Intelligence Committee. "I can't say what the impact of a new (Trump) administration will have on Russian behavior." The previous breaches and recent scanning of some states' voter registration data bases prompted intelligence authorities to ramp-up cyber defenses in advance of the general election earlier this month.

TITANPOINTE
The Intercept, Ryan Gallagher, Henrik Moltke, 2016 11 16
New York - For many New Yorkers, **33 Thomas Street -- known as the "Long Lines Building" -- has been a source of mystery for years.** It has been labeled one of the city's weirdest and most iconic skyscrapers, but little information has ever been published about its purpose. It is not uncommon to keep the public in the dark about a site containing vital telecommunications equipment. But 33 Thomas Street is different: An investigation by The

Intercept indicates that the skyscraper is more than a mere nerve center for long-distance phone calls. It **also appears to be one of the most important National Security Agency surveillance sites on U.S. soil -- a covert monitoring hub that is used to tap into phone calls, faxes, and internet data.** Documents obtained by The Intercept from the NSA whistleblower Edward Snowden do not explicitly name 33 Thomas Street as a surveillance facility. However -- taken together with architectural plans, public records, and interviews with former AT&T employees conducted for this article -- they provide compelling evidence that 33 Thomas Street has served as an NSA surveillance site, code-named TITANPOINTE. Inside 33 Thomas Street there is a major international "gateway switch," according to a former AT&T engineer, which routes phone calls between the United States and countries across the world. A series of top-secret NSA memos suggest that the agency has tapped into these calls from a secure facility within the AT&T building.

La CPI veut enquêter sur les prisons secrètes de la CIA
Le Monde, Stéphanie Maupas, 2016 11 16
Washington - Des **Américains auraient eu " recours à des méthodes constitutives de crimes de guerre " L'enquête à venir de la Cour pénale internationale (CPI) sur les crimes commis en Afghanistan devrait notamment porter sur les crimes commis par l'Agence centrale de renseignement (CIA)** américaine dans les prisons secrètes installées en Pologne, en Roumanie et en Lituanie. Dans un document rendu public lundi 14 novembre et portant sur les dix examens préliminaires menés actuellement par ses services, dont l'un porte sur la guerre en Afghanistan, la procureure Fatou Bensouda indique qu'elle pourrait enquêter sur les crimes commis par la CIA dans les prisons secrètes en Europe où " des membres présumés d'Al-Qaida ou des talibans auraient été transférés " depuis l'Afghanistan. Le bureau de la procureure avait ouvert un examen préliminaire - une étape préalable à l'ouverture d'une enquête - en 2007, et répertorié de nombreux crimes contre l'humanité et crimes de guerre commis par les talibans, par la police, par les services secrets afghans et par les forces armées américaines.

NSA Chief: 'Uneven' Cooperation Between Public, Private Sectors Impedes Cyber Defenses
Wall Street Journal, Alan Cullison, 2016 11 16
New York - The **head of the U.S. National Security Agency said "uneven" cooperation between the government and private sector has hampered the fight against a "literal onslaught" of cyber attacks from criminal and state-supported hackers**. Speaking at The Wall Street Journal CEO Council, **Adm. Michael S. Rogers** said the host of hackers is "so large and so diverse" that perpetrators are difficult to identify. About two-thirds are criminals or criminal groups looking to steal personal information for financial gain, and the balance are state-sponsored hackers, he said. He said company leaders need to take a personal interest in cyber security, which has become too important a matter to be delegated entirely to network security specialists.

U.S. Officials Fear Trump Is Playing Into Terrorists' Hands
The Daily Beast, Shane Harris, Nancy A. Youssef, 2016 11 16
Washington - **U.S. officials who've been working to refute terrorist propaganda and blunt recruitment by ISIS and other groups are bracing for a Donald Trump administration, fearing that he and his advisers could set back their efforts by years and play into terrorists' hands**. Three U.S. officials told The Daily Beast that President-elect Trump's campaign rhetoric, combined with the names now surfacing as potential top national security advisers in the next administration, signal a dramatically different approach that could give ISIS ammunition to claim that the United States is engaged in a religious war. In fact, ISIS

commanders have already begun to make that argument. "This guy [Trump] is a complete maniac," Abu Omar Khorasani, an ISIS leader in Afghanistan, told Reuters. "His utter hate towards Muslims will make our job much easier because we can recruit thousands." Equating radical terrorism with Islam was not only inaccurate, it was "not very helpful if we are talking about a lasting ISIS defeat," one defense official told The Daily Beast, adding that it allows the terror group to claim that it is defending Muslims everywhere. "They will say, 'Join us. America has declared war on Islam.'"

Why Mike Rogers's departure from the Trump team is alarming
Washington Post, David Ignatius, 2016 11 16
Column - The **ouster of former congressman Mike Rogers (R-Mich.) from Donald Trump's transition team is a worrisome sign of continuing internecine battles in the GOP and the ascendancy of Trump's personal political allies in shaping the president-elect's agenda**. Rogers, a widely respected former FBI agent who headed the House Intelligence Committee, had been seen as a figure of stability and continuity in intelligence matters. He was mentioned as a possible next director of the CIA or director of national intelligence.. Rogers had angered House GOP hard-liners when his committee issued a bipartisan report in 2014 clearing Hillary Clinton of personal wrongdoing in the 2012 Benghazi incident. That report was characteristic of the way Rogers chaired the committee, in a working partnership with then-ranking Democrat, Rep. C.A. Dutch Ruppersberger (Md.). (Rogers added "additional views" that criticized "senior State Department officials" for dismissing threat warnings, denying requests for extra security in eastern Libya and other errors.)

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

Elite police unit to guard airports and nuclear sites
London Times, Francis Elliott, 2016 11 22
London - **Theresa May is to approve plans for an elite armed police force to protect Britain's most sensitive infrastructure from a Paris-style terrorist attack**. The new force would merge existing bodies including the **British Transport Police, Civil Nuclear Constabulary and Ministry of Defence Police.** Mrs May, as home secretary, said there was a need for a central command because of the targeting of transport hubs and civil nuclear sites by Islamist terrorist groups in Europe last year. Whitehall sources said that ministers were determined to end so-called "blue light races" in which forces competed to respond first to incidents. Protocol usually grants overall control of the response to an incident to the first force that arrives.

Parliament hands police and Government sweeping spying powers with new bill
The Independent (UK), Andrew Griffin, 2016 11 19
London - The **House of Lords has passed the Investigatory Powers Bill**, putting the huge spying powers on their way to becoming law within weeks. The bill - which forces internet companies to keep records on their users for up to a year, and allows the Government to force companies to hack into or break things they've sold so they can be spied on - has been fought against by privacy campaigners and technology companies including Apple and Twitter. But the Government has worked to continue to pass the bill, despite objections from those companies that the legislation is not possible to enforce and would make customers unsafe. The House of

Lords's agreement to the text now means that it just awaits Royal Assent, at which point it will become law.

SAS favourite ready to take on world
London Times, Deborah Haynes, 2016 11 19
London - The **man wanted by Donald Trump as his national security adviser has a close relationship with Britain's special forces** (Deborah Haynes writes). **Lieutenant-General Michael Flynn is highly regarded by SAS soldiers who worked with him against al-Qaeda in Iraq after the invasion in 2003 and in covert operations against the Taliban in Afghanistan**. "He is one of the brothers from another mother," a former SAS officer said. "He is a legend. It will make the bond between UK and US special forces even stronger with Mike in the White House. He has killed a lot of bad guys one way or another. He is good news." An outspoken maverick, General Flynn, 57, joined the army as an intelligence officer in the 1980s. He was director of intelligence for Joint Special Operations Command from 2004 until 2007. He was credited with helping to develop a powerful fighting machine, using **American and British special forces and spy agencies**, that fused intelligence with lethal force to break al-Qaeda's Iraq network.

'Extreme surveillance' becomes UK law with barely a whimper
The Guardian (London), Ewen MacAskill, 2016 11 19
London - A **bill giving the UK intelligence agencies and police the most sweeping surveillance powers in the western world has passed into law with barely a whimper**, meeting only token resistance over the past 12 months from inside parliament and barely any from outside. The **Investigatory Powers Act**, given royal assent on Thursday, legalises a whole range of tools for snooping and hacking by the security services unmatched by any other country in western Europe or even the US. The security agencies and police began the year braced for at least some opposition, rehearsing arguments for the debate. In the end, faced with public apathy and an opposition in disarray, the government did not have to make a single substantial concession to the privacy lobby. US whistleblower Edward Snowden tweeted: "The UK has just legalised the most extreme surveillance in the history of western democracy. It goes further than many autocracies." Snowden in 2013 revealed the scale of mass surveillance - or bulk data collection as the security agencies prefer to describe it - by the US National Security Agency and the **UK's GCHQ**, which work in tandem. But, against a backdrop of fears of Islamist attacks, the privacy lobby has failed to make much headway.

Return to Table of Contents/ Retour à la table des matières

Australia / Australie

Controversial terror laws clear parliament
Australian Associated Press, Roje Adaimy, 2016 11 22
Canberra - **Authorities will soon be able to impose control orders on children as young as 14 after controversial counter-terrorism laws cleared parliament. A bill that included a suite of measures passed the lower house** on Tuesday after changes were made in the Senate earlier this month. Aside from reducing from 16 the age a person can be subject to a control order, the legislation creates a new search, telecommunications interception and surveillance regime for those under the orders. Courts will be required to appoint a lawyer to act for minors under 18 if they don't already have one in proceedings relating to a control order. It also makes advocating genocide illegal.

Chinese spies in Australia on the rise, former diplomat Chen Yonglin says
ABC (Australia), Andrew Greene, 2016 11 20
Canberra - A **former Chinese diplomat who sensationally quit his job in 2005 breaks a lengthy silence to warn of a growing number of spies and agents working for Beijing in Australia**. Chen Yonglin, the Chinese diplomat who sensationally quit his job more than a decade ago, has broken a lengthy silence to warn of a growing number of spies and agents working for Beijing in Australia. In 2005, Mr Chen caused global headlines when he claimed China was operating a network of "over 1,000 Chinese secret agents and informants in Australia". The former diplomat, who now works as a businessman, has warned the number of secretive Chinese operatives has steadily grown since he stopped working for China's foreign service. "

Buyer beware of sending data overseas: former spy boss
Canberra Times, David Ellery, 2016 11 18
Canberra - **Australia's former top spy has warned companies doing business with foreign call centres and data storage providers to do their homework before sending sensitive information offshore. David Irvine, a former head of both ASIO and ASIS**, said once information left Australia it was no longer protected by Australian sovereign law. This made it possible for Australians' private details, including phone records, sourced through call centre workers in India and elsewhere, to be offered for sale by Al Solutions, a Mumbai security firm. "If you lose control of your data, that sort of thing is entirely possible," he said. "It relates to your ability to have suitable arrangements and controls in place with your external suppliers." The shift towards cloud computing and the storage of sensitive corporate and government data in commercial data centres had been going on for almost a decade.

Telcos face questions as black-market data prompts warnings
Sydney Morning Herald, Lucy Battersby & Nick McKenzie, 2016 11 18
Canberra - The **Australian Information and Privacy Commissioner is investigating allegations personal information held by telcos can be bought on the black market from overseas call centres**. "I am concerned about allegations that personal information of Australian telecommunication customers is being offered for sale online. My office is making inquiries with Optus, Telstra and Vodafone to determine what further action I may take in this matter," Timothy Pilgrim said on Thursday. Meanwhile, the **former head of both ASIO and ASIS, David Irvine, warned the industry that once information left Australia, it was no longer protected by Australian sovereign law.** "If you lose control of your data, that sort of thing is entirely possible," he said at the Association of Corporate Counsel National Conference in Canberra on Thursday.

Return to Table of Contents/ Retour à la table des matières

New Zealand / Nouvelle-Zélande

PM calling for answers overdamaged city buildings
New Zealand Herald, Matthew Backhouse, 2016 11 17
Wellington— Modern **buildings in central Wellington should never have been so badly damaged in Monday's earthquake** and only lucky timing prevented any deaths, a seismic engineer says. The Prime Minister is now calling for answers after two government buildings,

both built within the past decade, were among the worst hit in the magnitude 7.8 quake. Wellington council inspectors have so far found 60 buildings of concern with signs of structural damage, and 28 at risk of part of the building falling down. Wellington Mayor Justin Lester yesterday said the city's most badly damaged building, the tower at 61 Molesworth St, would need to be deconstructed. An **exclusion zone** was yesterday widened to include Pipitea House, built in 2011, because of concerns with its facade in high winds. The building houses the **Government Communications Security Bureau and the Security Intelligence Service**.

Defence plan outlines major New Zealand military spending program
Xinhua News Agency, John Macdonald, 2016 11 16
Wellington - The New **Zealand government Wednesday unveiled details of a major military spending program to align its forces' capabilities with those of Australia and other defense partners**. The **Defence Capability Plan 2016** detailed spending of 20 billion NZ dollars (14.19 billion U.S. dollars) on the **New Zealand Defence Force (NZDF)** out to 2030 equal to 1 percent of gross domestic product each year. The plan said New Zealand sought to maintain interoperability with Australia, so the two countries could coordinate peace and security operations in the South Pacific.

Return to Table of Contents/ Retour à la table des matières

International

China / Chine

China doubles down on internet control after tough new law
Associated Press, Gerry Shih, 2016 11 17
Beijing - **China's leaders and official media are pushing for greater control of the internet and technology products as tensions surrounding a far-reaching Chinese cybersecurity law** loom over a gathering this week of the world's leading tech firms and Chinese officials. The Communist Party's mouthpiece People's Daily warned in an editorial on Thursday that China must break monopolies over core technologies and standards and remain untethered to other countries' technology supply chains. The commentary, aimed apparently at Silicon Valley in unusually stark terms, comes one day after **President Xi Jinping called for "more fair and equitable" governance of the internet at the opening of the state-run World Internet Conference.**

Threats from cyberspace 'pressing and vital' in China: top State secret official
Global Times, Staff reporter, 2016 11 17
Beijing - **Security threats coming from cyberspace are pressing and vital and China must increase its efforts to improve security technology to safeguard national interests, said a top official from the State secret administration**. "A series of Internet leaks in China and other countries show the threats coming from cyberspace are pressing and vital, and the technology to safeguard information security needs to be reliable, self- developed and controllable," **Tian Jing**, director of the **National Administration for the Protection of State Secrets**, told the People's Daily in an interview that was published on the newspaper's website on Wednesday..

President Xi stresses int'l cooperation in cyberspace governance
Xinhua News Agency, Staff reporter, 2016 11 16
Beijing - **Chinese President Xi Jinping on Wednesday called for increased international cooperation in cyberspace governance and the building of a cyberspace community of common destiny.** Noting that Internet development has no boundaries, Xi said **China is willing to work with the international community for the common welfare for all people**, to uphold the concept of cyberspace sovereignty and to make the global cyberspace governance system fairer and more reasonable. Xi made the remarks while giving a speech via video at the opening ceremony of the third World Internet Conference (WIC) in the riverside town of Wuzhen, east China's Zhejiang Province. Liu Yunshan, a member of the **Standing Committee of the Political Bureau of the Communist Party of China (CPC) Central Committee**, attended the opening ceremony of the WIC and delivered a speech.

Return to Table of Contents/ Retour à la table des matières

Russia / Russie

Ukraine blames Russian security service for prank call to president
Reuters, 2016 11 17
Kiev— **Ukraine on Thursday blamed the Russian state security service for orchestrating a prank call to Ukrainian President Petro Poroshenko from someone pretending to be the president of Kyrgyzstan.** Earlier in November, Poroshenko's office announced a conversation with Kyrgyz leader Almazbek Atambayev, only for the latter to issue a statement saying the call had not taken place.A recording of the call was subsequently published online, but Kiev said parts where Poroshenko was critical of Russia and its President Vladimir Putin were cut. Russia annexed the Crimean peninsula from Ukraine in 2014 and supports separatist rebels in Ukraine's eastern Donbass region. "Now I understand why the so-called pranksters waited for so long. They were doctoring the conversation and had to wait even longer to get approval from their supervisors in the Kremlin and the **FSB**," said Svyatoslav Tsegolko, Poroshenko's spokesman.

L'étrange arrestation d'un ministre russe
Le Figaro, Pierre Avril, 2016 11 16
Moscou - Le **ministre de l'Économie a été interpellé, alors qu'il recevait un pot-de-vin de 2 millions de dollars**. C'est un séisme dans le monde politique russe. Pour la première fois depuis la chute de l'URSS, il y a vingt-cinq ans, un haut membre du gouvernement russe a été arrêté pour corruption. Le **ministre de l'Économie, Alexeï Oulioukaïev, en personne a été interpellé par le FSB (ex-KGB) dans la nuit de lundi à mardi**, alors qu'il recevait un pot-de-vin de 2 millions de dollars. Il a ensuite été conduit devant un juge qui a délivré un mandat d'arrêt à domicile. Ce pilier du gouvernement, considéré comme un libéral, est officiellement accusé d'avoir monnayé son soutien au rachat, par le géant pétrolier mondial Rosneft, de son concurrent Bashneft, entreprise publique classée au sixième rang du secteur. Détail piquant, l'entreprise accusée d'avoir corrompu le haut fonctionnaire - Rosneft - est la même qui aurait dénoncé le scandale auprès des autorités judiciaires, à travers son responsable de la sécurité, lui- même un ancien du FSB.

Return to Table of Contents/ Retour à la table des matières

Europe

Un attentat « déjoué » rappelle la persistance de cellules organisées en France
Le Monde, Elise Vincent, 2016 11 22
Strasbourg, France - Le **ministère de l'intérieur a annoncé l'arrestation à Strasbourg et Marseille de sept personnes, soupçonnées d'avoir planifié des attaques terroristes en France**. C'est un important projet d'attentat, possiblement fait d'attaques simultanées, qui a été «déjoué» suite à une vague d'interpellations à Strasbourg et à Marseille, dans la nuit du samedi 19novembre au dimanche 20novembre. Le ministre de l'intérieur, Bernard Cazeneuve, l'a annoncé lui-même, lundi 21novembre. Une série d'arrestations qui s'ajoute à d'autres et à la vingtaine d'attentats «déjoués» depuis le début de l'année, selon la place Beauvau, et vient rappeler que des cellules très structurées sont toujours dormantes, en France. Alors que le dernier attentat sur le sol français, le 26juillet, à Saint-Etienne-du-Rouvray (Seine-Maritime), a mis au jour l'existence d'un djihad «low cost», sans argent, et sans plan prévu très en amont, les interpellations réalisées dans le cadre de cette **vaste opération conduite par la Direction générale de la sécurité intérieure (DGSI), prouvent l'existence parallèle d'un modèle inverse.**

Finland: Centre to counter hybrid warfare to be established in Helsinki
Esmerk Finnish News, 2016 11 22
Helsinki— **Several Nato and EU countries plan to establish a centre in Finland to counter hybrid warfare.** The structure of the centre will be light and it will consist of networks. Head of Department Mikko Saarelainen of **Finnish Security Intelligence Service (Supo)** has been appointed Project Manager of the centre. Representatives of 11 countries including the USA and Baltic countries participated in the constituent meeting in Helsinki in Finland. The centre will begin its operations in spring 2017 in Helsinki. It will employ 4-6 persons. The costs will be approximately EUR 2mn, of which Finland probably will cover the majority.

Renseignement : l'autorité de contrôle des écoutes passe à l'offensive
Le Monde, Jacques Follorou, 2016 11 22
Paris - La **CNCTR vient de mettre au jour un pan entier des interceptions, celles par voie hertzienne, qui lui étaient jusqu'ici interdites d'accès.** C'est une ligne de front invisible pour le grand public, où se parle une langue indigeste. C'est pourtant là que se défendent les frontières de l'Etat de droit. Après avoir subi quelques revers, la **Commission de contrôle des techniques de renseignement (CNCTR)** repart à l'offensive, profitant de la censure, le 21 octobre, par le Conseil constitutionnel, de l'article du code de sécurité intérieure consacré à la surveillance des communications circulant par la voie hertzienne.

Nucléaire: les services belges n'ont rien trouvé dans le "darknet"
Agence Belga, 2016 11 22
Bruxelles— **Ni les services de sécurité, ni une société privée n'ont trouvé sur le "darknet" des documents relatifs aux installations nucléaires belges** qui auraient mis en péril la sécurité de celles-ci, a indiqué mardi le directeur du Centre de cybersécurité, Miguel De Bruycker, devant la sous-commission "sécurité nucléaire" de la Chambre. Les journaux de SudPresse ont relaté le mois passé la façon dont ils avaient trouvé sur le "darknet" (des réseaux de partage anonymes utilisés en général par des criminels) des plans des centrales nucléaires de Tihange. Le **Centre de cybersécurité en a immédiatement référé à la Sûreté de l'Etat et aux renseignements militaires (SGRS) afin** de savoir si des documents mettant

en jeu la sécurité des installations nucléaires se trouvaient dans le "darknet". Une société privée a également été consultée et un "pirate éthique" a proposé ses services.

Alleged CIA prison in Lithuania on international prosecutors' radar screen
Baltic News Network, 2016 11 21
Vilnius— **Lithuania may face additional international pressure over suspicions that Americans operated a secret prison for terror suspects near Vilnius** a decade ago as prosecutors of the International Criminal Court (ICC) are considering launching a full-scale investigation into allegations that prisoners were tortured at the **Central Intelligence Agency's secret detention facilities.** Law experts think that investigators may ask for information from Lithuania, but add that Washington's refusal to cooperate may bring the case to a halt. Fatou Bensouda, the chief prosecutor of The Hague court, released last week a preliminary report on allegations that US troops and CIA agents might have tortured terror suspects.

L'affaire Squarcini ravive les tensions LVMH-Hermès
Le Monde, Simon Piel, 2016 11 19
Paris - Selon nos informations, **Hermès a décidé, après avoir reçu un avis à victime de la part des magistrats instructeurs, de se constituer partie civile le 12 octobre dans l'affaire qui vise l'ancien directeur de la Direction centrale du renseignement intérieur (ex-DCRI, aujourd'hui DGSI), Bernard Squarcini**. Une décision qui n'a rien d'anodin. Selon le code de procédure pénale, cela signifie que l'entreprise Hermès considère qu'elle a pu être " lésée par un délit " . Elle va désormais pouvoir suivre l'instruction en ayant accès au dossier et éventuellement faire des - demandes d'actes.

Le procès du vol de données des services secrets s'ouvre à Bellinzone
Le Temps, 2016 11 19
Zurich— **Le Service de renseignement de la Confédération (SRC) a frôlé la catastrophe en 2012, lorsque l'un de ses collaborateurs a dérobé une masse de données**. Quatre ans plus tard, l'informaticien à l'origine de l'une des plus graves crises de confiance qu'aient **connu le renseignement helvétique, comparaît devant le Tribunal pénal fédéral de Bellinzone**. Entre-temps, C. B., 48 ans, a quitté la banlieue bernoise où il vivait au moment des faits, pour retrouver sa région d'origine de Salerne, en Italie. Il réside depuis 2014 avec sa femme sur cette côte napolitaine. Se présentera-t-il à son procès mercredi prochain? L'homme est au bénéfice d'un saufconduit, comme l'indiquait le Tages-Anzeiger jeudi. Ce document, délivré par le tribunal, permet à un accusé résidant à l'étranger de se rendre librement à son procès en Suisse, sans risquer d'être arrêté. Selon son avocat, contacté par Le Temps, il a fait part de son intention de se présenter devant la cour, à Bellinzone. C. B. répond des chefs d'espionnage politique aggravé et de tentative de violation du secret de fonction. Des crimes passibles tous les deux de peines allant jusqu'à trois ans de prison au plus.

German intelligence agency reconsiders surveillance of right-wing 'Reichsbürger'
Deutsche Welle, 2016 11 19
Berlin - A month on since a so-called "Reichsbürger" fatally shot a policeman near the southwestern city of Nuremberg, **Germany's intelligence agency - the "Verfassungsschutz" - may be one step closer to tightening surveillance on the right-wing group**. This was the latest development on Saturday, according to information presented to the German Press Agency (DPA). In a reply to a question submitted by the Green party, the German Interior Ministry said it has asked Germany's intelligence agency to review its previous assessment of the Reichsbürger scene. The review has not yet been finalized, however. The Reichsbürger movement has gained greater attention since October, after one member in Nuremberg wounded three police officers and killed another in a shootout. Responding to the possibility of

stricter surveillance on Saturday, Green party politician Irene Mihalic told DPA: "This terrible event in Bavaria wasn't necessary to recognize that the Reichsbürger are a dangerous right-wing movement."

Sécurité du mégafichier : les sénateurs très inquiets
Le Figaro, Jean-Marc Leclerc, 2016 11 17
Paris - La **droite sénatoriale demande la suspension du décret visant à rassembler les données personnelles des Français**. Sous l'impulsion du président les Républicains de la commission des lois du Sénat, Philippe Bas, la droite sénatoriale a réclamé, ce mercredi, la « suspension » du décret de **Bernard Cazeneuve** visant à instaurer un mégafichier national d'identité. Ce décret avait été publié dans la torpeur des vacances de la Toussaint, le dimanche 30 octobre, sans même un débat préalable au Parlement. Le ministre de l'Intérieur l'a maintenu malgré une vive polémique, tout en acceptant finalement d'en débattre à l'Assemblée et au Sénat. Rappelons que ce **fichier TES (titres électroniques sécurisés)** ajoute au fichier des demandeurs de passeports celui des cartes d'identité. Il doit rassembler à terme les données personnelles et biométriques (identité, couleurs des yeux, domicile, photo, empreintes digitales...) de 60 millions de Français.

Germany alarmed about potential Russian interference in election: spy chief
Reuters, Staff report, 2016 11 16
Berlin - **Germany is alarmed that Russia may seek to interfere in its national elections next year, the domestic intelligence chief said**, echoing concerns raised in the United States before Donald Trump's presidential election victory. German officials have accused Moscow of trying to manipulate German media to fan popular angst over issues like the migrant crisis, weaken voter trust in moderate mainstream government under Chancellor Angela Merkel and breed divisions within the European Union so that it drops sanctions against Moscow. Intelligence officials have also pointed to Russian support for eurosceptic, anti-immigrant parties in Germany and across the EU. Last week, Merkel said she could not rule out Russia interfering in Germany's 2017 election through Internet attacks and misinformation campaigns. Hans-**Georg Maassen, head of the domestic BfV intelligence agency, cited the high-profile case last year of a German- Russian girl who Russian media said was kidnapped and raped by migrants in Berlin,** a claim later refuted by German authorities. "

Un ancien néonazi est nommé à la tête de la police ukrainienne
Le Figaro, Stéphane Siohan, 2016 11 16
Kiev - **Khatia Dekanoidze, une réformiste géorgienne, a démissionné et a aussitôt été remplacée par Vadim Troyan, un proche du ministre de l'Intérieur.** Un an après son arrivée à la tête de la police ukrainienne, Khatia Dekanoidze, 39 ans, a démissionné lundi de son poste en dénonçant la corruption et le blocage des réformes qu'elle avait engagées. En attendant la validation du cabinet des ministres, c'est son adjoint, Vadim Troyan, au profil extrême et inquiétant, qui va prendre la tête de la police, alors que cet ancien commandant du bataillon Azov a autrefois évolué dans la mouvance néonazie.

Fichier TES : la défense hasardeuse de Bernard Cazeneuve
L'Humanité, Aurélien Soucheyre, 2016 11 16
Paris - Après avoir oeuvré en catimini, **le gouvernement se retrouve sous le feu des projecteurs sur la question de ce gigantesque fichier qui compile les informations d'identité de 60 millions de Français.** Le ministre de l'Intérieur a tenté hier de minimiser les risques liés à ce projet. Sans convaincre. Bernard Cazeneuve est un bon défenseur. D'abord, le tacle glissé en douce, l'air de rien. Dimanche 30 octobre, paraissait dans le Journal officiel un décret signé de sa main prévoyant la création d'un gigantesque fichier informatique TES (titres

électroniques sécurisés) rassemblant les données personnelles et biométriques de plus de 60 millions de Français (l'Humanité du 3 novembre).

German court's ruling on mass spying is a victory for the BND and NSA
Deutsche Welle, Staff report, 2016 11 16
Berlin - In June 2013, media reports based on documents provided by whistleblower **Edward Snowden revealed the extent of global surveillance programs conducted by the US National Security Agency (NSA).** The leaks had a massive impact in Germany, especially after it was found that the **NSA was spying on European leaders and heads of government**, including German Chancellor Angela Merkel. The findings prompted the **"Bundesnachrichtendienst" (BND),** Germany's foreign spy agency, to deactivate around 40,000 of several million "selectors" - a collection of search parameters, including telephone numbers, keywords, URLs and addresses. On Tuesday, Germany's constitutional court ruled that the government was not obliged to transfer this secret list of selectors to a special parliamentary fact-finding commission on the NSA revelations. Tuesday's verdict proved to be a setback for politicians trying to get to the bottom of the BND's activities. "The ruling is a blow for any clarification on the activities of the BND and the NSA and for the entire parliamentary monitoring of secret services," Biselli told DW.

German domestic spy chief rejects Turkey's allegation it harbors PKK militants
Reuters, Staff report, 2016 11 15
Berlin - The **head of Germany's domestic spy agency on Tuesday rejected as "completely unjustified" Turkey's accusation that Germany is harboring militants tied to the banned Kurdistan Workers Party (PKK**). "That accusation is completely unjustified. We have been working for many years to ensure that the PKK in Germany poses no danger to Germany or Turkey," **Hans- Georg Maassen** told Reuters in an interview late on Tuesday. He said Germany had a good exchange of information with Turkey and that generally the countries worked well together on that issue. Turkish Foreign Minister Mevlut Cavusoglu on Tuesday said there were outstanding legal cases against 4,500 PKK members in Germany, but only three suspects had been sent back to Turkey so far. Asked if ties between the intelligence services of Germany and Turkey had deteriorated after Turkey's failed July 15 military coup, Maassen said only that cooperation was often difficult because of the different priorities set by the Turkish intelligence services.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Intelligence Minister: Enemies Unable to Distort Security in Iran
Fars News Agency, 2016 11 21
Tehran - **Iranian Intelligence Minister Seyed Mahmoud Alavi underlined that the country's armed and security forces are capable of safeguarding tranquility and security of the people**, and said the enemies are not able to harm Iran. "Thanks to Iran's skillful and professional security forces no anti-security agent dares to approach the Iranian borders," Alavi said on Friday. The Iranian intelligence minister underlined that security in Iran is higher than other regional countries and one of the highest in the entire world. In relevant remarks in July, Lieutenant Commander of the **IRGC Brigadier General Hossein Salami** underlined that Iran is the most secure country in the region.

Intelligence Minister: No anti-security agent dares to approach Iranian borders
Islamic Republic News Agency, 2016 11 18
Tehran - **Intelligence Minister Mahmoud Alavi said on Thursday that no anti-security agent dares to approach Iranian borders thanks to the skillful and professional security forces** of the country. He made the remarks in Shalamche border point in Khuzestan province southwest of Iran where he went to visit the process of Iranian pilgrims crossing the border into Iraq to attend the Arabaeen mourning ceremony in that country, IRNA reported.

Iran arrests 12 officials on spying charges (Canada).
Al Arabiya, Saleh Hamid, 2016 11 18
Dubai - **Iranian MP Hussein Ali Haji Degana has revealed that at least 12 top officials holding dual citizenship have been arrested in Iran on spying charges**. The MP added that among the 12 detained were officials who played key roles in the Iran nuclear deal signed last year. The MP demanded that the judiciary apparatus delivers its rulings with transparency, and that the officials' identity also be made public. Some of the officials who were arrested simply for holding dual citizenships.

Man Accused of Spying for Israel Referred to Judiciary
Naharnet Newsdesk, 2016 11 18
Beirut - A **Lebanese man was referred to the judiciary on Thursday on charges of spying for Israel,** the army said. "The **Intelligence Directorate** has referred Lebanese citizen Suheil Hussein Qaddoura to the relevant judicial authorities over his ties to the Israeli enemy," an army statement said. Qaddoura provided Israel with "information about the infrastructure in the Bekaa region," the statement added. Lebanese authorities had launched a national crackdown on Israeli espionage rings in 2009 which resulted in the arrest of more than 100 people. Lebanon and Israel remain technically in a state of war and convicted spies can face the death penalty.

Israeli accused of spying convicted of 'harassing' Romanian official
Jerusalem Post, Staff Report, 2016 11 17
Jerusalem - **Romania has sentenced an Israeli national accused of alleged espionage to a suspended prison term of two years and eight months on charges of harassing the country's anti-corruption czar**, according to local media. After pleading guilty to attempting to intimidate the director of Romania's National Anti-corruption Directorate, Laura Kovesi, a Bucharest court also ordered David Geclowicz to serve 80 days of community service. Geclowicz, an employee of the **private Israeli intelligence firm Black Cube**, allegedly admitted to targeting three people close to Kovesi, Romania's Agerpres reported.

Cyber concerns attract experts from around the world to Tel Aviv confab
The Jerusalem Post, Anna Ahronheim, 2016 11 16
Jerusalem—Thousands of top decision-makers, along with senior government and law enforcement officials from 80 countries, gathered in **Tel Aviv this week for the fourth International Homeland Security and Cyber Conference.** The conference, which runs November 14 to November 17 at Tel Aviv's Convention Center, focuses on the **ever-changing challenge of protecting data from the merging of physical and cyber crime**. Israel is a leader in cyber security. **Former chief of Shin Bet Yoram Cohen** talked about the large number of third-generation Muslim immigrant youths who did not integrate into European society and "underwent an identity crisis which caused them to become disenfranchised with the state."

Return to Table of Contents/ Retour à la table des matières

Asia / Asie

S. Korea, Japan to sign intel-sharing pact Wednesday
Yonhap News Agency, Staff reporter, 2016 11 21
Seoul - **South Korea and Japan plan to sign a military intelligence-sharing pact this week to better counter mounting threats from North Korea**, the defense ministry said Monday. The two countries signed a provisional General Security of Military Information Agreement (GSOMIA) last week, less than a month after they resumed discussions on Oct. 27. "We are planning to formally sign the GSOMIA on Wednesday upon approval by President Park Geun-hye after it is passed by the Cabinet on Tuesday," a ministry official said. Defense Minister Han Min-koo and Japanese Ambassador to Seoul Yasumasa Nagamine are expected to sign it at the defense ministry in Seoul, he said.

Centre, State joint mechanism to block conversion of terror funds
Daily Excelsior, 2016 11 18
Sanjeev— The **Government of India has set up high level joint team to unearth attempts to convert hawala money and terror funds into white by exchanging notes in the banks and in the process reach to the real sources of the funds in Jammu and Kashmir** especially the Kashmir valley. The decision followed a high level meeting chaired today by Union Home Minister Rajnath Singh in New Delhi with top **officials of the Ministry Research and Analysis Wing (RAW) Intelligence Bureau (IB) and other Intelligence agencies** exclusively on effectively blocking terror funding postdemonetization of big notes on November 8. Official sources told the Excelsior that top officials of Union Home Ministry Incharge Jammu and Kashmir desk Enforcement Directorate Finance Ministry etc would jointly monitor the postdemonetization impact on terror funding by staying in regular touch with Chief Secretary BR Sharma Director General of Police K Rajendra Kumar and Banking officials and taking inputs from the concerned agencies.

Our intelligence agency is similar to a militant group: Former spy
Indo-Asian News Service, 2016 11 18
New Delhi— He started off as a taxi driver, went on to become **a spy for an Indian intelligence** agency, spent 11 years in a Pakistan jail and is now running an association for the welfare of unsung heroes. Disappointed by the lack of support from the Indian government, **Vinod Sawhney says there is no difference between a militant organisation and India's intelligence agency**. Sawhney, now 66, was a taxi driver a few decades ago before an intelligence official boarded his taxi as a passenger. "He (the official) brainwashed me. He said it was a government job and spoke about patriotism. So, I got lured to become a spy without knowing my actual job."

Mossad, RAW cooperation deepens
The International News, 2016 11 17
Islamabad - **Indian intelligence and Israeli secret service are in alliance together with extensive military cooperation as** they take on extremist Muslims groups. RAW stands for **Research and Analysis Wing** is the intelligence gathering agency of the government of India like the CIA. This was set up in 1968 at the behest of the then Indian prime minister Indira Gandhi. Right from its inception, RAW realized the importance of cooperation with the Israeli secret service MOSSAD. Initial contacts were established through the Israeli consulate in Mumbai. Over the years the bonds between the two agencies have strengthened with a

common threat of Islamic terrorism and fundamentalism. **MOSSAD is one of the top spy agencies in the world and can rank as equivalent to the Soviet NKVD, German Gestapo, and the CIA**.

India and Israel reaffirm cooperation against terrorism and extremism
Times of India, Indrani Bagchi, 2016 11 16
New Delhi - **India and Israel reaffirmed their current cooperation against terrorism and extremism** as Israel president Reuvin Rivlin kicked off a week-long visit to India. After talks with Prime Minister Narendra Modi, Rivlin said, "Nothing can justify terror... Israel and India are threatened by terror because we uphold the values of freedom. We stand together in defending our people and values," Rivlin said. In his statement, Modi said, "We recognize that terrorism is a global challenge, knows no boundaries and has extensive links with other forms of organized crime. We agreed that the international community must act with resolve and determination against terror networks and States that harbour them. Failure to act and silence of speech only encourages the terrorists."

Return to Table of Contents/ Retour à la table des matières

Africa / Afrique

Des espions parmi nous
L'Expression (Algérie), Wahida Bahri, 2016 11 21
Alger - Les investigations se sont soldées par des interpellations et des mises en examen Ils se faisaient passer pour des membres de la **Commission nationale de lutte contre la corruption**. Les éléments de la brigade de recherche et d'investigation, relevant du groupement de la **Gendarmerie nationale ont démantelé un réseau national d'espionnage**, apprend-on de source judiciaire. Le pot aux roses a été découvert suite à l'arrestation de trois individus, accusés d'usurpation d'identité, escroquerie, faux et usage de faux et falsification de visas, ainsi que l'imitation des sceaux des ministères, dont la griffe du Premier ministre Abdelmalek Sellal, et espionnage pour le compte de parties étrangères, a rapporté la même source. Sont impliqués dans cette affaire, un greffier en chef du tribunal d'Oum El Bouaghi, en retraite qui se faisait passer pour le secrétaire général de la Commission nationale de lutte contre la corruption, un patriote AA. A et AA.K, son fils spécialisé dans la programmation informatique.

Changing the name of ministry of intelligence was a real stroke of genius by the government
Sunday World (South Africa), Vusi Nzapheza, 2016 11 20
There was a time when we had a **ministry of intelligence**. There were also ministries of housing and foreign affairs. Until some bored bureaucrat yawned and decided the names had to change. Where there was housing, we now have human settlements even though the mandate is still to build RDP houses. International relations has replaced foreign affairs despite the job remaining the same. **The one department whose name change I agree with is intelligence. No one can accuse State Security Minister David "Rhino Horn" Mahlobo of intelligence**. The one task he executed with aplomb was jamming the signal last year to prevent the broadcast of chaotic parliamentary proceedings. This week we learnt he also has cabinet's most perfectly manicured nails from frequent visits to a Chinese spa in Mbombela. The massage parlour was exposed in a TV documentary as the haven of self-confessed rhino poacher Guan Jiang Guang, who claims to be the minister's friend.

Return to Table of Contents/ Retour à la table des matières

Americas / Amériques

Senior Venezuelan Diplomat Detained Under Unclear Circumstances
Venezuelan Analysis, Lucas Koerner, 2016 11 18
Caracas— A leading Venezuelan diplomatic official has been taken into custody by authorities following a raid on his Caracas office last week. **Ricardo Moreno, North America director for the Venezuelan Foreign Ministry, was detained by agents of the National Bolivarian Intelligence Service (SEBIN)** on November 10. A resident in the United States for 20 years, Moreno is a widely respected Chavista activist with a long organizing track record in solidarity with the Bolivarian Revolution. As founder of the Los Angeles-based Simon Bolívar Association following the 2002 US-sponsored coup against the late former president Hugo Chávez, Moreno appeared widely in US Hispanic media debating with leading anti-Chavista figures, such as FEDECAMERAS President Carlos Fernandez and former US Under-Secretary of State Otto Reich.

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

30-11-2016 to/au 06-12-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Security shouldn't trump privacy, watchdogs to tell Trudeau government
Canadian Press, Jim Bronskill, 2016 12 06
Ottawa - **Privacy commissioners from across the country will tell the Trudeau government today to make respect for personal information a cornerstone of its revamped national security policy**. Federal privacy commissioner **Daniel Therrien** and all of his provincial and territorial counterparts are signing a joint submission to the government's security review. Therrien and privacy czars from two provinces _ Ontario's Brian Beamish and Jean Charter of Quebec _ will appear in Ottawa today to discuss the submission. Therrien's office says it will address key issues including information sharing, encryption and the collection and use of metadata by national security agencies and law enforcement. In October, Therrien told a House of Commons committee it is crucial that there be more transparency about national security so that Canadians can better understand the issues. The **Trudeau government has committed to ensure all CSIS warrants respect the Charter of Rights and Freedoms**, to preserve legitimate protest and advocacy and to define terrorist propaganda more clearly. The Liberals say they say will do a better job of balancing collective security with rights and freedoms. Just last month a Federal Court judge ruled that CSIS violated the law by keeping potentially revealing electronic data over a 10-year period about people who were not targets of investigation. CSIS processed the data beginning in 2006 through its **Operational Data Analysis Centre** to produce intelligence that can reveal specific details about individuals. The improperly retained material was metadata _ information associated with a communication, such as a telephone number or email address, but not the message itself.

Canadian security agencies 'consulting' with U.S. Homeland Security to vet Syrian refugees coming to Canada
The Hill Times, Abbas Rana, 2016 12 06
Ottawa—**Canadian security agencies responsible for vetting the thousands of Syrian refugees who have been arriving in Canada since late last year have been using a "robust" and "multi-layered" security check process that includes consulting U.S. Homeland Security databases**. "On the Syrian refugee decisions, we consulted with the Americans on everyone to make sure there was not somebody identified as a security risk," said **Gary Doer**, former Canadian ambassador to the U.S. from October 2009 to March 2016, at a panel discussion organized by The Literary Review of Canada, on its 25-year anniversary gala in Toronto on Oct. 13. "We had an agreement with Homeland Security and the United States, and a protocol of what we were going through. Asked for a comment last week, Public Safety and Emergency Preparedness Minister **Ralph Goodale's** (Wascana, Sask.) office referred The Hill Times to a press conference Mr. Goodale held in Ottawa last year held to explain the process of bringing in the Syrian refugees. Mr. Goodale told reporters the security mechanism used by Canadians to screen Syrian refugees was designed by the Departments of Immigration and Refugees Canada, the **Department of National Defence, the Canada Border Services Agency, CSIS and the RCMP.** He added that the security screening system included "checking against Canadian and U.S. databases." "It includes the identification of vulnerable applicants to come to Canada soon," Mr. Goodale said on Nov. 24, 2015, at the National Press Theatre.

Not Mounties' 'full-time job'
Toronto Star, Michelle Shephard and Mitch Potter, 2016 12 05

When a Canadian is kidnapped abroad, some **RCMP** officers go the distance and beyond, putting their families second to better serve a hostage's terrified relatives. They answer their phones any hour of the day and night, fly far away, provide comfort and assurance when they can. Then there are those who clock in and out. Families can call them after quitting time to flag sudden news about a hostage half a world away, but they learn not to expect a shared sense of urgency. The desperation will go to voice mail. Relatives of Canadian hostages who spoke with the Star for this series report varying experiences with the frontline Mounties who acted as **Family Liaison Officers (FLOs) - the crucial point of contact between the family and the government - and as investigating officers**. Some were astonished at the indifference they encountered as they scrambled to get answers. More than one relative said they were impatiently rebuffed with excuses along the lines of officers having "to get back to their full-time jobs."

Canada should appoint kidnapping czar as part of hostage approach, says ex-CSIS expert
CBC.CA, Lisa Laventure, 2016 12 03
Ottawa - **Canada should consider appointing a kidnapping "czar" and adopt a more standardized approach when Canadians are kidnapped abroad, says a former senior member of CSIS** who now heads up a private security firm. A permanent government point person directing efforts to free Canadians held for ransom would bring continuity to the federal government's approach to resolving hostage takings, said **Andy Ellis**, a former assistant director of operations at Canada's national intelligence agency. Ellis is currently doing pro bono work on two kidnapping cases involving Canadians. In an interview with CBC's Power & Politics Thursday, Ellis said the role would help streamline efforts between the departments responsible for responding to kidnappings. The government should also be prepared to turn to the private sector for input and assistance in kidnapping cases, he said. "As kidnapping becomes an industry, I think it requires an industrial response," Ellis told host Rosemary Barton. The recommendation comes after CBC's special report on the abductions and killings of Canadians Robert Hall and John Ridsdel in the Philippines by the militant group Abu Sayyaf.

New president of Canada Border Services Agency selected
Ottawa Citizen Online, Kathryn May, 2016 12 03
Ottawa - **Prime Minister Justin Trudeau has appointed a new president of the Canada Border Services Agency** in his latest shuffle of the top ranks of Canada's public service. **John Ossowski,** deputy commissioner of the Canada Revenue Agency, steps into the top job at the border agency with years of experience in security and safety. He was previously the associate deputy minister at **Public Safety** and also did stints in senior jobs handling security issues at Treasury Board and at the **Communications Security Establishment**. Ossowski's appointment comes on the heels of his predecessor at CBSA, **Linda Lizotte-MacPherson**, announcing her retirement.

Canada's hostage 'war room' is more like a leaderless boardroom
Toronto Star, Michelle Shephard and Mitch Potter, 2016 12 01
Toronto - **Canada's war room is more like a boardroom -- where a leaderless, interdepartmental committee of good people with good intentions meet and deal not only with kidnappers' demands but also with bureaucratic and political inertia**. Interviews with more than 50 people, including government and security officials, past and present, and former hostages and their relatives, reveal a range of obstacles, including lack of leadership, lack of continuity, unnecessary secrecy and political paralysis. Problems with Canada's approach were flagged eight years ago when Stephen Harper was prime minister and Ottawa was overwhelmed by five overseas abductions in five months: freelance journalist Amanda Lindhout

in Somalia; CBC reporter Mellissa Fung in Afghanistan; aspiring filmmaker Beverly Giesbrecht in Pakistan; and Canadian diplomats Robert Fowler and Louis Guay in Niger, where they were working for the United Nations. **John Proctor, who worked on the Canadian effort as a senior intelligence adviser with the Department of National Defence, confirmed that a comprehensive policy was ready to go when Parliament was prorogued in December 2009**. "There was a very serious effort to put together all the pieces -- and it died completely," Proctor, now a vice-president of global cybersecurity for the Ottawa-based firm CGI, told the Star. Bob Rae, former MP and lawyer, says if changes have been made, he hasn't seen them. The attacks of Sept. 11, 2001, proved a key turning point for Western governments grappling with abductions overseas, sparking a rise in the number of hostage-takings and the political risk. "What happened after 9/11 was that everybody's budgetary dollars became so focused on terrorism," says **Gary Noesner, who spent the last 10 years of his career as chief of the FBI Crisis Negotiation Unit** before retiring in 2003. "Everybody wanted a piece of pie. So now you had 20 cooks in the kitchen and nobody knew what anyone was making." Among the gaps in Canada's hostage response system, multiple sources told the Star, are a lack of support and expertise in handling the very specific and evolving challenge of overseas kidnapping. "I don't think it's resourced enough," says **Andy Ellis**, who retired this year as assistant director of operations at the **Canadian Security Intelligence Service**.

U.S.-style 'fusion cells' among recommendations for improving Canadian policy on hostages

CBC News, Lisa Laventure and Rosemary Barton, 2016 12 01

Ottawa—The **government is facing calls to review its approach to supporting families of Canadians kidnapped abroad and address alleged shortcomings in its response to the cases of two men abducted in the Philippines** in 2015. Among the recommendations is establishing a U.S.-style "fusion cell" that would improve co-ordination between government departments in the hopes of resolving hostage situations. "Every Western country is moving towards a fusion cell approach," says **Lee Humphrey**, a former Canadian soldier who now works as an international security consultant. He believes Canada hasn't done enough to adapt to an increase in international kidnappings. "Canada does not seem to get it, and perhaps it's because there's been no political blowback, but there is no emphasis on fixing [our approach to kidnappings], despite the numerous cases during the last few years of very public hostage takings of Canadians internationally." Humphrey says Canadian families have complained for years that the government lacks a cohesive strategy to support and communicate with relatives of kidnapped Canadians. The U.S. review resulted in a presidential directive and executive order. Announced in June 2015, it ensures that families would no longer be threatened with criminal prosecution if they attempted to pay ransoms to terrorist groups. The presidential directive also ordered the creation of a Hostage Recovery Fusion Cell, which is a specialized unit staffed by people from the departments of defence, state, justice and treasury, the FBI and the intelligence community with expertise in kidnapping. A **fusion cell** is meant to literally bring experts from each department together in the same room. Led by the FBI, the cell aims to better share information and improve how the government develops hostage recovery plans. Humphrey says Canada should strongly consider establishing a similar model. He says a **Canadian fusion cell should be led by the RCMP and would bring together experts from the departments of National Defence, Global Affairs, Justice and CSIS** to form a single, specialized hostage recovery team that would speak with one voice.

Inside the RCMP's plan for a 'new public narrative' on cyber surveillance

Vice News, Justin Ling, 2016 11 30

Toronto—A four-page memo obtained by VICE News sheds light on how the **Royal Canadian Mounted Police intends to lobby the public for new surveillance powers**. As the Trudeau

government contemplates new powers for the federal police force, the documents call for the RCMP to push for "the creation of a new public narrative around why police need judicially authorized and timely access to online information." The memo was prepared by the RCMP in advance of a February meeting in Washington, D.C., where Public Safety Minister Ralph Goodale sat down with his American, British, Australian, and New Zealand counterparts in the Five Eyes intelligence partnership. The previous Canadian government tried to sell to the public mandatory decryption powers and more expansive communication interception technology in Bill C-30, in 2012. Then-Public Safety Minister Vic Toews employed the euphemistic tagline of "lawful access," only to have that phrase pick up negative connotation as public opinion turned against many of those legislative proposals. The bill was later shelved and, ultimately, killed. The RCMP is not looking to make the same mistake. "It will be important for the Public Safety Portfolio to reframe 'lawful access' as broader 'going dark' digital evidence challenges," the February memo reads. The **Public Safety Portfolio includes everyone from Minister Ralph Goodale to the Canadian Security Intelligence Service and the Canadian Border Services Agency.**

Border plan comes up short
Toronto Star, Bruce Campion-Smith, 2016 11 30
Ottawa - A **high-profile strategy to ease the flow of travellers and trade to the United States and boost border security has had little impact, a new report** says. The **"Beyond the Border Action Plan"** was unveiled in December, 2011 to much fanfare to boost trade and eliminate border bottlenecks that had worsened due to heightened security in the wake of the 2001 terror attacks. But five years later, an audit of the initiatives launched by federal departments and agencies to implement the plan found little evidence that any of them had improved security or made life easier for travellers. "We concluded that the selected departments and agencies achieved limited results towards the objectives ... of enhancing security and accelerating the legitimate flow of travel and trade," says a report prepared by the auditor general. While the departments and agencies met the commitment laid out by the plan, "they faced many challenges in carrying out the initiatives and lacked performance indicators to assess results," said the report.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

Appeals Court to Examine Ex-CIA Officer's Leak Conviction
Associated Press, Staff report, 2016 12 06
Richmond, Va. - The **case of former CIA officer convicted of leaking classified details of an operation to thwart Iran's nuclear program is heading to a federal appeals court**. The 4th U.S. Circuit Court of Appeals will hear arguments in **Jeffrey Sterling's case** Tuesday. Sterling was sentenced to 3 1/2 years in prison after being convicted in 2015 of leaking details of a CIA mission to New York Times journalist James Risen. The leaked mission involved giving flawed nuclear blueprints to Iran in the hopes that they would spend years trying to develop a product that would never work. Sterling maintains that he wasn't Risen's source.

Obama to tout counterterror legacy, even as Trump threatens changes
CNN.com, Kevin Liptak, 2016 12 06
Washington - **President Barack Obama plans to provide a final summation of his national security record Tuesday, reaffirming his counterterrorism strategy** even as his successor

has threatened to reverse course on many of Obama's priorities. During a speech at MacDill Air Force Base, the Florida headquarters of US Central Command and Special Operations Command, Obama plans to again argue for closing the naval prison at Guantanamo Bay and maintaining a ban on torture -- both areas where President-elect Donald Trump says he'll change course. **Ben Rhodes, Obama's deputy national security adviser, told reporters Monday that Obama was not attempting to send a message directly to Trump through his speech**. But he said there would be important takeaways for the next commander-in-chief included in Obama's remarks..

Panel Backs Warrantless Collection of Email
New York Times, Charlie Savage, 2016 12 06
Washington - A **federal appeals court on Monday upheld the 2013 conviction of a Somali-American man for trying to detonate a bomb at a Christmas tree lighting ceremony in Portland**, Ore., rejecting his arguments that the F.**B.I. had entrapped him** and that the government had unconstitutionally intercepted his emails without a warrant. The ruling -- by a three-judge panel of the Court of Appeals for the Ninth Circuit, in San Francisco -- was particularly important because it upheld the government's use of emails gathered without a warrant under the **FISA Amendments Act** of 2008. The law permits the government, on domestic soil, to collect phone calls and emails of noncitizens abroad, even when they are communicating with an American. The case centered on Mohamed Mohamud, who was 19 when he tried to blow up what he thought was a bomb.

Security Adviser and Son Share Penchant for Spreading False Stories About Clinton
New York Times, Matthew Rosenberg, 2016 12 06
Washington - For **Lt. Gen. Michael T. Flynn**, who is President-elect Donald J. Trump's choice for national security adviser, **pushing conspiracy theories about Hillary Clinton is a family affair: Both he and his son, Michael G. Flynn, have used social media to spread fake news stories linking Mrs. Clinton to underage sex rings and other serious crimes, backed by no evidence.** The Twitter habits of both men are attracting renewed attention after a man fired a rifle on Sunday inside Comet Ping Pong, a Washington pizza restaurant that was the subject of false stories during the campaign tying it and the Clinton campaign to a child sex trafficking ring. Well before he joined the Trump campaign, the elder Mr. Flynn, 57, a former director of the **Defense Intelligence Agency**, pushed unsubstantiated claims about Islamic law's spreading in the United States and about the attack on the American diplomatic compound in Benghazi, Libya. But in his emergence this year as the angry former general out to help Mr. Trump clean up Washington, Mr. Flynn added wild stories about Hillary Clinton to his stock of unproven tales.

Obama Has a Plan to Fix Cybersecurity, But Its Success Depends on Trump
Wired (US), Andy Greenberg, 2016 12 05
New York - The **Obama White House has had to reckon with cybersecurity like no other presidential administration in history**, from China's 2009 hack of Google, to the Office of Personnel Management breach, to the rise of botnets built from dangerously insecure "internet-of-things" devices. Now, in the waning days of Obama's presidency, **his team has a new plan to shore up America's protections from digital threats. Whether any of it happens, though, is up to Donald Trump**. Late Friday afternoon last week, the White House's Commission on Enhancing National Cybersecurity released the results of a nine-month study of America's cybersecurity problems. Its recommendations, in a hundred-page report, cover a lot of ground. It proposes fixing the shambolic security of internet-of-things consumer devices like routers and webcams, re-organizing responsibility for the cybersecurity of federal agencies, and fostering a new generation of skilled American cybersecurity experts, among other actionable

steps. But as President Obama acknowledged in a statement accompanying those recommendations, actualizing them is largely out of his hands. He asked the cybersecurity commission to brief President-elect Trump's transition team on its work as soon as possible.

Face-to-face with Edward Snowden in Moscow on Trump, Putin and dwindling hopes of a presidential pardon
Yahoo News, Michael Isikoff, 2016 12 05
Washington - **In an exclusive interview in Russia with Yahoo Global News Anchor Katie Couric, Edward Snowden**, the fugitive whistleblower who leaked information about U.S. surveillance activities, **says he is "kind of encouraged" by the idea that Russian President Vladimir Putin might return him to the U.S. to stand trial because that would show the world he's not a spy and Russia "doesn't own me."** But he also acknowledged he isn't eager to return home to face U.S. justice, saying such a prospect "would be a threat to my liberty and to my life." Speaking for 90 minutes in a Moscow hotel room, Snowden -- calm and completely unrepentant -- also took new swipes at top U.S. intelligence officials, claiming they have accused him of damaging national security only because they were "embarrassed" by his disclosures of classified **National Security Agency** documents and worried about their "reputations." Those comments drew an angry rebuke Sunday from the Obama administration's former top counterterrorism official. "Snowden is delusional," said **Matt Olsen, the former director of the National Counterterrorism Center**, when read excerpts of the interview. "It wasn't so many years ago that people were saying, 'This guy's a Russian spy,'" said Snowden when asked by Couric how "nervous" he was about the possibility of losing his Russian sanctuary and being sent home to face criminal charges of theft of government property and violations of the Espionage Act.

Into the dark world of espionage
The Jerusalem Post, Geroge Medovoy, 2016 12 03
Washington— The shiny green Jaguar XKR greeted me in the lobby of the **International Spy Museum,** which is housed in a restored 19th-century building in downtown Washington. The prized car, driven by the villain of the 2002 James Bond movie Die Another Day, looked as striking as it did in the film, but it had a new role now: building curiosity about the dark world of espionage. As the greeting on the lobby wall announced: For your eyes only. Entry beyond this point is on a need-toknow basis. Who needs to know? All who would understand the world, all who would glimpse the unseen hands that touch our lives...." Within the museum is a **large collection of international espionage artifacts**, and there are special exhibits, too, like Exquisitely Evil: 50 Years of Bond Villains," which was on display during my visit. Also among the museum's offerings are spy workshops like Surveillance 201," a scenario in which participants look for secrets, and a summer spy camp" for children that ends with a mission-accomplished cake." The **museum's advisory board is composed of real-life espionage veterans** like Oleg Danilovich Kalugin, who was a major-general in the 1st Chief Directorate of the KGB, where he conducted espionage as a Radio Moscow correspondent with the United Nations, and R. James Woolsey, Jr., the former director of the Central Intelligence Agency.

James Mattis, Trump's Choice for Defense, Favors Working With Allies
New York Times, Helene Cooper & Eric Schmitt, 2016 12 03
Washington - President-elect **Donald J. Trump's selection of Gen. James N. Mattis as defense secretary signals a more assertive American posture in the Middle East** -- one that people close to him say would most likely include more American troops on the ground in Iraq and Afghanistan, more Navy patrols in the Persian Gulf and more fighter jets in the Middle East. "The closest thing we have to Gen. George Patton," Mr. Trump said in announcing his selection on Thursday night. At first glance, the similarity is there: Like General Mattis, General

Patton, who led American troops into Nazi Germany during World War II, was a colorful, hard-charging advocate of aggressive offensive action. But officials who know General Mattis caution that he views a tough American posture overseas as something to deter war with potential foes like Iran, not to start one. And although he was so hawkish on Iran as head of United States Central Command from 2010 to 2013 that the Obama administration cut short his tour, General Mattis has since said that tearing up the Iran nuclear agreement, as Mr. Trump has vowed to do, would hurt the United States. General Mattis now favors working closely with allies to strictly enforce the deal.

U.S. Bars Chinese Deal for Tech Firm
Wall Street Journal, William Mauldin, 2016 12 03
Washington - **President Barack Obama took the rare step of forbidding a foreign company from buying a firm with U.S. assets**, telling a **Chinese investment fund** that it cannot complete a deal for German technology company **Aixtron SE**. Mr. Obama's move, only his second outright ban on a foreign acquisition, shows the increasing suspicion the U**.S. harbors toward Chinese acquisitions of certain U.S. firms,** even before the arrival of President-elect Donald Trump, who made criticism of Beijing a cornerstone of his campaign. The Treasury Department on Friday said Mr. Obama had issued an order barring **Fujian Grand Chip Investment Fund LP, part-owned by the Chinese government,** from buying Aixtron. The ban follows a recommendation from the Committee on Foreign Investment in the U.S., or CFIUS, which confidentially reviews foreign acquisitions solely on national-security grounds.

US spy agencies fight Congress over plan for probe of covert Russian influence campaign
Reuters, Mark Hosenball and Jonathan Landay, 2016 12 03
Washington - The **top U.S. intelligence officer has asked Congress to drop a provision in a pending bill that would create a special committee to combat Russian efforts to exert covert influence abroad,** saying such a panel would duplicate current work and hinder cooperation with foreign allies. **Director of National Intelligence James Clapper** laid out the objections of the U.S. intelligence community in a Sept. 9 letter to the chairmen and top Democrats on the House of Representatives and Senate intelligence committees. He charged that parts of the bill amounted to "micromanagement" of the intelligence community. The intelligence bill, an annual measure that provides broad Congressional authorization for a wide range of U.S. intelligence activities and agencies, has already been approved by both intelligence committees and the House of Representatives.

Diplomacy in the Age of Covert Surveillance --- Robin Raphel was a Pakistan expert -- the FBI thought she was a spy
Wall Street Journal, Adam Entous and Devlin Barrett, 2016 12 03
Washington - Just before 8 on the morning of Oct. 21, 2014, **Robin Raphel** climbed into her Ford Focus, put her purple briefcase on the passenger's seat and began the 20-minute drive from her house in Washington to her office at the **State Department**. It was a routine Tuesday. The main event on her schedule was a staff meeting. Raphel swiped her badge at the revolving security door. Later, as she joined her colleagues in a conference room to discuss office schedules, her mobile phone, which she had left at her desk, began to ring. It was Slomin's Home Security. When she didn't pick up, the operator called her daughter Alexandra, who raced to the house to check the doors and windows. When Raphel returned, the phone rang again. It was Alexandra, in a panic. Burglars hadn't set off the alarm. It was the **Federal Bureau of Investigation**. Raphel grabbed her purse and ran out. As she pulled up to her house, she saw agents going in and out, walking across the oriental rugs she had trundled back from South Asia. They boxed up everything electronic. In the basement, they opened the drawers of a

mahogany file cabinet. They pulled out a stack of files. Two FBI agents approached her, their faces stony. "Do you know any foreigners?" they asked. Raphel's jaw dropped. She had served as a diplomat in six capitals on four continents. She had been an ambassador. Knowing foreigners had been her job. "Of course," she responded, "Tons . . . Hundreds." Three weeks before the FBI raided her house, Raphel had touched down at Benazir Bhutto International Airport in Islamabad. The city was in an anxious state. All summer, **U.S. intelligence agencies had been intercepting rumors about a possible coup.** Alarm bells were ringing in the State Department's office of the Special Representative for Afghanistan and Pakistan, where Raphel worked, and went all the way to the White House. At a dinner party at the home of an American diplomat in Islamabad's elite E-7 sector, Raphel and a group of Pakistani politicians pulled their seats into a circle.

U.S. to Delay NATO Center
Wall Street Journal, Julian Barnes, 2016 12 02
Brussels - The U.**S. Congress is ready to approve legislation aimed at delaying the relocation ofa North Atlantic Treaty Organization intelligence center**, possibly providing the incoming Trump administration with leverage to prod the alliance into expanding its counterterrorism work. President-elect Donald Trump has said he wants NATO to focus more on fighting terrorism, a shift many allies oppose as either outside the alliance's remit or as a distraction from its traditional focus on countering Russia. The final version of the Defense Authorization Act, set for a vote by the Houseon Friday and the Senate next week, blocks any funds from being spent to move the so-called **NATO Intelligence Fusion Cell from the Molesworth Royal Air Force base, in central England, to the Croughton base, about 50 miles southwest**.

Bill to help ID threats, challenges at northern border heads to Obama's desk (Canada)
Dickinson Press (North Dakota), April Baumgarten, 2016 12 01
Washington - A **bill U.S. lawmakers hope will help identify threats and challenges facing federal agents at the northern border is going to President Barack Obama's desk**. The House of Representatives unanimously passed the **Northern Border Security Review Act** on Tuesday without objection, meaning there were no changes to the bill. Obama has 10 days from when the bill was passed by Congress to decide whether he will sign the bill into law, but Sen. Heidi Heitkamp, D-N.D., expects the president will put his signature on the document. "This bill will give us an excellent opportunity to have a strategy that we all can evaluate and review in our oversight responsibilities," she said. She added the U.**S. is lucky to have Canada as a friendly, trusted ally**. There are Canadian border officials at the Pembina port aiding Border Patrol agents, and there could be a bill to further facilitate relationships with border forces from Canada.

Bill to combat foreign propaganda advances in Congress
Washington Post, Craig Timberg, 2016 12 01
Washington - **Congressional negotiators on Wednesday approved an initiative to track and combat foreign propaganda amid growing concerns that Russian efforts to spread "fake news" and disinformation threaten U.S. national security**. The measure, part of the National Defense Authorization Act approved by a conference committee, calls on the State Department to lead governmentwide efforts to identify propaganda and counter its effects. The authorization is for $160 million over two years. If approved by the full House and Senate, the measure could reach President Obama in December.

Michael Flynn, a Top Trump Adviser, Ties China and North Korea to Jihadists
New York Times, Edward Wong, 2016 12 01

Analysis - **President-elect Donald J. Trump's pick for national security adviser, retired Lt. Gen. Michael T. Flynn, has been much more outspoken about militant Islamists than he has about China and North Korea, the two main strategic concerns of the United States in Asia**. That has left scholars and analysts looking for clues about his views on Asia. A book published in July for which he was a co-author, "The Field of Fight: How We Can Win the Global War Against Radical Islam and Its Allies," offers some tea leaves. The **half-dozen mentions of China and North Korea are couched in generalities**, but there are glimpses into what the general thinks of the two nations. General Flynn wrote that the United States needed to confront a global "alliance" between "radical Islamists" and the governments of China and North Korea, as well as Russia. China and North Korea are officially secular Communist states, and China has blamed religious extremists for violence in Muslim areas of its Xinjiang region. In the book, General Flynn acknowledges that people may find the idea of an alliance between the Communist nations and jihadists to be strange, but asserts that it exists. He does not go into details on the alliance. **By appointing General Flynn, a former Army intelligence officer, Mr. Trump has signaled that he intends to prioritize policy on the Middle East and jihadist groups,** though the Obama administration seems to have stressed to Mr. Trump the urgency of dealing with North Korea's nuclear program.

Just one Trump transition aide for U.S. spy agencies - officials
Reuters, Jonathan Landy, Mark Hosenball, 2016 12 01
Washington - **Only one member of President-elect Donald Trump's transition team is dealing with the CIA and the 16 other offices and agencies that make up the U.S. intelligence community**, four U.S. officials said Wednesday. Geoffrey Kahn, a former House intelligence committee staffer, is the only person named so far to Trump's intelligence community "landing team," they said. As a result, said one senior career intelligence officer, briefing books prepared by the **Office of the Director of National Intelligence, the National Security Agency, the National Counterterrorism Center, and 13 other agencies** and organizations are "waiting for someone to read them." "It seems like an odd time to put issues like cyber security and international terrorism on the back burner," said the official, who spoke on the condition of anonymity. Trump on Tuesday received only his third intelligence briefing since he won the Nov. 8 presidential election, despite an offer from President Barack Obama of daily briefings, three of the officials said.

FBI to gain expanded hacking powers as Senate effort to block fails
Reuters, Staff report, 2016 11 30
Washington - A **last-ditch effort in the Senate to block or delay rule changes that would expand the U.S. government's hacking powers failed** Wednesday, despite concerns the changes would jeopardize the privacy rights of innocent Americans and risk possible abuse by the incoming administration of President-elect Donald Trump. Democratic Senator Ron Wyden attempted three times to delay the changes which, will take effect on Thursday and allow U.S. judges will be able to **issue search warrants that give the FBI the authority to remotely access computers in any jurisdiction, potentially even overseas**. His efforts were blocked by Senator John Cornyn of Texas, the Senate's second-ranking Republican. The changes will allow judges to issue warrants in cases when a suspect uses anonymizing technology to conceal the location of his or her computer or for an investigation into a network of hacked or infected computers, such as a botnet. In an effort to address concerns, U.S. Assistant Attorney General Leslie Caldwell wrote a blog post this week arguing that the benefits given to authorities from the rule changes outweighed any potential for "unintended harm."

Internet Archive looks to take digital collection to Canada
ZD Net (US), Jonathan Chadwick, 2016 11 30

San Francisco - **The Internet Archive is looking to replicate its database in Canada in the face of potentially increased surveillance powers under a Donald Trump presidency in the United States.** The San Francisco- based organisation said in a blog post that it is seeking donations for an "**Internet Archive of Canada**", which had been set as a goal in response to the November 9 election result and the greater web restrictions that will likely follow. "[The election result] was a firm reminder that institutions like ours, built for the long term, need to design for change," the post says. "For us, it means keeping our cultural materials safe, private, and perpetually accessible. It means preparing for a web that may face greater restrictions ... government surveillance is not going away; indeed, it looks like it will increase." Despite Internet Archive looking to back up its data in Canada, one Snowden document revealed the close collaboration between the NSA and the country's **Communications Security Establishment Canada (CSEC).**

CIA's Brennan says tearing up Iran deal would be 'folly'
Reuters, Staff report, 2016 11 30
Washington - **Outgoing CIA Director John Brennan has said it would be the "height of folly" for U.S. President-elect Donald Trump to tear up Washington's deal with Tehran because it would make it more likely that Iran and others would acquire nuclear weapons**. "It could lead to a weapons program inside of Iran that could lead other states in the region to embark on their own programs," Brennan said in an interview with the BBC aired on Wednesday. "So I think it would be the height of folly if the next administration were to tear up that agreement." Brennan also said that in dealing with the Syrian crisis, Trump should be cautious in trying to work with Russia.

Elite U.S. Special Operators Build Center for Perpetual War on Terror
The Daily Beast, Kimberly Dozier, 2016 11 29
Washington - **Preparing for a multi-generational, international fight against terrorists, U.S. special operations chiefs are launching a new counterterrorist nerve center at an undisclosed location in the Middle East to fight the so-called Islamic State, al Qaeda, and any other terrorist actor.** The **Joint Special Operations Command**, the U.S. military's premier counterterrorist strike force, is expanding its existing targeting nerve center in the region to make space for more American terror hunting personnel from three-letter agencies like the **CIA, NSA, and FBI to foreign partners like Britain, France, Iraq and Jordan**. The Obama administration is enshrining the strike force's role of gathering multiple points of view on who to kill and capture, as it did in Iraq and Afghanistan into a permanent information sharing platform, two U.S. officials tell The Daily Beast, speaking anonymously because they were not authorized to discuss the secret task force publicly. "This has been going on," said a senior U.S. official briefed on the expanded mission. "We're just putting it on steroids."

FBI may have also been investigating Trump
VICE News, Jason Leopold, 2016 11 29
Washington - **Eleven days before the election, FBI director James Comey wrote a letter to Congress letting them know that the agency had found additional emails that "appear to be pertinent" to the bureau's investigation of Hillary Clinton's private email server**. Now, three weeks after the election, the **FBI has responded to a longstanding VICE News Freedom of Information Act lawsuit, revealing that the bureau may very well have been investigating Donald Trump as well.** In September, VICE News and Ryan Shapiro, a doctoral candidate at MIT and research affiliate at the Berkman Klein Center for Internet & Society at Harvard University, filed the lawsuit against the FBI demanding documents connected to a pair of incendiary comments Trump made on the campaign trail over the summer. In July, he called upon Russia to track down "30,000 emails [from Hillary Clinton's private email server] that are

missing." We asked the FBI to grant us expedited processing because there was an urgent need to inform the public before they went to the polls on November 8. But the FBI refused to respond to our request before the election. "The nature of your request implicates investigative records the FBI may or may not compile pursuant to its broad criminal and national security investigative missions and functions," said the bureau's response, which is embedded at the end of this story. **"Accordingly, the FBI cannot confirm or deny the existence of any such records about your subject as the mere acknowledgment of such records existence or nonexistence would in and of itself trigger foreseeable harm to agency interests."**

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

British anti-terror advisers sent to Gulf
London Daily Telegraph, Laura Hughes, 2016 12 06
London - **Britain will spend millions helping Middle East countries beef up security at their airports to help detect terrorists**, Theresa May will pledge as she says, "Gulf security is our security". At a meeting of the **Gulf Cooperation Council (GCC)** in Bahrain, Mrs May will announce plans for a joint taskforce to increase counter terrorism financing and training in the region. British experts will help improve traveller screening systems at airports in the Middle East, in light of growing fears of Isil plots targeted at airlines. Mrs May will today become the first British Prime Minister - and the first woman - to attend the annual gathering. She will announce a series of additional security measures, including the establishment of a new joint **UKGCC Working Group on Counter-Terrorism and Border Security**.

Former spy sues after MI5 'hid' his stress disorder
Sunday Times (UK), Sean Rayment, 2016 12 04
London - A **former MI5 agent who developed post traumatic stress disorder (PTSD) after infiltrating al-Qaeda is suing the British government for £1m**, The Sunday Times can reveal. The **former agent, who cannot be identified for security reasons, is now serving life for a murder he claims was committed as a direct result of his mental condition**. He has told The Sunday Times that after years of therapy he now believes the crime would never have been committed if he had received treatment for the illness. Legal papers have been served on MI5. The former agent's lawyers are in negotiations with Treasury solicitors, who are acting on behalf of the security service. He has told The Sunday Times that he spied for both **MI5 and MI6**, undertaking missions in Britain, Pakistan and Egypt.Targets included members of his local community, university students, worshippers at his mosque and British jihadists attempting to join al-Qaeda. He claims MI6 medical files reveal that he developed the illness after witnessing the beheading of a family in Pakistan.

Our spies need to be better molecatchers
London Times, Ben Macintyre, 2016 12 03
Column: The **German equivalent of a mole in spy jargon is U- boot: an unidentified threat lurking just below the surface, unseen, silent and lethal**. This week, Germany's domestic intelligence agency discovered a U-boat in its midst that has already inflicted huge reputational damage -- an Islamist convert who infiltrated the agency to gather secrets and alert his "religious brothers" to impending danger, and who may have been planning an attack on its headquarters. Unbeknown to them the mole, a married father of four, had acted in gay pornographic films and secretly converted to Islam in 2014. A proper vetting procedure would

have brought this to light and set off every alarm bell. Instead, the German authorities admitted, he remained "inconspicuous during the application process, training and at work". The **case has prompted much sniggering but before we indulge in schadenfreude it is worth recalling that Britain has suffered the worst mole infestation of any western power**. We have been penetrated like this before, we may well be penetrated now, and we may not discover it for years. The mole, U-boat, or "sleeper agent" is every spy agency's nightmare: the spy who makes himself eligible for employment by his foe's intelligence service, lies low, and then destroys the machine from within by passing on its secrets, warning its targets, and betraying its agents. The most successful moles in history were the Cambridge spies of the 1930s, the communist converts working for the **KGB who infiltrated MI5, MI6 and** the Foreign Office. Britain used the same techniques to undermine German intelligence during the Second World War.

UK security officials to discuss Iran nuclear deal with Donald Trump's camp
The Independent (UK), Joe Watts, 2016 12 01
London - **British security officials are set to discuss the Iran nuclear deal with Donald Trump's advisors after the President-elect signalled he would "tear up" the agreement**. Downing Street said the UK placed a great deal of importance on the pact and had put "substantial diplomatic effort" into securing it. It comes after the director of the **CIA** issued a stark warning against dumping the deal, something Mr Trump has pledged, claiming it would be "the height of folly" and "disastrous". A Downing Street spokesperson said: "Most Americans know what our position is on the Iran deal given that we've played such a part securing that agreement.

All western spy agencies , including MI5 , are vulnerable to infiltration by Islamists . Here's why
London Daily Telegraph, Nigel West, 2016 11 30
Column - The **news that the German security service BfV may have been penetrated by an Islamic terrorist organization will come as no surprise to western counter-intelligence analysts**. In fact it will serve only as an unpleasant reminder of the vulnerability of such agencies when entrance and vetting standards are compromised in an effort to acquire language skills. At the heart of the **continuing challenge of countering so- called "hostile penetration"** is the balance that has to be struck in the acquisition of intelligence staff with foreign dialects - which are essential if a security apparatus is to monitor the communications of terror suspects speaking in their own patois, or to maintain physical and technical surveillance on extremists from the Middle East. Such language skills are of supreme importance when it comes to interrogation, where an interviewee's every nuance may be significant, and must be recognised for what it is. However, in the rush to embrace native-speaking interpreters and even case officers, many Western security services have reduced their standards and limited their background screening of candidates. Combined with the new policy of open recruitment, which amounts to an invitation to terrorist groups to try their luck, the problem of bad apples has been exacerbated. Most **security authorities acknowledge the problem - which was graphically illustrated by Nada Prouty, who infiltrated the FBI and then the CIA**. She was convicted in November 2007 of gaining illegal access to the files of both American agencies, but the subsequent investigation showed that she should never have been given a job in the first place. She had succeeded because of a desperate shortage of language skills, and ended up in Iraq as an interrogator. Note: Nigel West is the author of Tradecraft Secrets.

'Snooper's charter' bill becomes law, extending UK state surveillance
The Guardian (London), Alan Travis, 2016 11 29

London - The **"snooper's charter" bill extending the reach of state surveillance in Britain was given royal assent and became law on Tuesday** as signatures on a petition calling for it to be repealed passed the 130,000 mark. The home secretary, Amber Rudd, hailed the Investigatory Powers Act 2016 as "world-leading legislation" that provided "unprecedented transparency and substantial privacy protection". But privacy campaigners claimed that it would provide an international standard to authoritarian regimes around the world to justify their own intrusive surveillance powers. The new surveillance law requires web and phone companies to store everyone's web browsing histories for 12 months and give the police, security services and official agencies unprecedented access to the data.

Return to Table of Contents/ Retour à la table des matières

Australia / Australie

'A national security risk': Australian Border Force warns illegal tobacco trade may be fuelling terrorism
ABC (Australia), Nick McKenzie, 2016 12 05
Canberra - **Senior border security officials warn that illegal tobacco smuggling may be fuelling drug trafficking and terrorism fundraising**. Australians may not equate illegal tobacco smuggling with drug trafficking or terrorism fundraising, but senior border security officials are warning it may be fuelling both and posing a national security risk. In an exclusive interview with the ABC's 7.30 program and Fairfax Media, Australian Federal Police assistant commissioner Wayne Buchhorn -- who has been seconded to **Australian Border Force (ABF)** -- said he had "significant" concerns that some of the proceeds of the booming illicit tobacco smuggling trade into Australia were flowing to extremist groups overseas. "We are seeing crime gangs here in Australia, oftentimes Middle Eastern organised crime gangs, and the connections back into the Middle East ... [are] a significant concern for us in the current environment," he said.

Australia introduces new laws to keep terrorists in jail
Australian Associated Press, Claire Bickers, 2016 12 02
Canberra - **New counter-terrorism laws will allow the Federal Government to keep convicted terrorists in jail once their sentence expires if they are still deemed a threat**. The laws passed yesterday evening on the final sitting day of 2016. Several amendments were made to the original proposal to improve safeguards and oversight following recommendations by a parliamentary committee. "The scheme is a necessary response to the serious threat that terrorism poses to Australia and its people," Justice Minister Michael Keenan told MPs. It was the third **national security Bill** to pass in the final sitting fortnight of the year. Malcolm Turnbull announced the new measures in July, shortly after terror attacks in Nice. At the time, the Prime Minister said Australia could not be complacent in the wake of increasing terror attacks around the world.

ASIO boosts ranks with spies like us
Daily Telegraph (Australia), Charles Miranda, 2016 12 01
Melbourne - The **ranks of Australia's domestic intelligence agents have spiked to their biggest level in history and many of the new recruits are spies like us, with ASIO specifically targeting tradies.** The spy agency has confirmed it has hit a milestone in personnel numbers with a focus specifically on the recruitment this year of surveillance agents

for the ever present threat of terrorism but also to combat an alarming rise in "espionage and foreign interference by clandestine actors" in Australia. **ASIO now has 1800 personnel many of whom are tasked with combating terror but also a noted increased incursion of foreign agents** targeting the private and government sector's critical infrastructure, in the latter case notably the defence, intelligence and science industries. As the Telegraph exclusively revealed in February, it has been confirmed many of those recruited are ordinary citizens including lawyers, accountants and IT gurus but also surprisingly tradies. ASIO has specifically targeted tradies including electrical, mechanical, lock-smithing and building services to convert them into surveillance officers with "several thousand" trade- related applications from all over Australia received.

Federal Government's new counter-terrorism measures pass the Senate
ABC (Australia), Henry Belot, 2016 12 01
Canberra - The **Federal Government passes new counter-terrorism measures allowing convicted terrorists to be kept in jail once their sentences expire, should they be deemed a risk to society.** The Federal Government has passed new counter-terrorism measures allowing convicted terrorists to be kept in jail once their sentences expire, should they be deemed a risk to society. Prime Minister after high-profile terror attacks in Orlando, Nice and Paris. The legislation allows Attorney-General George Brandis to be able to apply for an extension 12 months before a sentence expires, rather than six months as originally proposed.

Return to Table of Contents/ Retour à la table des matières

New Zealand / Nouvelle-Zélande

The director of the Government Communications and Security Bureau says the level and complexity of cyber threats to New Zealand organisations is increasing.
Radio New Zealand News, Staff reporter, 2016 12 06
Wellington - The **director of the Government Communications and Security Bureau says the level and complexity of cyber threats to New Zealand organisations is increasing**. The Intelligence and Security Committee held its annual review of the GCSB and the Security Intelligence Service in Parliament today. In the last year, there have been 338 cyber threat incidents, compared with 190 in the previous year. The **GCSB's director, Andrew Hampton**, says New Zealand is being targeted by a growing range of international threats for financial gain. (Full report)

New Zealand Surprised as Prime Minister John Key Stands Down (Canada)
Wall Street Journal, Rhiannon Hoyle and Rachel Pannett, 2016 12 05
Sydney - **New Zealand Prime Minister John Key said Monday he would step down**, likely ending the political career of one Asia-Pacific's longest- serving conservative leaders and a key U.S. ally in the region. Mr. Key's support also held steady **amid allegations by former U.S. intelligence employee Edward Snowden that the government engaged in mass surveillance of its citizens**, a charge Mr. Key has strongly denied. **New Zealand is also part of the Five Eyes intelligence alliance with Australia, Canada, Britain and the U.S. Under the alliance**, the five countries have committed to sharing intelligence. Mr. Key said he would leave parliament before the next election. He has no immediate plans, although he said he would likely be interested in board positions in Australia and New Zealand, as well as across Asia and the U.S.

Kim Dotcom wants to know - is he being spied on again?
New Zealand Herald, David Fisher, 2016 12 04
Wellington - **Kim Dotcom wants to know - is he being spied on again?** The question came after the discovery of a surveillance camera in the penthouse suite of the Hilton on Auckland's Princes Wharf. And it turns out the answer might be "yes". The camera belongs to NZ Customs and is being used by the **NZ Defence Force** - although both agencies say any surveillance of Dotcom's home was accidental. The latest instalment in Dotcom's complicated relationship with New Zealand **government agencies** came one evening last month as the former Megaupload owner was looking across from his penthouse apartment towards the neighbouring Hilton.

The Commissioner of Security Warrants says he rejects very few warrants sought by the government's intelligence agencies, but some have to be 'tweaked' to comply with the law
Radio New Zealand News, Staff reporter, 2016 12 01
Wellington - The **Commissioner of Security Warrants says he rejects very few warrants sought by the government's intelligence agencies**, but some have to be 'tweaked' to comply with the law. The Commissioner, **Bruce Robertson**, and the Prime Minister jointly issue interception warrants for New Zealand residents or citizens. Mr Robertson appeared before a parliamentary committee considering a new law to set up the same warranting and compliance regime for both agencies. He told MPs the the Government Communications Security Bureau and the Security Intelligence Service know which warrants will get his sign-off.

Return to Table of Contents/ Retour à la table des matières

International

China / Chine

Xi calls for downsized military
Global Times, Deng Xiaoci, 2016 12 05
Beijing - **President Xi Jinping on Saturday called for a smaller military with better combat capability and optimized structure, a step further, experts said, toward mobilizing senior officers to conduct grass- roots military reform** after it was regrouped into five theater commands in February. Citing rapid changes to the global military environment, Xi, who is also chairman of the Central Military Commission and head of a leading group for deepening reform on national defense and the armed forces, spoke about the modern informationized warfare, noting that joint operations have grown to be the basic form of combat, reported the Xinhua News Agency. The president said at a two-day conference on military reform, which ended Saturday, that the military's structure must be adjusted and optimized, new types of forces developed, the ratios between different types of forces should be rationalized, and the number and the scale of the military should be downsized.

China takes censorship to sophisticated new level
Globe and Mail, Nathan Vanderklippe, 2016 12 01
Beijing - **China appears to have massively upgraded its powerful online censorship apparatus, using it to more severely block sensitive topics in group conversations while allowing freer rein in private chats** - a sign, one expert says, of a dramatic leap in the use of artificial intelligence to silence speech that falls afoul of the Communist Party. The growing sophistication of China's Internet blocking, uncovered by researchers at the University of

Toronto, offers a window into how the country's authoritarian regulators are growing savvier at choking out what they see as undesirable speech - while limiting the anger their deletions stir both domestically and abroad. **Researchers with U of T's Citizen Lab at the Munk School of Global Affairs studied the app WeChat, the principal artery of digital communication in China and owned by one of the country's largest Internet firms, Tencent Inc. They found evidence of a complex WeChat management system that alters degrees of censorship according to the situation.**

Microsoft, Intel, IBM Push Back on China Cybersecurity Rules
Dow Jones Newswire, Eva Dou, 2016 12 01
Beijing— **Tough new Chinese cybersecurity rules are providing a rare, behind-the-scenes look at a regulatory skirmish between U.S. technology companies and Beijing**. China is moving to require software companies, network-equipment makers and other technology suppliers to disclose their proprietary source code, the core intellectual property running their software, to prove their products can't be compromised by hackers. Tech companies are loath to offer up their source code, saying this will heighten the risk of their code falling into the hands of rivals or malefactors--and may not guarantee it is hack-proof. Microsoft Corp., Intel Corp. and International Business Machines Corp. are among those filing objections. **Chinese authorities have said these measures are necessary to guard against foreign espionage tools** being embedded in software used here. They frequently cite claims by former U.S. National Security Agency contractor Edward Snowden that such back doors were routinely built into U.S. technology products sold overseas. Beijing maintains that its security rules apply to domestic and foreign companies equally. When China passed the cybersecurity law last month, a spokesman for the internet regulator said foreigners who thought the law would favor domestic firms had a "misunderstanding, a biased view." But in Technical Committee 260's discussions, certain government officials argued for the standards to be drafted to favor domestic companies. "The big trend is called shifting to domestic production," wrote **Guo Qiquan, chief engineer at the China Ministry of Public Security's Network Security Bureau, in a suggestion that the committee marked "approved."**

China military says it's seriously concerned by Japan-South Korea pact
Reuters, Ben Blanchard, 2016 11 30
Beijing - **China's Defence Ministry on Wednesday expressed serious concern about South Korea and Japan signing a military intelligence pact** to share sensitive information on the threat posed by North Korea's missile and nuclear activities. The signing of **the General Security of Military Information Agreement had originally been expected in 2012, but South Korea postponed it due to domestic opposition**. The case for the neighbours to pool intelligence has increased, however, as North Korea has been testing different types of missiles at a faster rate, and claims it has the capability to mount a nuclear warhead on a missile.

Return to Table of Contents/ Retour à la table des matières

Russia / Russie

FSB reports foreign special services preparing massive cyber attacks
ITAR-TASS World Service, Staff report, 2016 12 02
Moscow - **Foreign special services are preparing to carry out massive cyber attacks starting from December 5 aimed at destabilizing** Russia's financial system, the Federal Security Service said on its website on Friday. The goal of the cyber attacks is also to destroy

the activity of "a range of major Russian banks," according to the FSB. The servers and command centers for carrying out these cyber attacks are located in the Netherlands and are owned by Ukraine's hosting company BlazingFast.

Major Russian banks say unaffected by cybersecurity threats
ITAR-TASS World Service, Staff report, 2016 12 02
Moscow - **Russia's leading financial group VTB and the biggest lender Sberbank said on Friday cyber threats have not affected their activities. Earlier in the day, Russia's Federal Security Service (FSB)** announced that foreign special services were plotting a series of cyber attacks starting from December 5 aimed at destabilizing the country's financial system, including the activity of major Russian banks. "The security systems of the group's banks meet all the latest requirements and guarantee full protection of our clients' operations," the press service of the VTB Group told TASS. Sberbank, the third largest bank in Europe, said it is "working in a normal mode."

La Russie dit avoir déjoué une cyberattaque contre ses banques
Reuters, Christian Lowe avec Elena Fabrichnaya et Kira Zavialova, 2016 12 02
Moscou - La **Russie a annoncé vendredi avoir mis en échec un complot ourdi par des espions étrangers pour semer le chaos dans le système bancaire russe par des cyberattaques** coordonnées et la diffusion de fausses informations sur l'état de ses banques sur les réseaux sociaux. Le **Renseignement intérieur russe (FSB)** précise dans un communiqué que les serveurs qui devaient servir à lancer les cyberattaques sont situés aux Pays-Bas et qu'ils sont enregistrés auprès de BlazingFast, une société ukrainienne d'hébergement de sites internet.

Foreign intelligence head: West's 'compulsory globalization' policy sparks public backlash
ITAR-TASS World Service, Staff report, 2016 11 30
Moscow - The **West's zealous policy of "compulsory globalization" has generated a natural resistance in some countries including the US, Russia's Foreign Intelligence Service Director Sergei Naryshkin** said at the Primakov Readings international conference in Moscow. He pointed out that a candidate encouraging the public to cherish national traditions had won the recent US presidential election. Naryshkin also said that a while ago many swore by an unshakable unipolar world forever, but now the number of countries guided by their national interests, has started to grow.

Return to Table of Contents/ Retour à la table des matières

Europe

Government finalizes draft work for restructuring of Turkish intelligence
Daily Sabah, Staff report, 2016 12 06
Ankara - As **part of the constitutional change to switch from a parliamentary system to a presidential one, the government has finalized its draft work on the restructuring of Turkey's intelligence unit.** In that respect, once the system of governance has shifted to a presidential system, the head and coordinator of the intelligence unit will be the Presidency, with the unit referred to as the "**National Security Directorate**." The restructuring of the intelligence unit was brought to attention by Prime Minister Binali Yildirim shortly after the Gülenist Terror Group's (FETÖ) July 15 coup attempt. Prime Minister Yildirim had initially said that the National

Intelligence Organization (MIT) would be restructured and domestic intelligence would be handled by a separate unit, putting foreign intelligence under the MIT umbrella. Explaining that MIT monitors intelligence sharing between the police, gendarmerie and other institutions, Yildirim said, "Today's need is the compilation of domestic intelligence under one entity. Foreign intelligence will continue to be compiled under the MIT." Furthermore, the National Security Directorate will have similar features to the U.S. national intelligence unit, with the directorate under the Presidency and the national security director appointed by the Presidency as well. The **intelligence unit**, in that respect, will not only serve as the overseer of the aforementioned gendarmerie, local police and intelligence units but also function as coordinator among them. However, if the system is not changed to a presidential one, the directorate will operate under the Prime Ministry.It is almost definite that domestic and foreign intelligence are going to be separated into two different units while the MIT will be in charge of foreign intelligence, like the **Central Intelligence Agency (CIA) in the U.S. The Signal Intelligence Division** which was formerly under the control of the General Staff of Electronic Systems' Command and is currently operating under the MIT. That will change with a presidential system, in which the division would be operated under the National Security Directorate.

Pas de postes supplémentaires au SRC pour l'instant
Agence Télégraphique Suisse, 2016 12 06
Genève— **Les moyens prévus pour le Service de renseignement de la Confédération (SRC) sont pour l'instant suffisants**. Fort de cette conviction, le Conseil des Etats a enterré mardi tacitement une motion du National qui réclamait plus de personnel. Depuis le dépôt du texte en septembre **2015, 86 postes supplémentaires ont été créés dans le domaine de la lutte contre le terrorisme, dont 23 pour le SRC, a** rappelé Isidor Baumann (PDC/UR) au nom de la commission. L'application de la nouvelle loi sur le renseignement s'accompagnera par ailleurs de la création de 19,5 emplois. Le SRC ne peut actuellement justifier le besoin d'autres postes, en a conclu la commission, suivie à l'unanimité par le plénum ainsi que par le ministre de la défense Guy Parmelin. Si le niveau de menace devait augmenter, la Chambre des cantons encourage toutefois le Conseil fédéral à soumettre sans tarder au Parlement des propositions d'augmentation des effectifs.

Un suivi à la fois sécuritaire et social
Tribune de Genève, S.R., 2016 12 06
Genève - Conscient des risques liés à la radicalisation, **Genève maintient ses efforts en matière de sécurité et de prévention.** Des mesures d'accompagnement de personnes radicalisées ont notamment été annoncées hier, lors de la troisième conférence de presse du genre organisée en un an, suite aux attentats de Paris. « La Suisse n'est pas un îlot et la menace reste élevée ici aussi » , rappelle **Paul Zinniker, vice-directeur du Service de renseignement de la Confédération (SRC),** devant les médias. « Nous prenons très au sérieux les menaces, sans céder à la terreur, livre Pierre Maudet, chef du Département de la sécurité et de l'économie (DSE). Nous avons plus un coup d'avance qu'un coup de retard désormais. En un an, nous avons développé une prise en charge globale des phénomènes de radicalisation. »

Genève affine sa stratégie pour lutter contre la radicalisation
Le Temps (Suisse), Laure Lugon Zugravu, 2016 12 06
Genève –. Le **canton réagit face aux phénomènes de radicalisation**. Si l'outil de prévention est désormais opérationnel, une approche éducative a été mise en place pour prendre en charge les voyageurs du djihad qui rentreront. A Genève, **340 cas de radicalisation ont été signalés depuis 2014 par le Service de renseignement de la Confédération (SRC), soit 19 de plus qu'en juin.** Parmi eux, 35 sont suivis car ils présentent un danger pour la sécurité

intérieure. Ces gens ne résident pas forcément à Genève, mais y travaillent ou y ont une vie sociale, note Monica Bonfanti, cheffe de la police. Genève n'a pas enregistré de nouveau départ depuis juin, où cinq départs étaient recensés. « Cette fois, nous avons un coup d'avance et non un coup de retard comme l'an dernier! »

Dutch Secret Service Investigated Far-right Leader's Ties to Israel
Haaretz, Shlomo Papirblat, 2016 12 05
Brussels - **Geert Wilders, leader of Holland's far-right anti- Muslim Party of Freedom, was investigated in the past by the country's General Intelligence and Security Service (AVID)** over his "ties to Israel and their possible influence on his loyalty." Wilders, whose party is leading the polls ahead of the upcoming election in March, is likely to be a key figure in the next government. The undercover investigation was exposed over the weekend by the veteran daily De Volkskrant. According to the article, AVID agents conducted the investigation from 2009 to 2010, with its existence and results remaining unknown until now.

Lithuanian police searching for suspected spy
Baltic News Service, 2016 12 05
Vilnius—**Vilnius police is searching for a suspected spy,** the Vilnius County Central Police Commissariat said. **Vladimir Sokolov, 50, is suspected of seizing, buying and otherwise collecting information that constitutes a Lithuanian state secret or any other information that may be interesting to foreign intelligence**. Under Lithuanian laws, the punishment for the crime is between three and 15 years in prison. According to information available to the police, the man is suspected of spying in an organized group. **Aurelija Katkuviene, strategic communications chief at the State Security Department,** told BNS that all information in connection to the search was part of a pre-trial investigation, adding that the department would not provide any information.

Jean-Marc Gadoullet. Un agent très special
LePoint.fr, Hubert Coudurier, 2016 12 04
Paris - C'est **un ancien du 11e Choc, le bras armé de la Direction générale de la Sécurité extérieure (DGSE). Dans son livre (*), Jean-Marc Gadoullet évoque son expérience d'agent secret au service de la France sur les théâtres d'opération africains comme dans les Balkans.** Et surtout au Sahel, lors d'une libération d'otages controversée pour laquelle il donne sa version. 6.000 personnes, 600 millions d'euros de budget : la **DGSE, dont le siège est situé boulevard Mortier dans le 20e arrondissement de Paris, reste encore mystérieuse, même si son directeur, le très discret Bernard Bajolet, a autorisé le tournage de la série de Canal plus « Le bureau des légendes »**, dont l'acteur principal, Mathieu Kassovitz, lui donne enfin une incarnation que la CIA a conquise depuis longtemps grâce à Hollywood. À l'heure où le chef de l'État est stigmatisé pour avoir révélé son ordre de procéder à quatre opérations « Homo » (pour homicides) alors que la politique de liquidations ciblées de terroristes est presque devenue une routine, cette plongée dans le monde du renseignement que propose Gadoullet tombe à pic. Ce n'est ni la première ni la dernière. On se souvient des mémoires **d'anciens directeurs de la DGSE, comme Claude Silberzahn, confessé par notre chroniqueur Jean Guisnel, ou encore d'Alexandre de Marenches (patron de l'ancêtre de la DGSE, le Service de documentation extérieure et de contre-espionnage (SDECE),** qui lui, s'était confié à Christine Ockrent.

Western spy agencies face nightmare as moles thrive online
The Australian, Ben Macintyre, 2016 12 04
Canberra - The **German equivalent of a mole in spy jargon is U-boot (U-boat): an unidentified threat lurking just below the surface, unseen, silent and lethal. Germany's**

domestic intelligence agency discovered a U- boat in its midst last week that has already inflicted huge reputational damage -- an Islamist convert who infiltrated the agency to gather secrets and alert his "religious brothers" to impending danger, and who may have been planning an attack on its headquarters. Unknown to them the mole, a married father of four, had acted in gay pornographic films and secretly converted to Islam in 2014. A proper vetting procedure would have brought this to light and set off every alarm bell. Instead, the German authorities admitted, he remained "inconspicuous during the application process, training and at work". The mole, U-boat, or "sleeper agent" is every spy agency's nightmare: the spy who makes himself eligible for employment by his foe's intelligence service, lays low, and then destroys the machine from within by passing on its secrets, warning its targets, and betraying its agents. The most **successful moles in history were the Cambridge spies of the 1930s, the communist converts working for the KGB who infiltrated Britain's MI5, MI6 and the Foreign Office**. Britain used the same techniques to undermine German intelligence during World War II. Today the deep penetration agent is back to haunt the intelligence services.

Europol: 'IS' likely to target EU in 'near future'
Deutsche Welle, Staff report, 2016 12 02
Berlin - **The so-called "Islamic State" group is likely to carry out terror attacks in the European Union in the near future, Europol said in a report** on Friday. The Sunni extremist group has "both the will and the capability" to strike both soft and hard targets in Europe, especially those countries participating in the anti-IS coalition, the EU police agency said. "EU Member States that participate in the anti-IS coalition are regarded by IS as legitimate targets," it said, pointing to particular risk in France, Belgium, Germany, the Netherlands and the United Kingdom. The report warns that as IS is weakened and defeated in Syria and Iraq, foreign fighters may return to Europe with their families, posing a long-term security challenge.

French poll warning over Russian hacking threat
London Times, Adam Sage, 2016 12 02
Paris - **France's political parties have been summoned to a meeting by the country's top spy agency and told to strengthen their defences against cyberattacks amid fears that Russian hackers could seek to influence the presidential election next year**. French intelligence agencies endorse claims that the Kremlin tried to sway the US presidential race, and believe that similar tactics might be deployed in France. Germany's spy chief expressed concern this week that Russia would use cyberattacks to spread misinformation before the German elections next autumn. The issue is particularly sensitive in France given President Putin's support for right- wing presidential election candidates. He is an admirer of François Fillon, of the Republican party, and has close ties with Marine Le Pen, leader of the far-right National Front.

Wikileaks releases 2,420 documents from German government NSA inquiry
Deutsche Welle, Staff report, 2016 12 02
Berlin - The **documents contained 90 gigabytes of information including many classified documents, according to the statement on the Wikileaks website on Thursday**. They are the property of government agencies such as the **Federal Intelligence Service (BND, pictured above) and the Federal Office for the Protection of the Constitution (BfV).** The published materials had been submitted last year as part of a German parliamentary inquiry into the surveillance activities of the BND and its cooperation with the NSA. "The collection contains early agreements between the BND and the NSA and internal processes at the BND, but also more recent details on the close collaboration between the two agencies," Wikileaks announced, adding: "This substantial new collection of primary source documents provides significant new evidence (of their collaboration)." The documents, Wikileaks claimed, contain the

answers to questions posed by the inquiry committee as well as administrative documents, correspondence, agreements and press reactions.

Communist spies behind the Iron Curtain kept 'top secret' file on Donald Trump when he married Ivana - and interrogated her father about him
Mail Online, 2016 12 02
London— Top **secret intelligence files on US president-elect Donald Trump have emerged in the Czech Republic where he was kept under observation for years by Communist-era spies.**Trump came under scrutiny following his marriage to Czechoslovakian-born Olympic skier Ivana Zelnickova in 1977. Now the **long buried documents - marked 'Top Secret' - have emerged in the Czech media after nearly 40 years**. The files - often written in the language used by the feared **StB secret police** - describe Trump as 'the most successful young man of America' and a 'political influencer.' They go on to say how Trump 'totally s*** himself' when he first met Ivana. They offer insight into the astonishing naivete of the Communist secret police about the West. The Communist secret police investigated Ivana and how she rose from humble beginnings to become the star of American high society.

What we know about the 'gay porn star turned Islamist spy'
The Local (Germany), Staff report, 2016 12 01
Berlin - News this week that a member of the **BfV was a suspected Islamist** was already strange enough, but then both the Washington Post and Bild reported that the suspect of Spanish origin had starred in gay porn videos, found while investigators searched his home. The case has raised questions about security flaws in the intelligence service and it will perhaps take some time before all the answers are revealed, but here's what we know so far. **The suspect was arrested on November 17th after chatting online with a man posing as another Islamist - who the suspect didn't realize was actually a colleague at the intelligence agency.** The suspect made "Islamist remarks online under a false name", according to the BfV. He also offered internal information during the chat. According to information obtained by DPA and other news outlets, the man had also told his chat partner that he could give other like-minded people access to the headquarters of the BfV in Cologne.

Belgium Employs Private Security Companies in Operations of Surveillance, Inspection
Asharq Al-Awsat, Abdullah Mustafa, 2016 12 01
Brussels - The **Belgian Interior Minister, Jan Jambon, said that security guards in the country will be allowed to practice some of the police missions like participating in questioning people to verify their identities or to inspect their bags as part of the new regulations adopted by the government concerning the work of private companies**. Discussions took place in the Parliament of Brussels on new solutions to reduce the burden of policemen after the last terrorist attack that took place in Brussels, which targeted an airport and a train station in the capital, killing 32 people and wounded 300 others.

Ces espions qui traquent les terroristes
L'Obs, Violette Lazard, 2016 12 01
Paris - **Alors que la menace terroriste demeure et qu'un nouvel attentat vient d'être évité, "l'Obs" a pu partager pendant plusieurs semaines le quotidiendes hommes du renseignement territorial chargés de surveiller les personnes radicalisées**. Une tâche aux allures de mission impossible De loin, les schémas accrochés aux murs ressemblent à des arbres généalogiques avec des traits noirs, en pagaille, et des petites photos à chaque extrémité. De près, on y décrypte rapidement les noms des principaux terroristes qui ont frappé la France ces derniers mois. Abdelhamid Abaaoud. Salah Abdeslam. Fabien Clain. Il y a là l'organigramme du 13 novembre. Juste à côté, celui des principales filières françaises. Cette

funeste décoration a été accrochée il y a quelques mois entre deux insignes de police et des décorations militaires dans les bureaux de la cellule chargée de l'évaluation de la radicalisation, dans ce **service du renseignement territorial (le SCRT, ex-RG.)** Pile à la hauteur du regard. Ce soir-là, la plupart des bureaux sont vides. Il est 19 heures. Marc a allumé une loupiote au-dessus du sien.

La Sûreté de l'État ne contrôle son personnel que tous les cinq ans
L'Avenir, Emmanuel Huet, 2016 12 01
Bruxelles— **Un islamiste infiltré dans les services de renseignement belge, est-ce possible?** La question mérite d'être posée après l'arrestation d'un des agents du renseignement intérieur allemand. Converti depuis 2014, il semble que l'islamiste présumé envisageait de mener un attentat au sein des services de renseignement allemand. En Belgique, **la VSSE (Sûreté de l'État) confirme que le risque zéro n'existe pas. Ni chez eux ni dans un autre service.** Du personnel d'entretien à la direction en passant par les analystes, les informaticiens… ce sont près de 550 personnes qui travaillent dans le bâtiment du North gate à Bruxelles. Et pour y rentrer, un bon CV ne suffit pas. Il faut montrer patte blanche… Un contrôle pour la personne et les membres de sa famille Au sein de la VSSE, on considère que chaque employé peut ou pourrait avoir accès à des informations classées «très secrètes». Dès lors, l'ensemble du personnel dispose d'une habilitation de sécurité de ce niveau. **L'habilitation est valable pour une période de 5 ans**. Et donc, une nouvelle enquête sera réalisée de manière périodique pour le personnel en place. Cette enquête complète porte aussi sur l'ensemble des personnes majeures qui composent le ménage. Car il ne s'agit pas de faire entrer n'importe qui à la Sûreté de l'État.

Un nouveau Vigipirate face au terrorisme
Le Figaro, Alain Barluet, 2016 12 01
Paris - **Validé mercredi par l'Élysée, ce plan rénové crée un troisième niveau d'alerte inédit : « urgence attentat »** . Défense La prolongation, à un niveau élevé, de la menace terroriste en France conduit l'État à s'adapter. Comme jamais auparavant, cette menace est évaluée en permanence et les « postures » de sécurité fréquemment ajustées, depuis les attaques survenues en 2015. Mais la « rupture stratégique » illustrée par les attaques de janvier et novembre 2015 impliquait, non plus une simple adaptation, mais une révision en profondeur du plan Vigipirate, supervisé par le premier ministre, et dont la première mouture remonte à 1978. Un Conseil de Défense, réuni mercredi à l'Élysée, a validé un plan renforcé, qualifié de « Vigipirate plus » , que Le Figaro a pu consulter. Cette même réunion, autour de François Hollande, a décidé la mise en place de mesures spécifiquement adaptées aux fêtes de Noël - vingt-septième « posture » de sécurité pour l'année 2016, là où, naguère, Vigipirate n'était adapté que trois ou quatre fois par an. Le **nouveau plan Vigipirate prévoit la création d'un système à trois niveaux de menace : « vigilance » , « sécurité renforcée/risque d'attentat » et « urgence attentat » , le plus élevé.**

Met a friendly stranger? Call us, say Lithuania's spyhunters
Reuters, 2016 11 30
Vilnius— A single mother takes a kindly man into her confidence. A student is plied with beer by a smiling stranger. Beguiling scenes. But **Lithuanians are being urged in TV adverts to be wary of the kindness of strangers and call a new 'spyline' to check if they aren't, perhaps, being lured into espionage by foreign agents.** By foreign agents, **Lithuania means the Kremlin.** Ties have always been tense with former imperial master Moscow. But since the annexation of Crimea, Russia is seen in Vilnius as a threat to Lithuania and the other Baltic states of Estonia and Latvia. "People don't even think that information is being squeezed out of them until it's too late," **Darius Jauniskis, the 48-year-old head of Lithuania's State Security**

Department, told Reuters. "So to prevent this, we are going public and we are explaining all this." The **Russian Foreign Ministry and the FSB security service did not immediately respond to written requests for comment**.

German domestic spy agency denies security lapse after Islamist mole
Deutsche Welle, Staff report, 2016 11 30
Berlin - **The head of the Office for the Protection of the Constitution (BfV), Hans-Georg Maassen, said that the body maintained all security standards and had no way of knowing that a 51-year-old employee, hired last April, was a follower of the radical Salafist movement**. "We carried out a thorough background check in which we interviewed five references and looked at the entire spectrum [of information]," Maassen told reporters. "He was the father of a large family from a solid economic background who did good work. He apparently radicalized himself." According to news magazine "Der Spiegel," the man, who was tasked by the BfV with observing the Salafist scene, had himself converted to Salafism in 2014 unbeknownst to the Office or even to his own family. He was uncovered after another BfV employee found him revealing confidential information on an Internet chat room and offering to help get a radical Islamist into BfV headquarters in Cologne, ostensibly for the purposes of a terror attack.

Arrested German spy was a onetime gay porn actor -- and a secret Islamist
Washington Post, Souad Mekhennet, Anthony Faiola, 2016 11 30
Berlin - Two weeks ago, **German intelligence agents noticed an unusual user in a chat room known as a digital hideout for Islamic militants. The man claimed to be one of them -- and said he was a German spy**. He was offering to help Islamists infiltrate his agency's defenses to stage a strike. Agents lured him into a private chat, and he gave away so many details about the spy agency -- and his own directives within it to thwart Islamists -- that they quickly identified him, arresting the 51-year- old the next day. Only then would the extent of his double life become clear. The German citizen of Spanish descent confessed to secretly converting to Islam in 2014. From there, his story took a stranger turn. Officials ran a check on the online alias he assumed in radical chat rooms. **The married father of four had used it before -- as recently as 2011 -- as his stage name for acting in gay pornographic films**. Authorities on Tuesday said they had arrested him on suspicion of preparing to commit a violent act and for violating state secrecy laws.. **One senior BfV official, who discussed the matter on the condition of anonymity because he was not authorized to speak to the media defended the agency, said it was virtually impossible to protect against a breach like this**.

Reports: German domestic spy agency finds Islamist amongst its own
Deutsche Welle, Staff report, 2016 11 29
Berlin - **Germany's domestic intelligence agency (BfV) has discovered an Islamist working within its own ranks**, according to domestic media reports on Tuesday. The case allegedly surrounds a 51-year-old German who planned to bomb the BfV headquarters in Cologne. According to Der Spiegel, the man was active on extremist websites. Using a pseudonym, he gave away secret information, allegedly gathering information on the times and details of raids against extremists. The news outlet wrote that the man's family was not even aware he had converted to Islam in 2014. Having previously worked at a bank, the man joined the BfV in April 2016 - joining a new task force monitoring the ever-growing Salafist scene in Germany.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Iran creates 'Cyber Brigades' for online war
Al Arabiya, Staff Writer, 2016 12 06
Dubai - The **commander of students' Basij militias, Ali Sabir Hamani, announced the formation of 'Cyber Brigades' comprising school students with the aim of taking part in cyber warfare launched against the Islamic Republic**. This would be in parallel to the 'Joint Cyber Army' of the Iranian Intelligence whose main task is to focus on monitoring online hostilities. According to the semi-official news agency, the committee has organized training programs attended by 200 of the 'elite' students from different Iranian provinces, trained on how to handle conflicts in cyberspace.

Syrie : le chef du renseignement sort de sa réserve pour prôner la fermeté
Le Monde, Madjid Zerrouky, 2016 12 05
Damas - **Le général Hassan regrette la " modération " du régime au début du soulèvement.** Si nous avions été plus fermes au début, nous n'en serions pas là aujourd'hui. " Cette phrase, le général syrien **-Jamil Al- Hassan, qui dirige les -redoutés services de renseignements de l'armée de l'air,** l'a répétée trois fois en moins d'un mois, en novembre. Cette notion de manque de " fermeté " laisse songeur au sujet d'un conflit qui a fait 300 000 morts, mais la -parole d'un chef de la machine répressive du régime syrien est rare. Elle prend aujourd'hui un relief particulier alors que les -lignes de défense rebelles dans la ville d'Alep s'effondrent.

Intelligence Minister: Iranian nation will never bow to terror attacks
Islamic Republic News Agency, 2016 12 01
Ahvaz - **Intelligence Minister Mahmoud Alavi said that Iranian nation will never surrender to terror attacks, as martyrdom is part of its religious culture**. Addressing the funeral procession of martyrs of the terror attack in Hilla, Iraq, on Wednesday, he added that Shia Muslims are ready for martyrdom and making sacrifices for the sake of God and Imam Hossein (AS), grandson of Prophet Mohammad (PBUH). Noting that Shia Muslims have never been alien to martyrdom and have always welcomed death for the sake of God, intelligence minister said that they will never succumb to the enemies, as Imam Hossein (AS) considered dignified death better than humiliated life.

Return to Table of Contents/ Retour à la table des matières

Asia / Asie

Canadian envoy lauds Bangladesh role in curbing terrorism
Bangladesh Sangbad Sangstha, 2016 12 06
Dhaka - **Canadian High Commissioner to Bangladesh Benoit-Pierre Laramee today lauded the Bangladesh's stand on fighting terrorism and religious extremism**. He made the remarks while he paid a courtesy call-on Road Transport and Bridges Minister and Awami League General Secretary Obaidul Quader at his office in the ministry. The Canadian high commissioner assured Quader that Canada will extend its cooperation to Bangladesh to curb trans-boundary terrorism. Laramee greeted the road transport minister for being elected as general secretary of Awami League. "Bangladesh's achievements in women empowerment, poverty alleviation, reducing dropout rate at educational institutions and gender equity are praiseworthy," the high commissioner said.

Cyber attacks on gov't agencies, ransomware programs to rise in 2017: report
Yonhap News Agency, Staff reporter, 2016 12 05
Seoul - **More cyber attacks on key government agencies and social infrastructure-related facilities, coupled with increased ransomware programs for mobile and desktop computers, are likely to take place next year, a state-run agency** said Monday. According to the **Korea Internet & Security Agency (KISA),** a series of cyber attacks may occur with the aim of stirring increased political and social instability in the country. In particular, military and North Korea-related sites would be the targets of their attacks, it said. Also, software and mobile devices will remain vulnerable to ransomware programs, it said.

Delhi, Dhaka to talk on terrorism, intel-info sharing
Times of India, Staff Report, 2016 12 05
New Delhi - **Anti-terror cooperation, sharing of intelligence inputs and how to jointly check cross-border smuggling will dominate the discussions between home secretaries of India and Bangladesh** which begin on Monday. Home secretary Rajiv Mehrishi and his Bangladeshi counterpart Mozammel Haque Khan and their teams will engage in intense discussions for two days to strengthen the anti-terrorism mechanism and sharing of information about terrorists.

Countdown begins for spy chief posts
The Telegraph (India), 2016 12 04
New Delhi— The **government is likely to pick the new heads of the Intelligence Bureau and the Research & Analysis Wing by mid-December**. The chief of external spy agency RAW, **Rajinder Khanna, and his internal intelligence counterpart Dineshwar Sharma of the IB are due to retire on December 31.** Home ministry sources said the contenders for the coveted IB director's post included two of the agency's special directors, S.K. Sinha and Rajiv Jain, and Mumbai police commissioner Dattatray Padsalgikar. "Sinha is an expert on Kashmir issues and counter-terrorism. He is a strong contender considering Prime Minister Narendra Modi's continuous focus on Kashmir and terror," a senior ministry official said.

24 ISI agents arrested in 2016: Govt
Kashmir Images, 2016 11 30
New Delhi— As **many as 24 ISI agents have been arrested for spying for the Pakistani intelligence agency** so far this year, the Lok Sabha was informed today. "In addition to these 24 agents, one Pakistani spy agent detected in October 2016 was Pakistan High Commission, New Delhi based intelligence officer Mehmood Akhtar," Minister of State for Home Hansraj Ahir said replying a written question. Of those, who were arrested so far this year, nine were detected in Rajasthan, six in Punjab, two in Gujarat, two in Jammu and Kashmir, one in Uttar Pradesh and four in Delhi. Ahir said some of the staff posted in Pakistan High Commission in New Delhi is suspected to be involved in running espionage network.

S. Korea vows full support for anti-money laundering body
Yonhap News Agency, Staff reporter, 2016 11 30
Seoul - **South Korea's financial authorities on Wednesday reaffirmed their commitment to fully support a global organization, based in the country, on anti-money laundering and counter -terrorism financing.** Jeong Eun-bo, vice chairman of the Financial Services Commission (FSC), delivered the message to Kevin Stephenson, head of the Training and Research Institute (TREIN) affiliated with the Financial Action Task Force (FATF). They met here on the sidelines of the inaugural regular consultation session between the FSC's Korea Financial Intelligence Unit and TREIN.

Return to Table of Contents/ Retour à la table des matières

Africa / Afrique

Security Agents, Informants Protection Bill Passes Second Reading
This Day (Nigeria), 2016 12 04
Abuja— A **bill seeking to guarantee the identity of national security agents, sources and informants from unlawful disclosure has passed through second reading in the House of Representatives**. The bill, sponsored by **Hon. Oluwole Oke**, named: 'a bill for an Act to Provide for the Protection of the **Identities of National Security Agencies Officers, Agents**, Sources, Informants and Operational Methods from Unlawful Disclosure and to Protect their Establishments, Facilities and Equipment against Unauthorised Access, as well as Provide for the Promotion and Engagement of **Nigeria's External Security** and for other related matters." The bill, however, prohibits the disclosure of the identity of an intelligence officer and criminalises any unlawful disclosures..He added that Nigerians are also wary of giving information to security agencies as the confidentiality of such disclosures cannot be guaranteed, therefore putting the informants at risk. The section equally proceeds to protect the facilities, installations and equipment of an **intelligence agency**.

Nigerian court rules security agency should release Shi'ite leader
Reuters, 2016 12 02
Abuja— The **leader of Nigeria's largest Shi'ite Muslim sect should be released after being held without charge for nearly a year by the country's security agency**, a court ruled on Friday. **Sheikh Ibrahim Zakzaky, leader of the Islamic Movement in Nigeria (IMN),** has been detained since mid-December 2015 after his followers clashed with the army in the northern city of Zaria. A judicial inquiry in August said 347 IMN members were killed and buried in mass graves after the violence. Security analysts have drawn parallels between IMN -- a minority sect in the mainly Sunni Muslim north -- with Boko Haram, the Sunni Muslim jihadist group whose insurgency began in 2009 after security forces killed hundreds of its members and its leader Mohammed Yusuf died in custody. A judge at the federal court in the capital, Abuja, said the IMN leader should be released. The judge rejected the argument by the **State Security Service** (SSS) that it was holding him for his own protection from locals in his home city of Zaria.

Sudanese Security continues crackdown on press, journalists strike
Sudan Tribune, 2016 12 02
Kthartoum— **Sudan's National Intelligence and Security Service (NISS) on Thursday has continued its mass confiscation of newspapers print-runs for the successive fourth day**, which coincided with the call for civil disobedience. On Wednesday, two dailies went on strike and did come out in protest against NISS crackdown on newspapers. Mass confiscation has emerged as a new technique of punishment by the NISS which tends to accuse the press of disseminating news that adversely impact on national security. On Thursday morning, NISS has confiscated the print-runs of Al-Tayyar, Al-Youm Al-Tali and Al-Watan for the third successive day without any explanation.

Return to Table of Contents/ Retour à la table des matières

Americas / Amériques

Chile court OK's extradition in 1976 car bombing in US
Associated Press, 2016 12 05
Santiago, Chile— **Chile's Supreme Court ruled Monday that the government can file an extradition request to the United States for two former secret police agents** wanted for a 1976 car bombing in Washington that killed a former Chilean ambassador and a U.S. citizen. In a unanimous decision, the court said the Foreign Ministry should begin the procedures needed to seek the extradition of U.S. citizen Michael Townley and Chilean Armando Fernandez Larios. They served under Gen. Augusto Pinochet's 1973-1990 dictatorship.The decision came after a request by Chilean Judge Mario Carroza, who specializes in human rights crimes. Declassified U.S. intelligence documents that came to light last year revealed that Pinochet directly ordered Letelier's assassination. One document includes an **assertion by the former head of Chile's intelligence agency, Manuel Contreras,** that "he authorized the assassination of Letelier" on "direct orders from Pinochet." In 2005, Contreras and his second in command were convicted in Letelier's death. Contreras died last year.

Return to Table of Contents/ Retour à la table des matières

The Agencies/Nouvelles des services

A weekly compendium on corporate and administrative issues of partner (and adversarial) intelligence agencies around the globe.
Un recueil hebdomadaire portant sur les enjeux de nature générale et administrative que connaissent les services de renseignement partenaires (et antagonistes) du monde entier.

Produced by the CSIS Communications Branch/ Publié par la Direction des communications du SCRS

11-05-2016 to/au 16-05-2016

Table of Contents/Table des matières

Five Eyes/Groupe des cinq

Canada

Review: A chilling cautionary tale
Calgary Herald, Eric Volmers, 2016 12 20
Superficially at least, there may be a rich irony to Justin **Pemberton's intriguing interactive documentary I Spy With My Five Eyes.** The New Zealand-Canadian coproduction is a **chilling cautionary tale about the changing nature of surveillance, making a convincing case that our daily actions are leaving glaring digital footprints that government spy agencies can easily access.** I Spy With My Five Eyes is also interactive - visitors are encouraged to share their views on this controversial topic. So, in essence, aren't people being asked to go online and share their views about the dangers of sharing too much online? Apparently, it's not the first time the New Zealand filmmaker has had this pointed out to him. **"Certainly, if you are someone who is of interest to the NSA or the Canada wing of Five Eyes or the New Zealand one or whatever, they would love to see that you have visited this website,"** says Pemberton, in an interview from his home in Auckland… Pemberton and his crew travelled to all of the Five Eye nations to interview a wide array of subjects. There are the usual lineup of activists, investigative journalists, political scientists, futurists and anthropologists. But the filmmaker also talks to figures such as Rhys Ball, a former spy with New Zealand's Security Intelligence Service; General Michael Hayden, former director of both the CIA and National Security Agency; and NSA employee turned whistleblower William Binney. Note: **To watch I Spy With My 5 Eyes, visit ispydoc.com.**

Perdus par les services secrets
Journal de Montréal, Sarah-Maude Lefebvre, 2016 12 19
Ottawa - **Six téléphones cellulaires et un ordinateur portable appartenant à des employés du Service canadien du renseignement de sécurité ont été volés ou perdus depuis quatre ans, a appris notre Bureau d'enquête. et le SCRS ne peut pas garantir que des informations sensibles ne sont pas tombées entre de mauvaises mains**. Le nombre d'appareils électroniques égarés par l'organisme chargé de lutter contre l'espionnage et le terrorisme au Canada peut sembler peu élevé à première vue. Mais les conséquences peuvent être cruciales pour la sécurité nationale, affirme l'ancien agent du SCRS **Michel Juneau-Katsuya**. «Nous ne pouvons pas élaborer davantage. Ce que je peux dire, c'est que le SCRS fonctionne conformément à la Loi sur le SCRS, aux directives ministérielles et à un système solide de politiques et de procédures internes», a indiqué le porte-parole **Tahera Mufti**.

Mis en garde, le SCRS n'a toujours rien fait
Journal de Montréal, Sarah-Maude Lefebvre, 2016 12 19
Ottawa - **Même s'il a été mis en garde il y a un an sur les dangers liés à la perte d'informations classifiées, le SCRS n'a toujours pas renforcé ses politiques de sécurité à ce jour**. En décembre 2015, le **Comité de surveillance des activités de renseignement de sécurité (CSARS)** avait rappelé à l'ordre l'organisme fédéral sur la nécessité de se protéger contre les fuites ou la perte de documents secrets. Le porte-parole **Tahera Mufti** a confirmé à notre Bureau d'enquête que les services secrets étaient toujours «en train de réviser ses politiques de sécurité interne connexes à la suite de l'examen du CSARS et ses recommandations ».

Canada's military too vulnerable to cyber attacks: documents
Global News, Monique Scotti, 2016 12 17
Ottawa - The **Department of National Defence and the Canadian Armed Forces are looking to improve their ability to defend against cyber attacks**, with newly released documents suggesting the current system remains woefully inadequate. DND/CAF published a request for "industry feedback" on Friday morning, stating that the Canadian military wants to develop a new system "that will enable a reliable, near-real-time analysis of its Information Technology Infrastructure (ITI) to detect and identify malicious activities and then provide decision aids and tools" to defend against those attacks. The initiative has been dubbed the **"Defensive Cyber Operations Decision Support Project"** and it's expected to set taxpayers back between $50 and $99 million. Friday's documents were released less than a month after the department's main webpage was hacked. Canadians trying to learn about career opportunities with the military at forces.ca instead found themselves staring at the **landing page of the Chinese central government's official web portal.** Details of the upgrade plan made public on Friday describe the project as a "complex multi-year requirement" that is still in its infancy. The final delivery date is slated for 2024.

Crossed wires hampered terrorism investigation
Ottawa Citizen, Gary Dimmock, 2016 12 16
Ottawa - In **2013, while the RCMP were still investigating how a suspected terrorist had quietly left Canada to join ISIL the previous year, Canada's spy agency informed the Mounties they had in fact already known the intimate details of the terrorism suspect's final hours before he boarded a plane for Syria, new court records reveal**. John Maguire left Canada in December 2012 to join ISIL in Syria, where he was featured in a propaganda video declaring religious war on his home country. The Islamic State reported Maguire died fighting in 2015, though his death has never been confirmed. Before he left for Syria, Maguire was the alleged star terrorism recruit of **Ottawa's Awso Peshdary**, 26. Peshdary was charged in February 2015 with recruiting, financing and facilitating terrorism. And the RCMP's case against Peshdary is where new details have emerged about the Mounties' investigation into an alleged Ottawa terror network.

Operation Picnic was secret phone-tapping feast for RCMP, historian discovers
Canadian Press, Jim Bronskill, 2016 12 15
Ottawa - The **federal government secretly gave RCMP security officials the authority to tap telephone calls without court oversight during the Cold War,** newly unearthed archival documents show. The surveillance program, codenamed **"Picnic,"** began as an emergency effort during the Korean War, but federal agencies collaborated with telephone companies in 1954 to continue the wiretaps, says Dennis Molinaro, who teaches history at Ontario's Trent University. Molinaro's research indicates the RCMP security branch was listening in on the embassies of East Bloc countries, "certain unfriendly organizations" and individuals suspected of disloyalty. It has long been known the Mounties kept an eye on a wide array of people and organizations - from church and gay rights groups to Quebec separatists and Communists - in the name of national security, amassing hundreds of thousands of dossiers. Mountie scandals in the **1970s led to a royal commission, the demise of the RCMP security service and creation in 1984 of the civilian Canadian Security Intelligence Service. Molinaro believes the documentation he has uncovered with the help of tenacious staff at Library and Archives Canada** helps flesh out how the RCMP surveillance of Canadians took place and implicates federal politicians and bureaucrats in making it happen. The issue of when - and how easily - police and intelligence services should be allowed to intercept personal communications continues to play out today, fuelled by former U.S. spy contractor Edward Snowden's revelations of widespread surveillance.

Surveillance de journaliste Le SCRS renie son engagement... et maintient le flou
La Presse+, Joël-Denis Bellavance, 2016 12 14
Ottawa - Les **dirigeants du Service canadien du renseignement de sécurité (SRCS) font volte-face : après s'être engagés devant un comité du Sénat le mois dernier à préciser si des journalistes avaient fait l'objet d'une enquête de leur part dans le passé**, ils reviennent sur leur parole dans une réponse écrite qui a été envoyée au sénateur conservateur Cl**aude Carignan.** Dans leur réponse écrite, les dirigeants du SCRS justifient cette volte-face en affirmant qu'ils pourraient « compromettre l'intégrité des opérations » de l'organisation et « nuire à sa capacité d'exercer le mandat que le Parlement lui a confié » s'ils confirmaient que le SCRS avait déjà eu un journaliste dans sa ligne de mire dans le passé. « Ainsi, le SCRS est au regret de ne pas pouvoir confirmer si des journalistes ont fait l'objet d'une de ses enquêtes, et ce, même si son représentant s'était engagé à donner une réponse spécifique », affirme le SCRS dans sa réponse écrite, obtenue par La Presse.

CSIS now says it will not report media surveillance
Toronto Star, Tonda MacCharles, 2016 12 14
Ottawa - **Canada's spy agency has backtracked on its promise to reveal to a Senate committee how many Canadian journalists it spied on in the past, citing operational security**. The **Canadian Security Intelligence Service** said while it "appreciates the importance of the question" to Canadians and the Senate committee on national security and defence, **"we regret that we cannot confirm whether journalists have been the subject of any CSIS investigation."** Conservative Sen. Claude Carignan called it a "bizarre response" and a "serious" breach of an undertaking to a parliamentary committee. He suggested it implies that surveillance of journalists is either still ongoing or has been recently suspended. "How can it harm operations if you don't have any operations ongoing?" he said in an interview. Carignan, who has tabled a private member's bill to protect journalists' sources, wondered if there had been surveillance operations of media that are currently suspended, especially after the controversial practice surfaced in Quebec where provincial and Montreal police were revealed to have spied on several top investigative reporters and columnists, apparently in search of police leaks. Last month, **Brian Rumig**, assistant director of CSIS operations, **conceded it was possible CSIS had in the past spied on reporters, although it has publicly said no reporters are currently under surveillance.**

Ray Boisvert named new Ontario provincial security advisor
iPolitics.ca, Amanda Connolly, 2016 12 14
Ottawa - The **former assistant director of intelligence at CSIS has been named to a newly-created post -- Ontario's provincial security advisor. Ray Boisvert will start in the new role on January 2, 2017,** and will be tasked with providing advice and intelligence on national security matters that fall under provincial responsibility, including efforts to build critical provincial infrastructure resilience and engaging with provincial security partners. The position is a new associate deputy minister position within the Ministry of Community Safety and Correctional Services. Boisvert will report to the deputy minister of the portfolio while also supporting the cabinet secretary and other senior leaders across the department. Boisvert has more than 30 years of experience in the national security field, including as assistant director of intelligence and director general of the counter-terrorism program at CSIS. Prior to joining CSIS he worked with the RCMP.

Return to Table of Contents/ Retour à la table des matières

United States / États-Unis

Could hackers knock out the power grid? (Canada)
USA Today, Bill Loveless, 2016 12 20
Washington - **Worries over cyberattacks on the USA are increasing in the aftermath of a presidential election in which the CIA alleged that Russia used such means to influence our electoral process**. For the moment, the vulnerability of polling and political operations to hacking gets most of the attention. But this week will mark the one-year anniversary of the first publicly acknowledged cyberincident to take down portions of a power grid, one of the most critical components of a nation's infrastructure. On Dec.23, 2015, about 225,000 customers of three electric distribution companies in western Ukraine lost power as a result of computer breaches and malware plants that investigations indicate began six months before. "The chain of events there is very unlikely to happen here," said Marcus Sachs, the senior vice president and chief security officer at the North American Electric Reliability Corp. (NERC), a non- profit industry organization that **oversees generation and transmission facilities and their control systems in the USA and Canada**."

Ex CIA Officer: Here's What Will Happen if Trump Doesn't Stop Scorning the CIA
Fortune, J.C. Carleson, 2016 12 19
Comment - As a novelist and screenwriter--someone who gets paid to entertain with my words--I can almost sympathize with President-elect Donald Trump's assessment that the **daily intelligence briefings the CIA keeps trying to foist on him might seem a bit dry and repetitive at times**. **Too much policy wonk and too little James Bond**, compliments of a team of analysts who do their work immune to the tyranny of page view metrics and click through rates. In a world where Breitbart headlines can create lurid stories out of thin air, the daily brief's stubborn reliance on facts and expert analysis might seem positively archaic. But I'm also a former CIA officer. From 2001 to 2011, I've worked on many of the issues that appear in those briefings, and I've traveled, lived, and worked in some of the places that pop up again and again, including Iraq and Afghanistan. More importantly, I have worked with many of the people who continue to quite literally risk their lives to obtain the information contained in those reports, whether or not Trump chooses to grant them an audience. And while we've heard a number of impassioned, highly persuasive pleas from senior- ranking intelligence and elected officials for Trump to reconsider his current brush-off of the CIA, I have not yet seen anyone address the issue on a more personal, individual level: the perspective of an actual spy on the ground. Note: J.C. Carleson is a former undercover CIA officer turned author.

Trump private security force 'playing with fire'
Politico, Kenneth Vogel, 2016 12 19
Grand Rapids - **President-elect Donald Trump has continued employing a private security and intelligence team at his victory rallies, and he is expected to keep at least some members of the team after he becomes president**, according to people familiar with the plans. The arrangement represents a major break from tradition. All modern presidents and presidents-elect have entrusted their personal security entirely to the Secret Service, and their event security mostly to local law enforcement, according to presidential security experts and Secret Service sources. But Trump -- who puts a premium on loyalty and has demonstrated great interest in having forceful security at his events -- has opted to maintain an aggressive and unprecedented private security force, **led by Keith Schiller, a retired New York City cop and Navy veteran who started working for Trump in 1999 as a part-time bodyguard, eventually rising to become his head of security**. Security officials warn that employing private security personnel heightens risks for the president-elect and his team, as well as for

protesters, dozens of whom have alleged racial profiling, undue force or aggression at the hands of Trump's security, with at least 10 joining a trio of lawsuits now pending against Trump, his campaign or its security.

Dismissing C.I.A. Findings Is an Insult to Hard-Working Intelligence Officers
New York Times (Room for Debate), Vicki Divoll, 2016 12 19
Comment - The **C.I.A. has concluded, with F.B.I. concurrence, that Russia engaged in a covert action operation to influence the 2016 election of the president of the United States. As you read this, awards are likely being bestowed on the Russian officers who designed and implemented one of the most important and successful operations in the history of their intelligence apparatus. So how has our president-elect reacted?** He has attacked the C.I.A. and dismissed its conclusions. He and his named national security adviser have angrily accused the agency of being incompetent and politically motivated. Trump darkly states, with no actual evidence of which we are aware, that the C.I.A. is wrong. We can only draw two possible conclusions from his bold assertions. Either he is willing to dismiss the work of the C.I.A., with no basis for doing so, because he is personally and politically embarrassed by their conclusions. Note: Vicki Divoll is a former C.I.A. assistant general counsel and former Senate Intelligence Committee general counsel.

Hussein, the C.I.A. and Me
New York Times, James Risen, 2016 12 19
Book Review - **Most C.I.A. memoirs are terrible -- defensive, jingoistic and worst of all, tedious. Others are doomed by the C.I.A.'s heavy-handed and mandatory censorship. There are exceptions, and that list includes the refreshingly candid "Debriefing the President: The Interrogation of Saddam Hussein" by John Nixon**. Mr. Nixon, the first C.I.A. officer to interrogate Hussein after his capture in December 2003, reveals gobsmacking facts about that deposed Iraqi leader that raise new questions about why the United States bothered to invade Iraq to oust him from power. These details will likely appall Americans who have watched their nation's blood and treasure wasted in Iraq ever since. More broadly, Mr. Nixon offers a stinging indictment of the C.I.A. and what he sees as the agency's dysfunctional process for providing intelligence to the president and other policy makers. The agency, he writes, is so eager to please the president -- any president -- that it will almost always give him the answers he wants to hear.

FBI agent quizzed over insider-trading-case leaks
Bloomberg News, 2016 12 18
Washington - An **FBI agent is under Justice Department scrutiny after federal prosecutors said they found "incontrovertible evidence" that he leaked confidential information about an insider-trading probe of Las Vegas gambler Billy Walters and golfer Phil Mickelson**. Walters, who was charged in May, has asked the judge in his case to determine whether prosecutors or FBI agents were behind the leaks published in news reports in 2014 and should be punished. While prosecutors initially said there was no leak, they reversed course Friday. The disclosure comes as the agency is under fire for its handling of an investigation into then-Democratic presidential candidate Hillary Clinton's use of a private email server. In a speech to donors **Thursday, Clinton said FBI Director James B. Comey's decision to disclose a fresh investigation of her emails less than two weeks before the election contributed to her defeat, according to a recording of the event obtained by the New York Times**. "The agent admitted that he disclosed confidential information about the investigation to the New York Times and Wall Street Journal reporters who wrote the articles," Assistant U.S. Attorney Joan Loughnane wrote to the judge about the Walters case. Jim Margolin, a spokesman for

Preet Bharara, the U.S. attorney for the Southern District of New York, declined to comment on the government's letter.

Henry Kissinger says "I hope we're doing some hacking" in Russia
Face the Nation (CBS), Rena Flores, 2016 12 18
Washington - **Former Secretary of State Henry Kissinger, responding to intelligence reports that Russia directed hacks to interfere with the U.S. election, is hoping that the American government is retaliating against the Kremlin with cyberattacks of its own.** "I don't doubt that the Russians are hacking us," Kissinger told CBS' "Face the Nation" in an interview that aired Sunday. "And I hope we're doing some hacking there." "Everybody has a hacking capability. And probably every intelligence service is hacking in the territory of other countries," he said. "But who exactly does what? That would be a very sensitive piece of information. But it's very difficult to communicate about it. Because nobody wants to admit the scope of what they're doing."

Priebus: Trump ready to accept Russia hacking report, if CIA, FBI get on same page
Fox News Sunday, Staff report, 2016 12 18
Washington - **Incoming White House Chief of Staff Reince Priebus suggested Sunday that President-elect Donald Trump will accept that Russia is behind the hacking of Democrats' email accounts during the 2016 White House race if the leaders of the U.S. intelligence community draft a report with that consensus agreement**. "I think he would accept the conclusion if they would get together, put out a report and show the American people they are on the same page," Priebus said on "Fox News Sunday." He suggested that the Trump team accepts CIA Director John Brennan's statement that Russia was involved. However, it remains wary about news media reports that **FBI Director James Comey** agrees. "Not when you have multiple people saying different things through third parties and media reports," Priebus told "Fox News Sunday." "It would be nice to hear from everybody."

Too much is labeled 'top secret'
Washington Post, Dianne Feinstein, 2016 12 18
OpEd: **We cannot expect to keep our nation's secrets secure - or provide meaningful oversight for our intelligence agencies - if proper classification of our country's secrets is as likely as a coin flip. Yet, according to the most recent review of classified documents by the Information Security Oversight Office (the office responsible for oversight of the government's classification system)**, improper classification markings were found on half of all classified documents. The rate was as high as 70 percent in certain agencies. That even seasoned national security professionals frequently fail to properly classify documents suggests that the system is broken. That's why the incoming administration must update its methods to protect classified national security information to reflect the realities of the digital era.

US 'got it so wrong' on Saddam Hussein, says CIA analyst who interrogated dictator
The Independent on Sunday (UK), Will Worley, 2016 12 18
Washington - **The US "got it wrong" about Saddam Hussein and Iraq, the CIA analyst who interrogated the former dictator has said. John Nixon** had numerous conversations with the deposed leader and now says that America was critically mistaken about their intervention Iraq in a number of ways. In particular, he claims, the CIA's view of Hussein's attitude to using chemical weapons was wrong. They were also mistaken about his health, personal habits and his involvement in running Iraq. Mr Nixon also criticised the conduct of George W Bush, under whose leadership America invaded Iraq, saying the former president heard "only what he wanted to hear" on the topic.

How a Putin Fan Overseas Pushed Pro-Trump Propaganda to Americans
New York Times, Mike McIntire, 2016 12 18
Washington - The **Patriot News Agency website popped up in July, soon after it became clear that Donald J. Trump would win the Republican presidential nomination**, bearing a logo of a red, white and blue eagle and the motto "Built by patriots, for patriots." Tucked away on a corner of the site, next to links for Twitter and YouTube, is a link to another social media platform that most Americans have never heard of: VKontakte, the Russian equivalent of Facebook. It is a clue that Patriot News, like **many sites that appeared out of nowhere and pumped out pro-Trump hoaxes tying his opponent Hillary Clinton to Satanism, pedophilia and other conspiracies, is actually run by foreigners based overseas**. But while most of those others seem be the work of young, apolitical opportunists cashing in on a conservative appetite for viral nonsense, operators of Patriot News had an explicitly partisan motivation: getting Mr. Trump elected. Patriot News -- whose postings were viewed and shared tens of thousands of times in the United States -- is among a constellation of websites run out of the United Kingdom that are linked to **James Dowson**, a far-right political activist who advocated Britain's exit from the European Union and is a fan of President Vladimir V. Putin of Russia. A vocal proponent of Christian nationalist, anti-immigrant movements in Europe, Mr. Dowson, 52, has spoken at a conference of far-right leaders in Russia and makes no secret of his hope that Mr. Trump will usher in an era of rapprochement with Mr. Putin. While it is easy to overstate the influence of fringe elements whose overall numbers remain very small, the explosion of **fake news** and propaganda sites and their possible impact on the presidential election have ignited alarm across the American political spectrum.

Trump national security pick Monica Crowley repeatedly pushed conspiracy theory about Clinton aide
CNN.com, 2016 12 17
Washington - **Fox News analyst Monica Crowley, Donald Trump's pick to be senior director of strategic communications for the National Security Council, repeatedly pushed an unfounded conspiracy theory that claimed Hillary Clinton's aide Huma Abedin has ties to Islamic extremists**. The claim, which circulated among far-right websites, has been labeled as false and unfounded by fact-checkers from the Washington Post, Politifact, and Snopes. Claims Abedin was tied to the Muslim Brotherhood are based on flimsy connections tying together people and events from decades ago. An email seeking comment sent to a Trump transition spokesperson, Trump national security adviser Michael Flynn, and Crowley was not immediately returned. In a 2013 exchange on Fox News's "Hannity," Crowley responded to another panelist who claimed ties between Abedin and the Muslim brotherhood by saying, "That's the real Huma Abedin story. It's not about Weiner's Weiner. It's about Huma Abedin and her ties to Islamic extremists."

What Was James Comey Thinking?
Esquire Magazine, Tim Weiner, 2016 12 17
Analysis: As the United States attorney for the Southern District of New York, **James B. Comey gave a speech to every new prosecutor he hired. Founded in 1789, the Southern District is the most prestigious post in the Justice Department outside Washington**. Wall Street titans and crooked politicians go down to the federal courthouse in lower Manhattan, they go on trial, and they go to prison. The power of a prosecutor is awesome, as Comey well knew. (There's a reason that the statue of Justice holds a sword along with a scale.) He told the young hotshot lawyers who were joining his team that when they stood up in court and proclaimed, "'I represent the United States of America,' people believe the next thing you say."..**Comey's reputation for integrity and independence led Barack Obama to make him the seventh**

FBI director in the nation's history. He was sworn in on September 4, 2013. Three years later, the man known as the straightest of straight shooters shot himself in the foot. The ricocheting bullet scarred his reputation, wounded the American body politic, and lodged in the heart of Hillary Clinton's presidential campaign. **On July 5, 2016, Comey sent an email from the J. Edgar Hoover Building in Washington to every FBI agent in the world. "I am about to walk downstairs to deliver a statement to the media about our investigation of Secretary Clinton's use of a personal email server during her time as Secretary of State,"** he said. He was going to "provide more detail about our process" than was usual, and he was doing so to satisfy the public's interest....If **he serves through the end of his statutory term, Comey will rise before dawn, read through overnight reports about threats to the United States, ride a black car to the White House, and brief the president, if the president will listen. He will report to congressional committees on life-and-death issues of national security**. The FBI is fighting battles across the nation and the world, surrounded by real and imagined enemies everywhere you look, and in places you can't see. There are terrorists and cyberwarriors. There are crooks and thieves. There are two houses of Congress. And then there's the White House. Our new president has a history of bending the law nearly to the breaking point. Trump might not like the cut of Jim Comey's jib. **But the FBI director must stand up and say no to a president when the Constitution requires it. It's the law, and it's a tradition. We could do worse than having Comey in charge.**

Obama Says He Told Putin: 'Cut It Out' on Hacking
New York Times, Mark Landler and David E Sanger, 2016 12 17
Washington - **President Obama said for the first time on Friday that he had held back before Election Day from retaliating against Russia for meddling in the presidential race for fear of inciting further hacking** "that could hamper vote counting." But he said he was weighing a mix of public and covert actions against the Russians in his last 34 days in office, actions that would increase "the costs for them." Mr. Obama said he was committed to sending the Kremlin a message that "we can do stuff to you," but without setting off an escalating cyberconflict.

FBI agrees with CIA that Russia aimed to help Trump win
Washington Post, Ellen Nakashima & Adam Entous, 2016 12 17
Washington - **FBI Director James B. Comey and Director of National Intelligence James R. Clapper Jr. are in agreement with a CIA assessment that Russia intervened in the 2016 election in part to help Donald Trump win the White House**, officials disclosed Friday, as President Obama issued a public warning to Moscow that it could face retaliation. New **revelations about Comey's position could put to rest suggestions by some lawmakers that the CIA and the FBI weren't on the same page on Russian President Vladimir Putin's intentions.** Russia has denied being behind the cyber-intrusions, which targeted the Democratic National Committee and the private emails of Hillary Clinton's campaign chairman, John Podesta. Trump, in turn, has repeatedly said he doubts the veracity of U.S. intelligence blaming Moscow for the hacks. "I think it's ridiculous," Trump said in an interview with "Fox News Sunday," his first Sunday news-show appearance since the Nov. 8 election. "I think it's just another excuse. I don't believe it. ... No, I don't believe it at all." At a "thank you" event Thursday night with some of her top campaign donors and fundraisers, Clinton said she believed Russian- backed hackers went after her campaign because of a personal grudge that Putin had against her. "Earlier this week, I met separately with FBI [Director] James Comey and **DNI Jim Clapper**, and there is strong consensus among us on the scope, nature, and intent of Russian interference in our presidential election," Brennan said, according to U.S. officials who have seen the message.

RNC Security Foiled Russian Hackers
Wall Street Journal, Julian E. Barnes, Devlin Barrett, 2016 12 16
New York - **Russian hackers tried to penetrate the computer networks of the Republican National Committee, using the same techniques that allowed them to infiltrate its Democratic counterpart, according to U.S. officials who have been briefed on the attempted intrusion.** But the intruders failed to get past security defenses on the RNC's computer networks, the officials said. And people close to the investigation said it indicated a less aggressive and much less persistent effort by **Russian intelligence** to hack the Republican group than the Democratic National Committee. Only a single email account linked to a long-departed RNC staffer was targeted. The disclosures came as a political furor grows over suspected Russian hacking of U.S. political organizations. The **Central Intelligence Agency has concluded that Russian hackers, whom analysts say work for that country's military and intelligence apparatus**, stole emails from the DNC, as well as another Democratic organization and the chairman of Hillary Clinton's presidential campaign, to harm her candidacy and boost Republican Donald Trump's chances of winning. Russia has denied the allegations. The possibility that Russians tried and failed to infiltrate the RNC doesn't necessarily conflict with the CIA's conclusion.

Russian hack almost brought the U.S. military to its knees
CBS News, David Martin, 2016 12 16
Washington - **Russian hackers struck at the heart of the U.S. military in August 2015 by seizing the e-mail system used by the Joint Chiefs of Staff, CBS News has learned**. Then-**Chairman of the Joint Chiefs Martin Dempsey was alerted to the attack by an early-morning phone call from the Director of the National Security Agency, Admiral Mike Rogers**. Now retired, Dempsey told CBS News in an exclusive interview that the attack was proceeding at an alarming speed. Within an hour, hackers had seized control of the unclassified e-mail system used by the Pentagon's Joint Staff, the organization of some 3,500 military officers and civilians who work for the Chairman. The attack, which officials now blame on Russia, began with 30,000 e-mails sent to a West Coast university. Of those 30,000, four were forwarded to members of the Joint Staff and one was opened -- allowing the hackers in. Since it was an unclassified network, the attack had no real intelligence value..

Something is broken at the FBI
Washington Post, John Podesta, 2016 12 16
Op-ed - **The more we learn about the Russian plot to sabotage Hillary Clinton's campaign and elect Donald Trump, and the failure of the FBI to adequately respond, the more shocking it gets**. The former acting director of the CIA has called the Russian cyberattack "the political equivalent of 9/11." Just as after the real 9/11, we need a robust, independent investigation into what went wrong inside the government and how to better protect our country in the future. As the former chair of the Clinton campaign and a direct target of Russian hacking, I understand just how serious this is. So I was surprised to read in the New York Times that when **the FBI discovered the Russian attack in September 2015**, it failed to send even a single agent to warn senior Democratic National Committee officials. Instead, messages were left with the DNC IT "help desk." As a former head of the FBI cyber division told the Times, this is a baffling decision: "We are not talking about an office that is in the middle of the woods of Montana." What takes this from baffling to downright infuriating is that at nearly the exact same time that no one at the FBI could be bothered to drive 10 minutes to raise the alarm at DNC headquarters, two agents accompanied by attorneys from the Justice Department were in Denver visiting a tech firm that had helped maintain Clinton's email server. This trip was part of what **FBI Director James B. Comey** described as a "painstaking" investigation of Clinton's emails, "requiring thousands of hours of effort" from dozens of agents who conducted at least

80 interviews and reviewed thousands of pages of documents. Note: John Podesta served as chair of Hillary Clinton's presidential campaign.

Trump's Dispute With CIA Puts Pompeo in a Bind
Roll Call, Ryan Lucas, 2016 12 16
Washington - In the **extraordinary public dispute between Donald Trump and the CIA, one man finds himself in a particularly tricky position: the president-elect's nominee to lead the agency, Rep. Mike Pompeo.** The tea party Republican from Kansas, who is expected to win Senate confirmation, **will have to repair a relationship between Trump and the CIA that has been battered by the president-elect's repeated disparagement of the agency's capabilities and competence.** "I think that we've never quite seen a moment like this in agency history where an incoming president was so openly critical and questioning of the agency's integrity," said Dennis Wilder, a former senior CIA official who retired this year. **John McLaughlin**, a **former deputy director and acting director of the CIA, said Pompeo should focus on the basics to win the agency's trust and confidence**. "All a CIA director needs to do to succeed is to approach the issues dispassionately, make sure all the evidence is taken into account, lay out what is actually known, what is less certain, and what conclusions logically come out of that," McLaughlin said in an email.

Trump in Denial as Evidence Grows Spymaster Putin Behind Election Hacks
ABC News, Multiple reporters, 2016 12 16
New York - **With intelligence officials convinced that Russian spook-turned-president Vladimir Putin personally directed cyber-attacks aimed at interfering with the U.S. election, President-elect Donald Trump continues to downplay and dismiss growing hacking concerns as politically motivated**. The hacks saw the systems and accounts of political organizations and figures like the Democratic National Committee breached, and private data - in the most notable cases, emails - spilled out into public view. "The primary goal of this attack on our election system was to sow chaos and apparently to help the candidate Donald Trump," Matt Olsen, an ABC News consultant and the former director of the National Counterterrorism Center, said. But Trump is having none of it. **"If Russia, or some other entity, was hacking, why did the White House wait so long to act?" Trump tweeted on Thursday. "Why did they only complain after Hillary lost?"**

Where is Trump getting his cybersecurity advice?
Christian Science Monitor, Aliya Sternstein, 2016 12 15
Washington - **Amid the growing controversy over intelligence reports that Russian hackers meddled in US elections to aid Donald Trump's campaign, it's unclear who the president-elect is listening to on matters of cybersecurity right** now. **Michael Flynn** may have the most sway over the president-elect on issues of cybersecurity. He's a member of Trump's transition team and the president-elect's incoming national security adviser. Among the people around Trump, the retired Army lieutenant general and former Defense Intelligence Agency head may be the most knowledgeable when it comes to the current state of digital espionage and how a country such as Russia operates in cyberspace. **"It appears that Gen. Flynn, his advice to the president, specifically about cybersecurity will probably be taken very seriously," says Dale Meyerrose, a retired Air Force major general**, who knows Flynn and served in the Bush administration as the first- ever intelligence community chief information officer. Flynn's expertise and association with cybersecurity issues stretches back more than a decade, back to when he was in uniform, says Mr. Meyerrose.

Why Didn't Obama Do More About Russian Election Hack?
NBC News, Multiple reporters, 2016 12 16

New York - The **Obama administration didn't respond more forcefully to Russian hacking before the presidential election because they didn't want to appear to be interfering in the election and they thought that Hillary Clinton was going to win and a potential cyber war with Russia wasn't worth it,** multiple high-level government officials told NBC News. "They thought she was going to win, so they were willing to kick the can down the road," said one U.S official familiar with the level of Russian hacking. The administration did take action in response to the hack prior to the election. In September, President Obama privately confronted Vladimir Putin about the hacks at the G-20 summit in China.

Obama On Russian Hacking: 'We Need To Take Action. And We Will'
NPR Morning Edition, Scott Detrow, 2016 12 16
Washington - **President Obama says the United States will respond to Russian cyberattacks that the intelligence community has concluded were part of an effort to influence the 2016 presidential election**. In an interview with NPR's Steve Inskeep that will air Friday on Morning Edition, Obama said, "I **think there is no doubt that when any foreign government tries to impact the integrity of our elections ... we need to take action**. And we will -- at a time and place of our own choosing. Some of it may be explicit and publicized; some of it may not be." With the question of Russia's ultimate motivation for the hack becoming increasingly divisive, Obama was careful to not endorse a CIA assessment, reported by NPR and other news outlets, that asserts that Russia's goal was to elect Trump. "There are still a whole range of assessments taking place among the agencies," **Obama told NPR, referring to an order he has given the U.S. intelligence community to conduct a full review of the cyberattacks before Inauguration Day**.

Kremlin Calls NBC Report Putin Directed Hack 'Laughable Nonsense'
NBC News, Ken Dilanian, 2016 12 15
New York - The **Kremlin on Thursday disputed an exclusive NBC News report that U.S. intelligence has documented Vladimir Putin's personal involvement in a Russian intelligence operation to interfere in the U.S. presidential election**. Putin spokesman **Dmitry Peskov told the AP the report was "laughable nonsense."** Maria Zakharova, a spokeswoman for the Russian Foreign Ministry, accused "Western media" of being a "shill" and a "mouthpiece of various power groups." NBC News reported Wednesday that the U.S. has information that Putin personally directed how material hacked by Russian intelligence agencies was used during the campaign. Anthony Scaramucci, a senior Trump transition team official, did not dispute Russia's involvement in an interview Thursday night with MSNBC's Brian Williams. "I don't think anybody thinks that you're wrong," he said of the NBC News report. "Our position right now is that we're waiting for more information...we reject the notion that people would cyberattack our institutions...We are very upset about it."

Afraid to Politicize Intelligence, Obama Delayed Blaming Russia for Hack
New York Times, Gardiner Harris, 2016 12 15
Washington - The **Obama administration spent months deliberating whether to blame Russia for a cyberattack on the Democratic National Committee, with action delayed in part because President Obama did not want to be blamed for politicizing intelligence**, the White House said on Wednesday. **Josh Earnest**, the White House press secretary, said that "it would've been inappropriate for White House figures -- including the president of the United States -- to be rushing the intelligence community to expedite their analysis of the situation." In particular, he described White House concerns that any statement by Mr. Obama would be viewed as using intelligence to meddle in the election on behalf of the president's preferred candidate, Hillary Clinton.

Comey to Trump: The Russians Didn't Influence the Election
Town Hall, Ed Klein, 2016 12 15
Washington - In **telephone conversations with Donald Trump, FBI Director James Comey assured the president-elect there was no credible evidence that Russia influenced the outcome of the recent U.S. presidential election by hacking the Democratic National Committee and the e-mails of John Podesta, the chairman of Hillary Clinton's presidential campaign**. What's more, Comey told Trump that **James Clapper**, the director of National Intelligence, agreed with this FBI assessment. The **only member of the U.S. intelligence community who was ready to assert that the Russians sanctioned the hacking was John Brennan, the director of the CIA**, according to sources who were briefed on Comey's conversations with Trump. "And Brennan takes his marching orders from President Obama," the sources quoted Comey as saying.

Donald Trump risks damaging intelligence agencies, warns former CIA chief
The Guardian (London), Julian Borger, 2016 12 15
Washington - **Donald Trump's public disparagement of US intelligence agencies would have a discouraging effort on the country's spies and undermine the moral authority of their leaders to send them "into harm's way",** a former CIA director said on Wednesday **Michael Hayden**, who served as both director of the CIA and NSA in the George W Bush administration, entered the growing controversy over the president-elect's attitude towards the US intelligence community, questioning its conclusion that Russia had hacked the Democratic National Committee and the CIA's finding that Moscow had meddled in the presidential election in Trump's favour. It also emerged that Trump had only met intelligence officials to receive what is normally a daily briefing, four times since the election. "I get it when I need it," he said. **An aide said on Wednesday that he would from now on receive a presidential daily brief three times a week instead of just once.** Hayden said that missing the daily briefing would be discouraging "but may not be catastrophic" if he was well briefed by top aides.

Intel agencies reject request for House committee briefing, citing larger probe
The Hill, Katie Bo Williams, 2016 12 15
Washington - The **Intelligence Community (IC) is refusing to provide the House Intelligence Committee with a requested Thursday briefing on Russian interference with the U.S. election, citing an ongoing review of the matter requested by President Obama**. According to a statement, the IC will not be offering comment to Congress until it completes that review, which will cover foreign interference in the electoral process since 2008. **"Once the review is complete in the coming weeks, the Intelligence Community stands ready to brief Congress -- and will make those findings available to the public consistent with protecting intelligence sources and methods," the Office of the Director of National Intelligence (ODNI) said in a statement.** The Obama review is scheduled to be completed by the time Donald Trump takes office on Jan. 20. Chairman Devin Nunes (R-Calif.) had asked the FBI, NSA, Office of the Director of National Intelligence and CIA to meet with committee members on Thursday, and called their refusal "unacceptable.".

James Clapper Has a Classified Blog. It's Called "Intercept."
The Intercept, Jeremy Scahill, 2016 12 15
Washington - **During his tenure as the Director of National Intelligence, James Clapper has maintained a classified blog. It's called "Intercept," and is only accessible to people within the intelligence community with clearance to access the government intelink site. It even offers a secret RSS feed so analysts will never miss a post**. Clapper's Intercept blog has no relationship to The Intercept, except that he hates pretty much everything we stand for. In one of his posts, written in May 2013 and obtained by The Intercept, Clapper posted a

handwritten letter he says he received from "a constituent in Nevada." It's unclear what makes this person a constituent since Clapper was not elected to any office. In any case, this constituent "discusses supporting the IC's [Intelligence Community's] position on civil liberties" in the aftermath of the Boston Marathon bombing. "If the american [sic] people are not willing to release some freedoms, they cannot blame the IC when they can't stop" domestic terror attacks because of the intelligence agencies "having their hands tied by Law [sic] & policy," the "constituent" wrote. He adds that Americans "cannot have your cake and eat it too," and then offers what has become a dangerous cliche in the post-Snowden mentality of the intelligence community: "So if one has nothing to hide why would a little government watching for mass protection be such a big question." The letter ends: "WE SUPPORT YOU."

Stolen Yahoo Data Includes Government Employee Information
Bloomberg News, Jordan Robertson, 2016 12 15
New York - **More than 150,000 U.S. government and military employees are among the victims of Yahoo! Inc.'s newly disclosed data breach, and their names, passwords, telephone numbers, security questions, birth dates, and backup e-mail addresses are now in the hands of cybercriminals**. It's a **leak that could allow foreign intelligence services to identify employees and hack their personal and work accounts, posing a threat to national security**. These employees had given their official government accounts to Yahoo in case they were ever locked out of their e- mail. The government accounts belong to current and former White House staff, U.S. congressmen and their aides, FBI agents, officials at the **National Security Agency, the Central Intelligence Agency, the Office of the Director of National Intelligence**, and each branch of the U.S. military. The list includes an FBI division chief and multiple special agents working around the U.S.; current and former diplomats in Pakistan, Syria and South Africa; a network administrator at NSA's Fort Meade headquarters; the chief of an Air Force intelligence group; and a human resources manager for the CIA. On Wednesday, Yahoo revealed the second major breach of its systems, following the September disclosure of a widespread hack.

U.S. Officials: Putin Personally Involved in U.S. Election Hack
NBC News, Multiple reporters, 2016 12 15
New York - **U.S. intelligence officials now believe with "a high level of confidence" that Russian President Vladimir Putin became personally involved in the covert Russian campaign to interfere in the U.S. presidential election,** senior U.S. intelligence officials told NBC News. Two senior officials with direct access to the information say new intelligence shows that Putin personally directed how hacked material from Democrats was leaked and otherwise used. The intelligence came from diplomatic sources and spies working for U.S. allies, the officials said. **Putin's objectives were multifaceted, a high-level intelligence source told NBC News.** What began as a "vendetta" against Hillary Clinton morphed into an effort to show corruption in American politics and to "split off key American allies by creating the image that [other countries] couldn't depend on the U.S. to be a credible global leader anymore," the official said.

Trump's national security adviser shared secrets without permission, files show
Washington Post, Craig Whitlock, Greg Miller, 2016 12 14
Washington - A **secret U.S. military investigation in 2010 determined that Michael T. Flynn, the retired Army general tapped to serve as national security adviser in the Trump White House, "inappropriately shared" classified information with foreign military officers in Afghanistan,** newly released documents show. **Although Flynn lacked authorization to share the classified material, he was not disciplined or reprimanded** after the investigation concluded that he did not act "knowingly" and that "there was no actual or potential damage to

national security as a result," according to Army records obtained by The Washington Post under the **Freedom of Information Act**. Flynn has previously acknowledged that he was investigated while serving as the U.S. military intelligence chief in Afghanistan for sharing secrets with British and Australian allies there. But he has dismissed the case as insignificant and has given few details.

Newly Uncovered Site Suggests NSA Exploits for Direct Sale
Motherboard (Vice), Joseph Cox, 2016 12 14
New York - The **Shadow Brokers--a hacker or group of hackers that stole computer exploits from the National Security Agency--has been quiet for some time**. After their auction and crowd-funded approach for selling the exploits met a lukewarm reception, the group seemingly stopped posting new messages in October. But a **newly uncovered website**, which includes a file apparently signed with The Shadow Brokers' cryptographic key, **suggests the group is trying to sell hacking tools directly to buyers one by one, and a cache of files appears to include more information on specific exploits**.

Past CIA director, British premier say Trump needs spy data
Associated Press, Staff report, 2016 12 14
Dubai - A **former CIA director and a former British prime minister offered simple advice on Wednesday for U.S. President-elect Donald Trump: Have daily intelligence briefings**. Both **Leon Panetta**, a former American spymaster and defense secretary, and Britain's former Prime Minister **David Cameron emphasized the point after Trump suggested he didn't need them.** "I have never seen a president who has said, 'I don't want that stuff.' Never seen it," Panetta said at the Arab Strategy Forum in Dubai. Cameron said: "It won't last." Panetta added: "It can't last."

Harry Reid Says Electors Should Have Intelligence Briefing
BuzzFeed News, Ben Smith, 2016 12 14
Washington - **Sen. Harry Reid told BuzzFeed News Tuesday that members of the Electoral College should receive an intelligence briefing on Russian interference in the US election before they vote on Dec. 19.** The Senate's minority leader was interviewed at a BuzzFeed Brews event, where the retiring Nevada lawmaker also reflected on the state of the US Senate. "I think this is as big a deal as Watergate, as 9/11. I think they should have a 9/11-type commission. I know that [US Sens.] Dianne Feinstein and Ben Cardin and others are calling for that. I think it's a step in the right direction," Reid said.

Trump's hostility to intelligence community enters the spotlight
The Hill, Katie Bo Williams, Julian Hattem, 2016 12 14
Washington - **Donald Trump's hostile approach to the critically important relationship between the White House and the U.S. intelligence community is unnerving officials and national security scholars**. The president-elect has signaled that he intends to treat intelligence with little attention to precedent. Former officials are concerned that the agencies on which Trump will rely to give him a decisionmaking advantage simply won't trust the president-elect -- with dire consequences. **"Intelligence officials are always worried about whether the president will have their back, particularly when the world they operate in is dangerous," said Amy Zegart, a co-director of the Center for International Security and Cooperation at Stanford University who studies the intelligence community. "This president is now knifing them from the front."**

Trump Feud Over Russia Intel Raises Deeper Concerns, Experts Say
NBC News, Benjy Sarlin, 2016 12 14

New York - **President-elect Donald Trump's ongoing feud with U.S. intelligence agencies over alleged hacking by Russia is unnerving outside national security experts, some of whom fear the frosty relationship could impact Trump's ability to govern**. Of course Trump -- who said in August the intelligence community's performance has been "catastrophic" -- wouldn't be the first president to have a strained relationship with his own agencies. But what separates Trump, some experts say, is his unusually harsh public criticism of the intelligence community's basic worth and and a lack of clarity on how he plans to gather facts if he refuses their counsel. "No presidents have been perfectly happy with intelligence assessments because intelligence assessments often bring bad news," **David Priess, author of "The President's Book of Secrets" and a former CIA officer and daily briefer to President George W. Bush**, told NBC News. "

Trump is playing a risky spy game
Washington Post, David Ignatius, 2016 12 14
Column - **Intelligence officers like to distinguish between knowable secrets that spies can steal and fuzzier mysteries that have to be assessed without final, definitive proof**. The intent of Russia's covert meddling in the 2016 U.S. presidential election is probably somewhere between the two. But after conversations with a half-dozen knowledgeable sources, here are two simple judgments: Russia's secret hacking against Democratic Party officials threatened the integrity of the U.S. political system. And President-elect Donald Trump shouldn't have criticized the CIA after its analysts told Congress about the Kremlin's efforts. Trump, unbelievably, seemed to be taking a potential adversary's side against his own nation's intelligence professionals. The evidence that led CIA analysts to conclude that Moscow's aim in 2016 was to help Trump -- rather than simply spread confusion -- was based on a variety of sources. One indication was that the Russians didn't disseminate information from their snooping into Republican files, as they had with the product of hacking against Democrats; the Russians also didn't disseminate material after Trump's victory. ...**Perhaps the trickiest task will fall to Rep. Mike Pompeo (R-Kan.), Trump's nominee to head the CIA**. He must reassure a battered agency workforce that the next administration values its own intelligence officers and is vigilant against machinations by foreign spies.

Former CIA Analyst: Russian Hacking Allegations of US Election Don't Add Up
Sputnik, Staff report, 2016 12 13
Moscow - The **Central Intelligence Agency has claimed that Russia interfered in the US election to help President-elect Donald Trump win, but one of their former officers has detailed why the agency's claims do not add up**. Speaking to Brian Becker on Sputnik Radio's Loud & Clear program, **former CIA analyst Ray McGovern asserted that it appears that the email releases from the Democratic Party are not hacks, but leaks**. "Today they are talking about having 'overwhelming circumstantial evidence.' Now we have overwhelming technical evidence. We have the former technical director of the National Security Agency that tells us that this is really just drivel," McGovern said of Bill Binney, a former highly-placed intelligence official with the NSA, turned whistleblower.

The Perfect Weapon: How Russian Cyberpower Invaded the U.S.
New York Times, Multiple reporters, 2016 12 13
Washington - When **Special Agent Adrian Hawkins of the Federal Bureau of Investigation** called the Democratic National Committee in September 2015 to pass along some troubling news about its computer network, he was transferred, naturally, to the help desk. His message was brief, if alarming. At least **one computer system belonging to the D.N.C. had been compromised by hackers federal investigators had named "the Dukes," a cyberespionage team linked to the Russian government.** It was the cryptic first sign of a

cyberespionage and information-warfare campaign devised to disrupt the 2016 presidential election, the first such attempt by a foreign power in American history. What started as an information-gathering operation, intelligence officials believe, ultimately morphed into an effort to harm one candidate, Hillary Clinton, and tip the election to her opponent, Donald J. Trump. Like another famous American election scandal, it started with a break-in at the D.N.C.

Return to Table of Contents/ Retour à la table des matières

United Kingdom / Royaume-Uni

GCHQ asked to step up action against cyber-attack threat to financial services
The Guardian (London), Jill Treanor, 2016 12 19
London - **More action may be needed to protect the financial services industry from a devastating cyber-attack**, the head of the Treasure select committee has suggested. Andrew Tyrie MP wrote to **Ciaran Martin, head of the new cybersecurity centre of UK surveillance agency GCHQ, saying the lines of responsibility and accountability for reducing cyber-threats are opaque.** Tyrie's letter to Martin, who is leading the Cheltenham-based National Cyber Security Centre (NCSC), uses last month's incident at Tesco Bank to illustrate the vulnerabilities of the financial system. In November, the banking arm of supermarket chain Tesco admitted that £2.5m had been stolen from 9,000 accounts in an incident which raised fresh concerns about the methods used by financial services firms to detect cyber-attacks.

'I was a Russian spy. So what?' Former double agent says Britain does work with Kremlin amid Cambridge concerns
London Daily Telegraph, Lydia Willgress, 2016 12 19
London - **It is a question that has rocked the academic world in Cambridge; are Russians trying to infiltrate the town's seminars on intelligence?** The whispers of espionage and double bluffs have reportedly been enough to make three experts resign from their positions as conveners of the academic forum - with many more arguing over the alleged links. But the public and academics need to move away from "the old John le Carré days" because in certain areas British and Russian intelligence services collaborate, a Cambridge academic and former double agent has now claimed. **Dr David Gosling, who worked as a spy for the Russians in the 1990s, told The Daily Telegraph** that it did not matter if operatives were targeting the **Cambridge Intelligence Seminar (CIS)** as the Russians often used "clandestine methods" to gain information that was not significant or secret. He insisted he had seen no evidence of proceedings or funding being influenced, and added that academics should be more worried about the Chinese attempting to infiltrate university labs. His comments came after Sir Richard Dearlove, the former MI6 chief, Stefan Halper, a former policy adviser at the White House, and leading espionage history Peter Martland all allegedly resigned from their positions amid concerns about Kremlin-backed funding.

MI5 'offered £30,000' to terror suspect
Sunday Times (UK), Tom Harper, 2016 12 18
London - A **businessman on trial for an alleged terror offence worked for MI5 and recorded an intelligence officer offering him £30,000 to spy for the British government**, a court was told last week. **Pervez Rafiq** is accused of taking part in a plot to smuggle money to jihadists in Syria using charity aid convoys. He denies arranging funds or property for the purposes of terrorism. His lawyer, Hossein Zahir, told the Old Bailey in London that Rafiq, 46,

from Birkby, Huddersfield, West Yorkshire, recorded a conversation with an MI5 officer called "Ben" after he was found guilty of a minor fraud in July 2013. Zahir told the jury: "MI5 jumped on this [the conviction]. Work with us and we will pay you ... Ben is offering him £30,000. Why would MI5 offer a man who is funding terrorism £30,000?" He said a transcript of the conversation also showed Ben advising Rafiq to get his lawyer to raise his previous co-operation with the authorities before he was sentenced.

Undercover SAS troops will be deployed to protect Christmas shoppers and New Year's Eve revellers against ISIS as hundreds of fighters return home to the UK
The Daily Mail Online, Rory Tingle, 2016 12 18
London- **SAS anti-terror troops will mingle with Christmas shoppers and New Year's Eve revellers to counter the threat from returning ISIS fighters**. Elite troopers will operate undercover in major British cities including London, Birmingham, Manchester and Leeds. They will work closely with **MI5 intelligence officers** to identify terror suspects, while Army bomb disposal experts will also be on hand to deal with suspicious devices. Expert snipers trained to kill suicide bombers moving through crowds will also be on hand to boost security. A source told the Star: 'MI5 believes hundreds of Britons who fought with Islamic State in Syria and Iraq will be returning to the UK in the next few months.

Cambridge spy forum splits over Moscow
London Times, George Sandeman, 2016 12 17
London - A **former head of MI6 is among a group of intelligence experts who have stepped down from their roles at a Cambridge University forum over fears of Kremlin influence**. **Sir Richard Dearlove**, the former head of the Secret Intelligence Service, was one of several academics who convened the **Cambridge Intelligence Seminar** -- a forum that brings together former practitioners and researchers of western spycraft. Stefan Halper, a senior foreign policy adviser who served in the White House during three Republican presidencies, and Peter Martland, a leading espionage historian, have joined Sir Richard in relinquishing their positions because of concerns regarding what they believe to be a Kremlin-backed operation to compromise the group, according to the Financial Times. The Cambridge Intelligence Seminar was established by Christopher Andrew, the official historian of MI5 and former chairman of the history faculty at the university. **Recent guests at its discussions include Mike Flynn, Donald Trump's choice as US national security adviser.**

Ex-MI6 boss 'leaves Cambridge over Russia'
Daily Telegraph (Australia), Lydia Willgress, 2016 12 17
London - The **former head of MI6 is one of three intelligence experts who have cut ties with Cambridge spy seminars amid claims about Russian funding. Sir Richard Dearlove**, who was head of the British secret service for five years from 1999, is believed to have resigned as convener of the **Cambridge Intelligence Seminar (CIS),** alongside Stefan Halper, a former policy adviser at the White House, and historian Peter Martland. Mr Halper reportedly said his decision to step down was due to "unacceptable Russian influence" on the group, which holds Friday seminars at Corpus Christi college. It comes after suspicions were raised that a new digital publishing house, Veruscript, which will help cover some CIS costs, may be linked to Russian intelligence services, the Financial Times reported.

German spies 'can't be trusted'
Daily Mail (UK), Allan Hall, Ian Drury, 2016 12 16
Berlin - **Relations between British and German spy chiefs have hit rock bottom because London says its counterparts in Berlin cannot be trusted to keep** secrets. At a time of escalating Islamic terror threats across Europe, **Germany's spy agency BND is being frozen**

out by GCHQ and the National Security Agency in the US. Both London and Washington believe insecure German data servers have contributed to the leaking of tens of thousands of classified documents to Wikileaks. And they have infuriated Berlin by refusing to hand over secret intelligence data demanded by left wing and Green politicians which they fear will be aired in the German parliament. It is understood that in November 2014 there was a meeting in Berlin between **Sir Simon McDonald**, the then British ambassador to Germany, together with Patrick **McGuinness, Deputy National Security Adviser for Intelligence, Security, and Resilience at the Cabinet Office,** and high security officials in Angela Merkel's government. The British made it plain at the meeting that co-operation between Britain and Germany was becoming increasingly problematic because of leaks. A source familiar with the meeting said: 'They stressed that a secret service is just that and that its workings and operations must remain secret and they felt that Germany was leaking them like a sieve." Britain fears a 'big debate' in the German parliament which would lay open secret sources and intelligence gathering techniques.

Police used spying powers 'unlawfully' to track down leaks
London Times, Fiona Hamilton, 2016 12 16
London - A **police force unlawfully spied on a string of journalists, a solicitor and two police officers** in an attempt to uncover leaks including the existence of a damning racism report, a tribunal has heard. Cleveland police used wide-ranging surveillance powers to trawl through four months of billing and call data related to five people, including a national newspaper journalist who had nothing to do with any of the leaks.

Return to Table of Contents/ Retour à la table des matières

Australia / Australie

ASIO spies infiltrate jihadist terror cells
The Australian, Paul Maley, 2016 12 19
Canberra - **Australia's domestic spy agency is running secret operations against Islamic State, inserting covert operatives into terrorist cells in a bid to thwart domestic attacks**. The Australian understands **ASIO has begun running a small number of so-called "special - intelligence operations"** as part of a broader push by police and security agencies to make full use of new far-reaching powers that have been codified in successive waves of national security legislation reform. Before the passage of the new laws, ASIO operatives could be vulnerable to prosecution for engaging in such operations. Since September 2014, the government has passed eight separate tranches of national security legislation that have either amended existing offences, created new ones or extended far- reaching surveillance, arrest and control powers to security agencies. Beyond secret intelligence operations, figures from the **Australian Federal Police** show police have arrested more than 40 suspected terrorists under changes to the law that lower the threshold for arrest in terrorism cases. Australian Federal Police and South Australian Police detectives on Thursday charged an Adelaide man for advocating terrorism after the 50-year-old allegedly uploaded extremist videos to social media. It was the first such case of its kind and **AFP Commissioner Andrew Colvin** said the creation of the offence had had a demonstrable effect on the level of extremist rhetoric in the community.

Debate grows over role of US-Australia intel facility
Straits Times, 2016 12 18

Canberra - In the Australian outback, a strange series of dome structures and vast antennas has protruded from the flat desert landscape for almost 50 years, but it remains shrouded in secrecy. The site, just outside the city of Alice Springs, is the **Joint Defence Facility Pine Gap, a United States-Australian intelligence facility which was built during the Cold War in the 1960s, and has since been used - according to analysts - to monitor Chinese and Russian missiles, eavesdrop on the Islamic State in Iraq and Syria (ISIS)** and order drone strikes in Pakistan. Pine Gap would provide the first signal to the US of a nuclear attack and is regarded as one of the most important US intelligence facilities outside its territory. The 20,000 sq km site employs about 800 people, roughly half are Americans and the rest Australians. Despite the **secrecy surrounding the facility**, analysts believe it continues to expand, and its role in intercepting signals intelligence has become ever more extensive in the age of mobile phone interception and drone attacks.

Return to Table of Contents/ Retour à la table des matières

New Zealand / Nouvelle-Zélande

Blunder hits security of NZ spy base
New Zealand Herald, David Fisher, 2016 12 17
Wellington - **Details of the construction of the top secret spy base at Tangimoana were filed with Archives New Zealand with no security rating, allowing the contents of the file to be copied**. The Archives NZ file which contains the details has now had access restricted for 100 years after the Weekend Herald told the **Government Communications Security Bureau** it had a copy. The construction file included details about the security system protecting the spy base. The Weekend Herald came across the file and other GCSB information while reviewing files about the security services held by Archives NZ, the national repository for public records. Built in the early 1980s, Tangimoana, 30km west of Palmerston North, was a signals link for Western powers during the Cold War.

Return to Table of Contents/ Retour à la table des matières

International

China / Chine

Respect our security, Beijing tells Seoul
South China Morning Post, Jane Li, 2016 12 16
Beijing - The **Ministry of National Defence has called for China and South Korea to "respect each other's security interests"** after media reports that China ignored a request by a South Korean naval ship to visit Shandong province. In a post on its website yesterday, the ministry said it attached great importance to developing **military-to-military relations with South Korea and was willing to carry out exchanges and cooperation in defence**. The statement came as media outlets, including Arirang News, cited the South Korean navy as saying one of its ships received no response to a request for entry to the port of Qingdao. The South Korean government has reportedly labelled the incident as a "punishment" for its planned deployment of the US Terminal High Altitude Area Defence (THAAD) missile system. Beijing and Moscow both strongly object to the deployment, saying the system's powerful radar could be used to spy on them. China's ambassador to South Korea has also said that THAAD's installation would destroy the bilateral relationship in "an instant". South Korean media have

reported that some China-South Korea business deals have been put on hold without explanation and Beijing has hinted that even cultural imports such as K-pop may suffer if THAAD goes ahead.

Beijing, Paris agree to more efficient pursuit of corrupt fugitives (Canada)
China Daily, Zhang Yan, 2016 12 15
Beijing - **Beijing and Paris will strengthen joint investigations of corrupt officials who have fled China, and also improve systems for the return of ill-gotten assets illegally transferred to France, a senior anti- graft official from the Ministry of Justice** said. Chinese judicial officers and their French counterparts will expand intelligence-sharing and evidence-collecting in major cases, said **Zhang Xiaoming**, deputy director-general of the Judicial Assistance and Foreign Affairs Department at the Ministry of Justice. They will set up a work team and work closely on investigating, freezing and confiscating the illicit money. They also will establish a quick-response procedure to combat cross-border economic crimes such as telecom fraud, he said. Zhang said that during a recent meeting in Beijing, law enforcement officers from both countries exchanged views on tracking down fugitives and returning their ill-gotten funds. "It's more than necessary to share information with our Chinese counterparts in a timely manner and, after obtaining intelligence, such as indications of money laundering or other economic fraud, access our system to continue the investigation," said Robert Gelli, head of the Directorate for Criminal Matters and Pardons of the Ministry of Justice of France. **In recent years, Western countries, including the United States, Canada and some European countries, have become popular destinations for corrupt officials because an absence of bilateral extradition treaties** and differences in legal systems make it harder to secure their return, according to the **Ministry of Public Security**.

Foreign NGOs on back foot as new Chinese law looms
Reuters, Christian Shepherd, 2016 12 15
Beijing - **Foreign organisations including social and environmental advocacy groups fear they could inadvertently break broadly defined new rules that take effect in China next month**, with some even shutting up shop to avoid such pitfalls. **Chinese President Xi Jinping's administration** has made sweeping changes to Chinese law in the name of boosting national security, including **a controversial cybersecurity law passed** last month and another targeting foreign non-governmental organisations (NGO), slated for Jan. 1. China says the NGO law, which grants broad powers to police to question NGO workers, monitor their finances and regulate their work, is necessary to regulate an unruly sector and that only those operating illegally have anything to fear.

China confirms official met with Trump adviser in New York
Global Times, Zhao Yusha, 2016 12 14
Beijing - The **Chinese foreign ministry said on Monday a Chinese State Councilor met a senior adviser of US President-elect Donald Trump as part of China's efforts to establish connections with Trump.** State Councilor Yang Jiechi met **Michael Flynn, Trump's choice for national security adviser**, during a recent stopover in New York on his way to Latin America, Geng Shuang, a spokesperson for Chinese foreign ministry, told a daily briefing on Monday. The two sides exchanged views on China-US relations and major issues of common interest, said Geng, without mentioning when exactly they met. Flynn is a retired US Army Lieutenant General, who until 2014 was head of the **Defense Intelligence Agency**, CNN reported. This is China's attempt to build connections with Trump's team, and paves the way for the next meeting, Wu Xinbo, director of the Center for American Studies at Fudan University told the Global Times on Tuesday, who declined to say whether the next meeting will involve other top officials from both sides.

Return to Table of Contents/ Retour à la table des matières

Russia / Russie

Les ressorts de la nouvelle cyber-guerre froide
Le Figaro, Pierre Avril, 2016 12 16
Moscou - **GUCCIFER 2.0, Fancy Bear, ATP 28, Cozy Bear Strontium... tels sont les nouveaux visages de la menace russe pesant sur l'Occident, selon les services de renseignement**. Derrière ces noms de code, se cachent des hackers russes menant des attaques contre des chaînes de télévision, contre des opérateurs téléphoniques, des fournisseurs de système de sécurité informatique et des partis politiques occidentaux. Selon le New York Times , ces spécialistes auraient attaqué les serveurs du Parti démocrate américain, avant de faire fuiter des informations confidentielles dans le but de favoriser Donald Trump face à Hillary Clinton. Fancy Bear ou APT 28 (« Advance Persistant Threat ») seraient liés aux **services de renseignement militaires russes, le GRU**. Selon des sources judiciaires françaises, ce groupe, connu sous ces deux noms d'emprunt, serait à l'origine de l'attaque dont a été victime la chaîne d'information française TV5 en avril 2015. À un an des **élections législatives allemandes,** scrutées de près par Moscou, **les services de renseignement intérieurs (BND)** ont annoncé une « hausse spectaculaire » des tentatives d'hameçonnage de la part de Fancy Bear, une technique consistant à infiltrer un réseau après l'envoi de mails servant d'accroche. Le même groupe serait impliqué dans le piratage du Parlement allemand en 2015.

Russian spies adopt new tactics to battle old enemy
Financial Times, David J. Lynch, 2016 12 14
Washington - **Russia's hacking during the US presidential campaign marks a significant escalation of a cold war-style espionage offensive aimed at recruiting spies, acquiring financial secrets and siphoning off advanced technologies**, according to court records and interviews. The resurgent espionage operation -- a reminder of Russian **President Vladimir Putin's lineage as a former KGB officer** -- is testing short-handed Federal Bureau of Investigation counter-intelligence units and challenging traditional spying norms. More than 100 **agents of Russia's SVR foreign intelligence service are believed to be operating in the US, according to a former FBI counter- intelligence official. Joel Brenner, US national counter-intelligence executive from 2006 to 2009**, says the "ramping up" of Russian spying is continuing as Moscow seeks to undermine US strength through information warfare and cyber attacks. "Russian efforts in the US are intense now," he said. "The Russians know they have to play jiu jitsu with the US instead of taking us on directly." Moscow's standard espionage operations in the US have long concentrated on ferreting out secrets and cultivating well-placed contacts.

Return to Table of Contents/ Retour à la table des matières

Europe

La Suisse pas plus menacée après le drame de Berlin
Agence Télégraphique Suisse, 2016 12 20
Berne— La **Suisse n'est pas davantage menacée après le drame du marché de Noël à Berlin. Le Service de renseignement de la Confédération (SRC) analyse la situation en**

permanence, a-t-il indiqué mardi à l'ats. Le SRC n'a pas attendu l'attaque au camion contre un marché de Noël à Berlin pour prendre des mesures. D'autres événements ont impliqué un renforcement de la sécurité, et ce type de mesures ne sont pas exclues à nouveau. L'attaque dans la capitale allemande montre en revanche que la menace terroriste reste élevée pour les pays européens, voire s'accroît, écrivent le SRC, l'Office fédéral de la police (Fedpol), le Département fédéral des affaires étrangères et les polices cantonales dans un communiqué conjoint.

PM says no signals of increased threat of terrorism in Lithuania
Baltic News Service, 2016 12 20
Vilnius— **Prime Minister Saulius Skvernelis on Tuesday called on Lithuanians not to panic in the wake of Monday's deadly truck attack in Berlin, saying that there are no signals of an increased threat of terrorism in the country**. "There is no need for panic or worry, at least for now. The situation is under control and there are no signals of an increased terrorism threat in Lithuania," he told reporters. When asked about the security situation in the country, the **prime minister underlined that an improved draft budget earmarks more funds for the State Security Department compared with that drafted by the previous government. "**The **initial 2017 budget provided for cutting funding for the State Security Department.** You understand that timely intelligence information can help prevent such attacks. We have found the means to step up the SSD's intelligence capabilities and this is my answer," he said. The previous government proposed to cut funding for the SSD by 54,000 euros next year compared with 2016, but 1.5 million euros were later added to the department's 2017 budget, raising it to over 26 million euros in total. **Darius Jauniskis, the department's director, has said that the state security agency will use the extra funds to develop its IT technologies and train its staff.**

Lukashenko congratulates Belarusian security service on professional holiday
Belarus Daily News, 2016 12 20
Minsk— **Belarus President Alexander Lukashenko has sent greetings to the senior staff, other personnel and veterans of the state security service as they celebrate their professional holiday – Day of Security Service Personnel**, BelTA learned from the press service of the Belarusian leader. “Since its foundation, the Belarusian security service has been protecting the lives and creative labor of our citizens. Today it is doing its best to promote the implementation of the state policy in the social sector, economy, and politics by solving crucial tasks to protect the constitutional system, prevent extremism and foreign interference in the internal affairs of the country,” the message of greetings reads.

Commandos du CPA 10, des soldats de l'ombre au coeur de l'armée de l'Air
Agence France-Presse, Journaliste maison, 2016 12 20
Base Orléans-Bricy, France - Sur la base aérienne d'Orléans-Bricy (France) "La spécialité de mon groupe d'action, c'est le terrorisme, la libération d'otages et la capture de chefs insurgés, de cibles importantes". **Pour raconter son expérience, ce soldat d'élite du "CPA 10" (Commando Parachutiste de l'Air no 10) témoigne cagoulé. Comme lui, tous les membres des forces spéciales (3.000 hommes au total), fer de lance de l'armée française, ne déclinent jamais leur identité et n'aiment pas faire parler d'eux. Contrairement aux agents de la DGSE, ils n'agissent jamais dans la clandestinité.** Ce sont des soldats de l'armée française. Mais leurs actions relèvent du secret défense et leurs modes opératoires impliquent discrétion et fulgurance. Les hommes du CPA 10 - composante Air des forces spéciales - sont derrière nombre d'opérations périlleuses, libérations d'otages, infiltrations en territoire ennemi, renseignement. Ils en paient aussi le prix fort, du Sahel à l'Irak.

Services secrets français - Enigma, la géniale machine dont la France n'a pas voulu
Le Point, François-Guillaume Lorrain, 2016 12 20

Paris— Dès 1931, la France possédait toutes les clés pour fabriquer la crypteuse des Allemands. Elle a préféré l'offrir aux Polonais. C'est l'histoire d'une formidable réussite et d'un formidable échec. La preuve que la France eut de l'or entre les mains, sans savoir rien en faire, sinon le transmettre à ses alliés, la Pologne et l'Angleterre. Tout commence un 1er novembre 1931 au Grand Hôtel de Verviers, en Belgique. Un voyageur allemand, Hans-Thilo Schmidt, **vient proposer ses services à un redoutable recruteur du Service de renseignements français**, Rodolphe Lemoine, ex-Rudolf Stahlmann, alias Rex, un Allemand qui est lui-même passé du côté hexagonal dès 1914. Schmidt, frère de l'ancien patron du Chiffre allemand et employé dans cette section, a contacté l'ambassade de France à Berlin, qui l'a renvoyé à Paris, selon la procédure. Ses motivations ? Faire bombance. Mal payé dans une Allemagne à la dérive, atteint physiquement dans sa chair pendant la Première Guerre mondiale, il est venu offrir à la France des informations stupéfiantes sur le parti nazi, le réarmement de l'Allemagne, son organisation militaire et policière, les intentions de Hitler, ainsi que sur une ancienne machine commerciale, Enigma, dont 70 000 exemplaires équipent tous les services d'outre-Rhin. L'épopée a été révélée en 1972 par le général Bertrand, qui avait créé, en 1930, le service du **Chiffre du Service de renseignements (SR),** puis par Paul Paillole, en 1975, ex-chef de la section allemande du contre-espionnage après 1936.

Services secrets français : les confessions d'un agent à Dakar
LePoint.fr, 2016 12 18
Analyse: **Comment entre-t-on dans les services secrets français ? Dominique Fonvielle* : Par hasard, dans mon cas.** Saint-Cyrien, je n'avais pas envie de végéter dans une garnison. On m'a admis au **SDECE**** sous réserve que je passe en six mois le concours d'entrée à Sciences Po et que je réussisse une licence d'anglais à la Sorbonne. En septembre 1978, j'entre officiellement dans le service. Je suis les cours de l'École de guerre pendant un an, j'effectue quelques missions pour la base de Paris, qui est clandestine. Dès 1979, me voilà « rédacteur-exploitant », c'est-à-dire analyste, pour l'Afrique. Je reçois les télégrammes chiffrés puis déchiffrés et j'en fais la synthèse. En juillet 1985, je deviens « rédacteur-exploitant » à Dakar, un très gros poste qui couvre, outre le Sénégal, le Mali, la Mauritanie, le Tchad, la Guinée, la Gambie, la Sierra Leone. Puis je suis chef du poste sous la couverture de deuxième secrétaire d'ambassade, donc de diplomate... Comment cela se passe-t-il ? C'est une vraie jungle ! On s'est ingénié à diviser les divers départements : renseignement, écoutes, contre-espionnage, conseillers français de la présidence. À **lire : "Mémoires d'un agent secret", de Dominique Fonvielle et Jérôme Marchand (Flammarion).**** Le Service de documentation extérieure et de contre-espionnage.

Services secrets français : sous Sarkozy, les grandes manoeuvres
LePoint.fr, Jean Guisnel et Olivia Recasens, 2016 12 17
Paris - La **réforme du renseignement intérieur voulue par le président n'a pas été guidée par une vision stratégique, mais par un esprit de vengeance**. Devenu président en 2007, **Nicolas Sarkozy n'a pas manqué d'agir rapidement en matière de renseignement extérieur**. Il faut dire qu'il a trouvé en arrivant un plan mis au point de longue date pour réformer ce secteur. Celui d'une équipe d'experts, réunis en 1995 au Secrétariat général de la défense nationale (**SGDN**) par **le préfet et ancien directeur de la DST, Rémy Pautrat**. Autour de lui, Jean-Louis Gergorin (Groupe Lagardère), Philippe Marland (préfet), Bernard Norlain (général), Michel Foucher (géographe), Bernard Esambert (ingénieur des Mines), Xavier de Lussy (contre-amiral). C'est l'ossature de la réforme du renseignement que le candidat Édouard Balladur souhaite mettre en place après son entrée à l'Élysée. Mais le vainqueur, Jacques

Chirac, n'en voudra pas. En 2007, Nicolas Sarkozy ressort donc le plan d'action des cartons et crée, en 2008, un Conseil national du renseignement (CNR), confié à un « coordonnateur ». Ce sera le diplomate Bernard Bajolet, clé de voûte d'une organisation nouvelle inspirée par un objectif exclusif : éviter des attentats sur le sol français. Alors que le quinquennat Sarkozy **est marqué par une baisse considérable des effectifs militaires, les services de renseignement extérieur (DGSE et DRM) voient croître leurs moyens humains et matériels.** En juin 2008, Sarkozy annonce que les services français vont s'engager dans la « lutte informatique offensive ». Si cette ambition a été confirmée par son successeur, l'une des idées maîtresses qui la sous-tendaient, le rapprochement des appareils de défense extérieure et de sécurité intérieure, connaît encore aujourd'hui de grosses difficultés de mise au point.

Le renseignement militaire s'allie aux start-up
Les Echos, Anne Drif, 2016 12 16
Creil, France - La **Direction du renseignement militaire veut capitaliser sur la French Tech**. Elle ouvre un campus d'expertise basé à Creil, réunissant start-up, grandes entreprises, écoles et instituts de recherche. La Direction du renseignement militaire (**DRM**) s'intéresse de très près à la French Tech. Elle vient de donner le coup d'envoi au premier « Intelligence Campus Entreprise », à Creil dans l'Oise, son nouveau pôle d'expertise des nouvelles technologies du renseignement.

SANS Agent Accused of Three Crimes
Bulgarian News Agency, 2016 12 16
Sofia— The **Anti-corruption Specialized Unit at Sofia's City Prosecution Office has arrested and is investigating an agent of the State Agency for National Security (SANS), suspected of three crimes.**The **agent, who was head of division in the Counter-intelligence Directorate,** is under investigation for fraud, a documentary offence and for revealing a state secret. The pre-trial proceedings were launched on a SANS alert about an agent who deceived foreign nationals that they would be granted permanent residence in Bulgaria, provided them with forged documents, and revealed a state secret. Documents were seized during a search of the agent's home and office in Sofia on Thursday.

Lithuania's state budget to be approved on 22 December
Lithuanian News Agency, 2016 12 16
Vilnius— Voting on the approval of Lithuania's state budget for 2017 is going to be held on 22 December. Minister of Finance Vilius Sapoka says that government sector expenditure and revenue can be balanced by 2019. "The government sector budget without a deficit will be reached in the medium term, by 2019," the finance minister said at Parliament while presenting the revised draft budget. **Compared with the initial draft budget, appropriations for the Public Procurement Office (VPT) were increased by EUR 0.35 million, the State Security Department (VSD) - by EUR 1.5 million** and the Competition Council - by EUR 0.22 million.

German, foreign secret services aware of PKK activities in EU, PKK leader says
Daily Sabah, Staff report, 2016 12 15
Istanbul - **German and other foreign intelligence services,** as well as European politicians, **have long been aware of the outlawed terrorist organization, the PKK's activities in Europe and have maintained communication, as acknowledged by Abdul Rahman Haji Ahmadi aka Haji Ahmadi, the leader of the PKK's Iranian offshoot Party of Free Life of Kurdistan (PJAK),** while talking to German TV station Westdeutscher Rundfunk (WDR) way back in 2007. Haji Ahmadi, who holds a German citizenship and lives there, told the WDR that he kept in touch with foreign secret services, including **Germany's Federal Intelligence Service or the Bundesnachrichtendienst.** "A young man came and said he was from the

BND. He asked what everyone else asks, and I have given the same answer I've given to you," Ahmedi said, and continued that they knew exactly who he was. "I have been in Europe for more than 43 years, mostly in Germany and they also know who I am. They also know since when I have been leading the PJAK/PKK."

NSA contre DGSE, petites écoutes entre amis (Canada)
Le Point, Jean Guisnel, 2016 12 15
Paris - Siphonnage. **L'espionnage informatique est l'arme fatale du renseignement, et les Français ne sont pas en reste**. Nous sommes en juin 2012. Edward Snowden est pour une année encore l'un de ces bons petits soldats de l'ombre, tapi dans une base secrète de la NSA à Hawaii. A Paris, Nicolas Sarkozy termine son mandat, quand le chef des services informatiques de l'Elysée, un homme de la DGSE, s'inquiète. Les services de renseignement canadiens En 2009, le **Centre de la sécurité des télécommunications du Canada (CSEC)** découvre une vaste opération de cyberespionnage baptisée Snowglobe et l'utilisation de Babar, un programme malicieux (maliciel). Le CSEC soupçonne les services secrets français.

Services secrets français - Moi, président, je permets de tuer
Le Point, Jean Guisnel, 2016 12 15
Paris - Au grand dam des officiers de la "Grande Muette", François Hollande a brisé le culte du secret. Le 31 août 2014, **François Hollande apprend de la DGSE qu'après une traque de vingt et un mois elle a repéré le chef des djihadistes chebabs somaliens, Ahmed Abdi Godane**. Celui-là même qui avait fait enlever deux sous-officiers du service Action de la DGSE à Mogadiscio, en juillet 2009. L'un s'était évadé, mais le second, connu sous l'IF (identité fausse) de Denis Allex, a été martyrisé jusqu'à ce qu'une opération de la DGSE visant à le libérer échoue, le 11 janvier 2013, à Mulo Marer. Le raid raté s'est soldé par la mort de l'otage et de deux de ses camarades du Centre parachutiste d'instruction spécialisée (CPIS) de Perpignan, ainsi que par celle de 17 chebabs. Face à face. A Creil, le 8 janvier 2014. Le président de la République avec le général Christophe Gomart, patron de la DRM, et un soldat français engagé au Mali.

Que valent nos agents secrets ?
Le Point, Rémi Kauffer, 2016 12 15
Paris - Contraste. Excellents en opérations spéciales, très bons en technologie, nos services ont souffert de leurs luttes intestines et de l'attitude de nos présidents. Que valent-ils, en effet ? Difficile de répondre à la question sans se pencher sur leur passé. Une trajectoire qui commence le 4 janvier 1946, quand un décret non publié au JO crée **le Service de documentation extérieure et de contre-espionnage (SDECE), où fusionnent les fidèles de Charles de Gaulle et ceux de son rival vaincu, le général Giraud. Gaulliste de 1940**, le premier patron du SDECE, André Dewavrin, dit le colonel Passy, voulait que son service soit rattaché aux Affaires étrangères, à l'instar du **MI6 britannique**. De Gaulle a tranché : le nouveau- né dépendra du chef du gouvernement. Même si le Général quitte le pouvoir par surprise le 20 janvier, le SDECE, lui, reste sous la tutelle de Matignon.. Autant dire que le savoir-faire que les Français gagnent dans l'action paramilitaire - coups de commando, sabotages, assassinats ciblés, y compris en Europe, implantation de contre- maquis (voir p. 194) -, ils le perdent dans le domaine du Renseignement contre le KGB et ses satellites. Quant au contre-espionnage judiciaire, il est depuis novembre 1944 l'apanage d'une police rattachée au ministère de l'Intérieur, la **Direction de la surveillance du territoire (DST), matrice de l'actuelle DGSI.**

Dans les carnets de Rondot
Le Point, Rémi Kauffer, 2016 12 15

Paris - La singularité de **Philippe Rondot, homme pivot des services français, c'est qu'au cours de sa longue carrière il sera amené à opérer non seulement au Service de documentation extérieure et de contre-espionnage, son affectation de départ, mais aussi à la DST, ancêtre de la DGSI,** à la Direction du renseignement militaire (**DRM**) ou au Centre d'analyse, de prospective et de stratégie du Quai d'Orsay. Une expérience unique qui fera de ce multicartes le conseiller de plusieurs gouvernements aux affaires arabes et aux questions de renseignement. Mais le plongera du coup dans cet univers politique pour lequel il n'était pas fait. Les dirigeants lui demandent tout et n'importe quoi, comme enquêter sur **l'affaire Clearstream** sur requête de Dominique de Villepin, alors Premier ministre, même s'il ne possède aucune compétence financière.

Espionne, lève-toi !
Le Point, Patrick Besson, 2016 12 15
Paris - « **Rainbow Warrior** ». **Dominique Prieur fut la victime collatérale de l'opération de sabordage visant le navire amiral de Greenpeace**. L'écrivain raconte le destin détonant de **la première femme officier de la DGSE.** Le fort de Noisy, à Romainville, est invisible, à moins d'entrer dans l'espionnage : c'est le siège du service Action de la DGSE. On ne voit que de hauts murs blancs surmontés de barbelés et quelques longues portes bleues. Impossible de négocier une visite auprès d'un soldat en faction : il n'y en a pas. Il y a des caméras, qui m'ont sans doute filmé. Le début du XXIe siècle : on passe tous à la télévision de surveillance. J'imagine la fouille au corps avant d'entrer dans le fort : déshabillage complet et toucher rectal. En mars 1985, Dominique Prieur est convoquée à Noisy pour une nouvelle mission. Elle est la première femme officier de la DGSE.

Jean Heinrich : « Nous agissons dans l'illégalité poussée à l'extrême »
Le Point, Jean Guisnel, 2016 12 15
Paris - Décryptage. **Ancien chef du service Action de la DGSE, le général décode le renseignement de l'après-guerre froide. Le Point : Quels ont été les effets de la fin de la guerre froide, pour le renseignement français ? Jean Heinrich : Durant la guerre froide, l'Otan se trouvait face à une menace cohérente et rationnelle : l'URSS et ses alliés. Les membres de l'Otan s'étaient réparti les zones de responsabilités**. A la France revenaient la Tchécoslovaquie et une partie de la Russie. Nous formions de jeunes sous-officiers chargés des écoutes en langues tchèque et russe. Nous partagions les résultats avec nos alliés, ce qui permettait de multiplier nos informations par un facteur quinze ou vingt ! Nous avions des renseignements de grande valeur et quand un pilote tchèque décollait, nous connaissions son nom, son grade, ses heures de vol, ses capacités opérationnelles. Du point de vue du renseignement militaire, on savait tout, d'autant que nous avions de bons contacts en face. Nous nous sommes laissés aller vers une certaine facilité.

La galaxie du Renseignement
Le Point, Journaliste maison, 2016 12 15
Paris - Organismes satellites La CNCTR Président : Francis Delon. **La Commission nationale de contrôle des techniques de renseignement instruit les demandes d'interception et de surveillance électronique présentées par les services.** Son avis est transmis au Premier ministre, dont la décision est souveraine. La DPR Présidente : **Patricia Adam. La Délégation parlementaire au renseignement contrôle l'action du gouvernement en la matière. Elle est bicamérale (trois députés, trois sénateurs) et bipartisane (majorité-opposition). Elle rend un rapport annuel et quatre de ses membres composent la commission de vérification des comptes spéciaux.** La CCSDN Présidente : **Evelyne Ratte**. La Commission consultative du secret de la défense nationale examine les demandes de la justice quand elle souhaite la déclassification d'un document émis par une administration et protégé par le secret de la

Défense nationale. La commission rend un avis que le gouvernement suit, ou pas. L'Académie du renseignement Directeur : **Cyrille Chabauty**. L'Académie assure la formation continue des fonctionnaires appartenant aux six services de renseignement. Elle dépend du Premier ministre et vise à renforcer les liens entre les fonctionnaires et à les doter d'une culture commune.

Le mythe du 2e Bureau
Le Point, Rémi Kauffer, 2016 12 15
Paris - Mise au point **La légende de l'officier du 2e Bureau séducteur, familier des missions périlleuses, des espionnes au regard de mystère et des vols de documents au nez et à la (fausse) barbe de l'ennemi, est tenace**. Née à la Belle Epoque, elle est ensuite véhiculée dans l'entre- deux-guerres par une pléiade de romanciers et de cinéastes. **Or le 2e Bureau n'est pas un organe d'espionnage comme le BCRA et ses modernes successeurs, le SDECE puis la DGSE, mais un service d'analyse des éléments divers collectés de sources soit humaines, soit technologiques, par les structures de renseignement**. Tout état-major d'une grande unité de l'armée française compte plusieurs bureaux spécialisés, le deuxième étant traditionnellement l'apanage d'officiers chargés d'éplucher les informations recueillies et d'en tirer des conclusions pratiques sur l'ordre de bataille de l'armée adverse, ses moyens, son moral, ses plans d'attaque ou de repli. A cette confusion entre renseignement et analyse, la légende ajoute une dimension physique. Ainsi l'homme-fiction du 2e Bureau préfigure-t-il l'espion « james-bondissant » des séries télé ou des films anglo-saxons d'aujourd'hui.

Le plus secret des services
Le Point, Jean Guisnel, 2016 12 15
Paris - **DGSE. Six mille agents servent la Sécurité extérieure. Leurs missions sont multiples, de l'information à l'action. On les imagine galopant pistolet dans une main et poignard dans l'autre, parcourant la planète pour trucider les ennemis de la France.** Cela arrive, mais c'est rare ! Ou alors on se les figure convoyant des sacs de billets de la Banque de France pour verser des rançons d'otages. Ça se produit aussi ! L'un de ces agents désabusés de l'armée des ombres se souvient que la somme (« énorme ! ») transportée pour payer la rançon d'un reporteur enlevé au Moyen-Orient voilà quelques années aurait suffi à remettre à flot son journal en fâcheuse posture. La DGSE, ce n'est pas que cela... C'est aussi, par exemple, le soutien apporté clandestinement, par tous les moyens illégaux imaginables, aux industries françaises dites « de souveraineté », celles qui contribuent à l'indépendance nationale.

Les espions recrutent
Le Point, Marc Le plongeon, 2016 12 15
Paris - Profil. Intéressé par la carrière ? Voici le mode d'emploi. **Pour les générations biberonnées aux James Bond et aux romans de John le Carré, le métier d'espion fait fantasmer, mais ne correspond pas tout à fait à la réalité.** Ajoutez à cela des aspects plus pragmatiques comme les aléas de la carrière, les sacrifices inhérents à la fonction (vie personnelle), le fait de devoir mentir même à ses proches... Au-delà des clichés, la « communauté du Renseignement » accueille des profils de plus en plus variés et aussi pointus que dans le privé : analystes, ingénieurs, agents de terrain, traducteurs (surtout en langues rares). Sur son site Internet, la **Direction du renseignement militaire (DRM) recrute sur CV des interprètes images, des ingénieurs en big data ou encore des spécialistes du renseignement géospatial. S'il est possible de rejoindre la DGSE à l'issue d'une scolarité à l'Ena**, des centaines d'étudiants - qui disposent au minimum d'une licence - tentent chaque année leur chance aux concours de la fonction publique. Pour les postes spécifiques comme des langues étrangères, hors administratif, la DGSE peut également embaucher sur contrat.

Le pionnier de l'antiterrorisme
Le Point, Roger Faligot*, 2016 12 15
Paris - Avant-garde. **Joseph Fourrier prend la tête de la première cellule spécialisée à la DGSE. Alors que l'informatique balbutie dans les années 1970, le colonel Joseph Fourrier utilise fiches en carton et cartes perforées. Une gageure pour cet ancien saint-cyrien blessé en Algérie en 1956, spécialiste de la division contre-espionnage (K)** que de donner naissance à la petite section K-Terro. Forte d'une dizaine de membres, cette cellule se développe en 1972. Une année charnière : en RFA s'illustre la Fraction armée rouge; en Italie, les Brigades rouges et l'Orchestre noir; en Irlande, l'Armée républicaine irlandaise (Ira) intensifie sa campagne militaire. La France se trouve aussi au centre des règlements de comptes entre Septembre noir et le **Mossad**, à la suite du massacre des athlètes israéliens par les Palestiniens lors des JO de Munich. Au Moyen-Orient survient un attentat sanglant à l'aéroport de Lod, à Tel-Aviv-Jaffa, organisé par l'Armée rouge japonaise (Nippon Sekigun) avec le Front populaire de libération de la Palestine.

Parliament Passes Conclusively Counter-Terrorism Act
Bulgarian News Agency, 2016 12 15
Sofia— **Bulgaria's Parliament Thursday passed conclusively the Counter-Terrorism Act, voting through the remaining provisions of the bill.** According to the clauses approved on Thursday, it will be admissible to restrict certain civil rights temporarily in the anti-terrorist operation zone. When requested to do so by the head of the operation, the mass media will have to transmit immediately unedited information needed to keep the public informed. The information that the mass media report during an anti-terrorist operation must not contain any data disclosing special techniques and tactics used in the operation, the identity of the persons involved in the operation, and other data that may impede the conduct of the operation or endanger human life and health. The **Transitional and Final Provisions of the Act amended the State Agency for National Security Act, empowering authorities of the Agency to apprehend persons in specified cases**.

Lithuania's state security agency to provide training for MPs
Baltic News Service, 2016 12 14
Vilnius— The **Lithuanian State Security Department is planning to organize training for newly-elected members of the parliament**. "We have many new members in the Seimas. **We have agreed that we will organize training in individual political groups to give them a better understanding of intelligence activities and to prevent delays in passing some laws** because of a lack of knowledge and to ensure that this process is smooth," Seimas Speaker Viktoras Pranckietis told reporters on Wednesday after meeting with Darius Jauniskis, the department's director. Jauniskis said that parliamentarians **need help to understand what intelligence is.** "There are many new members of the Seimas who are not very much familiar with intelligence and do not always understand the difference between intelligence and criminal intelligence. We must talk and help them understand how things work and it will then be easier to explain to them why certain laws are needed," the director said. He expects that a better understanding of the work of the **state security agency** and national security matters will help lawmakers in their work.

Berlin craint des cyberattaques russes
Tribune de Genève, Journaliste maison, 2016 12 14
Berlin - Les **renseignements soupçonnent Moscou de préparer des opérations de propagande pour influencer la campagne de 2017.** Après les cyberattaques qui ont émaillé la campagne électorale américaine, les Allemands redoutent à leur tour d'être victimes d'une

opération de déstabilisationde la part des services secrets russes. **Selon les services allemands de renseignements (Verfassungsschutz), chargés du contre- espionnage, les responsables politiques risquent fortement d'être visés par des cyberattaques et des opérations de propagande pendant la campagne électorale**. « Selon nos informations, il est clair qu'on cherche à influencer les élections de l'année prochaine en discréditant des responsables politiques » , a affirmé **Hans-Georg Maassen. Le patron du renseignement allemand** estime que les campagnes de désinformation russes ont pris beaucoup d'ampleur depuis la crise ukrainienne en 2014. Moscou aurait engagé « d'énormes moyens » pour financer les médias d'Etat, les instituts politiques proches du Kremlin et surtout les réseaux sociaux afin de brouiller les cartes du discours politique allemand et de créer ainsi un climat de peur au sein de la population.

Intelligence Report Confirms Growing Saudi, Qatari Support to Extremists in Germany
Fars News Agency, 2016 12 14
Tehran - An **intelligence report revealed on Tuesday that support by Saudi Arabia and Qatar for the extremists who follow the Wahabism movement in Germany has grown significantly**. The report pointed out that Riyadh and Doha had sent advocates "to spread the radical version of Islam," Suddeutsche Zeitung reported. According to the report, **the Foreign Intelligence Service (BND) and the Constitution Protection Commission, Germany's Internal Intelligence**, have wrote to the German government that religious organizations from the Persian Gulf have established mosques and educational institutions, as they had also sent advocates to Germany to "Spread the radical version of Islam. They added that "this conclusion is based on the evidence that has been reached so far.

Gulf state groups are 'supporting Salafists in Germany': report
The Local (Germany), Staff report, 2016 12 13
Berlin - Three major German news outlets have reported that **religious groups from Saudi Arabia, Kuwait and Qatar have been increasingly supporting Salafists in Germany, raising concerns among intelligence agencies**. The Süddeutsche Zeitung (SZ) as well as broadcasters NDR and WDR reported on Tuesday that a report by German intelligence agencies shows an increase in support from religious groups in the three Gulf states to Salafists in Germany. The media outlets state that these organizations have helped build school facilities, mosques and sent preachers to Germany to share a fundamentalist version of Islam. SZ reports that **Germany's BND and BfV intelligence agencies are concerned that the intolerant and ultra- conservative form of Islam could spread.** Currently they estimate there to be 10,000 members of the Salafist scene, and believe that refugees could also be drawn into it.

Return to Table of Contents/ Retour à la table des matières

Middle East / Moyen-Orient

Mossad chief and security delegation meet with Trump team
Ynetnews, Itamar Eichner and Tzipi Shmilovitz, 2016 12 19
Jerusalem - **Director of the Mossad, Yossi Cohen, clandestinely visited the United States to meet with President-elect Donald Trump's staff and brief them on pressing security matters** including the Iranian nuclear deal, the Syrian civil war, terror threats and the Palestinian issue. The security delegation was organized by Prime Minister Benjamin Netanyahu and was led by National Security Council head Yaakov Nagel. The **Israeli ambassador to the United States Ron Dermer was also present during meetings. The** two sides also discussed a regional conference to be hosted by Egypt and other initiatives on the agenda including a UN

initiative put forth by the Palestinians and New Zealand. Additionally, Israeli officials have also reached out to the President-elect to ask him to come out against President Obama and veto a Palestinian bid submitted to the Security Council.

L'ombre du Mossad sur le meurtre d'un islamiste à Sfax
Le Figaro, Cyrille Louis, 2016 12 19
Paris— **Une dizaine de balles tirées à bout portant. Ce mode opératoire ne ressemble guère aux complexes opérations du Mossad**. Mais le profil de la victime a d'emblée orienté les soupçons vers **l'agence de renseignements israélienne**. Cet ingénieur spécialiste des drones, âgé d'une quarantaine d'années, collaborait apparemment avec la branche militaire du Hamas. Son assassinat, vendredi dernier, alors qu'il circulait en voiture dans la ville tunisienne de Sfax, a aussitôt été imputé à l'État hébreu par le mouvement islamiste qui contrôle la bande de Gaza. « **Les Brigades Ezzedine al-Qassam** (la branche armée du Hamas) portent le deuil de leur commandant et **pilote Mohammed Zawari** », ont affirmé ses dirigeants. Selon les médias tunisiens, Zawari avait quitté son pays au début des années 1990 pour fuir la répression anti-islamiste de Ben Ali. Établi à Damas, il s'était rapproché du Hamas palestinien et du Hezbollah libanais, qu'il aurait aidés à se doter de drones militaires utilisables contre Israël. L'ingénieur avait ensuite regagné la Tunisie après la révolution de 2011, mais il continuait à se rendre au Liban.

Tunisia: 'Foreign Elements' Behind Assassination of Hamas Drone Expert
Haaretz, 2016 12 18
Jerusalem— **Mohammed Zawahri was killed last week in assassination attributed to Israel's Mossad.** Eight Tunisians have been arrested, police looking for Belgian suspect. Jack Khoury An undated photo of Mohammed Zawahri Facebook. Foreign elements were behind the assassination of a Hamas drone expert last Thursday, Tunisia announced on Sunday evening, following allegations that the engineer's death was orchesterated by Israel's Mossad. In a statement, the Tunisian government said it will continue to hunt down those involved in the assassination, both inside the country and outside of it.

Iran's Top Security Official, Putin Special Aide Discuss Latest Conditions in Aleppo
Fars News Agency, 2016 12 18
Tehran - Sec**retary of Iran's Supreme National Security Council (SNSC) Ali Shamkhani and Russian President's Special Envoy on Syria Alexander Lavrentiev in a meeting in Tehran on Sunday conferred on the latest situation in Aleppo**. "Liberation of Aleppo once again revealed the policies of the West and its regional backers for creating and sponsoring terrorism and rendering all-out political, media and military aid to the defeated Takfiri terrorists before the eyes and judgment of the world public opinion," Shamkhani said during the meeting on Sunday.

Ex-IDF Intel chief: Keep eye on Iran to prevent nuclear cheating
Jerusalem Post, Yonah Jeremy Bob, 2016 12 16
Jerusalem - The **intelligence needed to keep Iran from getting nuclear weapons is "a puzzle" that constantly needs to be assembled to prevent the Islamic Republic from cheating on the nuclear deal, former IDF Military Intelligence chief Maj.-Gen. (res.) Amos Yadlin** told The Jerusalem Post. Yadlin, currently director of the **Institute for National Security Studies (INSS)** in Tel Aviv, said that obtaining the right intelligence is one of the prerequisites to catching any Iranian attempt to walk across the nuclear threshold during the life of the deal it signed in 2015 or when the agreement's 2023, 2025 and 2030 deadlines expire.

State security officer shot; terror suspects charged
Lebanon Daily Star, Staff Report, 2016 12 16
Beirut - **Shots fired, wounding State Security officerTwo suspects opened fire on a state security officer Thursday in Akkar**, the state-run National News Agency reported. The **State Security Sgt. Mohammad H.** was on the road linking the town of Bibnine with Birqayel when he suffered gunshot wounds to his right thigh. He was admitted to Mazloum Hospital in Tripoli. His condition was reported as stable. Security forces are searching for the suspects, who are still at large.

UK envoy meets Lebanese security chiefs to discuss police program
Lebanon Daily Star, Staff Report, 2016 12 15
Beirut - **Britain's ambassador to Lebanon held his first meeting with the country's security heads to discuss improving the Lebanese police force**, following last week's announcement of a $16.5 million fund for the **Internal Security Forces**. "The U.K. is committed to Lebanon's stability, security and prosperity," Ambassador Hugo Shorter said in a statement after the meeting. "At the heart of this must be a state capable of providing the ultimate guarantee of security." The meeting followed the signing of an agreement in June between the U.K and **Ministry of Interior ISF Director General to create the British Police Support Project (BPSP)**.

Beyrouth, nid d'espions
Le Point, Rémi Kauffer, 2016 12 15
Beyrouth - Duels. **Comment la France s'est retrouvée prise au piège dans la capitale libanaise.** Au Liban, la complexité moyen-orientale a toujours atteint des sommets. Ajoutons les vagues de réfugiés palestiniens, fruits des guerres israélo-arabes, et, dans les années 1960 et 1970, le bourgeonnement de milices armées. Pendant ce temps, à Damas, Hafez el-Assad, officier d'aviation issu de la communauté religieuse minoritaire des alaouites, une branche du chiisme, instaure la dictature. Son objectif : une grande Syrie, dont le Liban ne serait qu'une province. Comme autrefois, au temps de l'Empire ottoman. Le décor est planté pour une tragédie que les services secrets d'une dizaine de pays vont rendre indéchiffrable. Dès les années 1980, Beyrouth remplace Berlin comme centre mondial de la guerre secrète. Une guerre dans laquelle le **SDECE puis son héritière, la DGSE, vont se trouver impliqués**.

Report: Mossad Chief Investigated for Receipt of Mariah Carey Tickets
Haaretz, 2016 12 14
Jerusalem—The **Civil Service Commission has launched an investigation into suspicions that Mossad head Yossi Cohen received free tickets to a Mariah Carey concert worth thousands of shekels from Australian billionaire James Packer**, Channel 10 reported on Wednesday. Channel 10 also reported on Wednesday that Cohen had spent time at Packer's luxury Tel Aviv hotel suite, or had free use of the premises, when Prime Minister Benjamin Netanyahu's son, Yair Netanyahu, was there as well. The commission is investigating whether Packer's gift amounted to receipt of an illegal benefit or favor, the report said. Cohen headed the National Security Council at the time but is now director of the Mossad.

Au coeur des services secrets de Daech
L'Express, Boris Thiolay, 2016 12 14
Raqqa - **L'organisation djihadiste possède ses propres unités de renseignement**. Ce sont elles qui ont planifié les attentats menés en France et Belgique en 2015 et en 2016. Enquête sur un corps d'élite toujours menaçant. L'homme, encagoulé et revêtu d'un uniforme camouflé, parle un français sans accent. Derrière lui, dans un décor de ruines, un prisonnier bâillonné est attaché, les bras en croix. Ce vademecum du terrorisme individuel peut être vu comme une

réplique à un événement survenu en France, cinq jours plus tôt. Le **21 novembre, les policiers de la Direction générale de la sécurité intérieure (DGSI) ont démantelé une cellule djihadiste qui prévoyait de commettre des tueries dans Paris et en Ile-de- France, le 1er décembre**. Ce petit groupe était « téléguidé » depuis la Syrie par un membre francophone de Daech.

Return to Table of Contents/ Retour à la table des matières

Asia / Asie

Top diplomat defector will take a public role in the South
Korea JoongAng Daily, 2016 12 21
Seoul— **Thae Yong-ho**, the senior North Korean diplomat who defected to the South with his family in August, will begin public activities starting Friday. The former deputy ambassador in London says he wants to dedicate his life to reunification. “Rather than seeking personal success, I want to dedicate my life to enabling a quicker unification — the hope of our people — so that the North Korean people can be freed from oppression and persecution,” Thae was quoted as saying to a group of lawmakers Monday. Various government sources Tuesday say that Thae, the **most senior North Korean diplomat to ever defect, is expected to work as a researcher of North Korea affairs at a state institute affiliated with the National Intelligence Service (NIS).** He is expected to remain in the public eye, unlike other senior North Korean defectors who remain private. That could bring risks to his personal safety Rep. Lee Cheol-woo, chair of the **National Assembly’s intelligence committee**, held a three-hour close-door meeting with Thae in Seoul on Monday with a bipartisan group of lawmakers on the committee.

Rajiv Jain made IB chief, Anil Dhasmana to head RAW
The Times of India, Neeraj Chauhan, 2016 12 19
New Delhi— The **government made two important appointments on Saturday with Jharkhand cadre 1980-batch IPS officer and a J&K hand Rajiv Jain and 1981-batch Madhya Pradesh cadre IPS officer Anil Kumar Dhasmana, an expert on Pakistan, named next chiefs of Intelligence Bureau and Research and Analysis Wing**. The two officers, presently second in command in their respective agencies, who were seen as frontrunners for the two crucial responsibilities, will head India's internal and external intelligence gathering agencies. Sources in the two agencies described Jain and Dhasmana as competent choices with both having significant experience on Jammu and Kashmir, Pakistan and Afghanistan. They will serve as chiefs for the next two years. Jain **takes over from IB chief Dineshwar Sharma** while Dhasmana **succeeds RAW chief Rajinder Khanna**. Jain, presently special director in the IB, joined the agency in 1989 as assistant director and has since worked in different capacities, including chief of Delhi Subsidiary Intelligence Bureau (SIB), considered politically sensitive, apart from Ahmedabad and J&K desks. Officials told TOI that Jain is an expert on J&K and Islamic extremism and has supervised many operations in the recent past.

India appoints new army, air force and intelligence chiefs
The Peninsula, 2016 12 18
New Delhi - The **Indian government has appointed new heads of its army and air force among a series senior military and intelligence appointments**, officials said, two weeks before its two most senior defence force chiefs are due to retire. **Vice Chief of Army Staff Lieutenant General Bipin Rawat was named as the new chief of the army to succeed General Dalbir Singh Suhaag. Air Marshal Birender Singh Dhanoa, a fighter pilot, was**

chosen as the new chief of India's air force to replace Air Chief Marshal Arup Raha. The appointments were announced on Twitter by a defence ministry spokesman late on Saturday. The appointment of Rawat, a counterinsurgency specialist, raised eyebrows among opposition parties because he was given the job ahead of two more senior candidates.

India, Tajikistan to step up anti-terror, defence cooperation
Press Trust of India, 2016 12 17
New Delhi - **Stating that they live in an extended neighbourhood that continues to face multiple security challenges, India and Tajikistan today decided to strengthen defence cooperation and inked a pact to share financial intelligence to counter money laundering and financing of terrorism.** The pact was among three signed by the two countries after comprehensive talks between Prime Minister Narendra Modi and Tajik President Emomali Rahmon on strategic issues including threats posed by radicalisation and extremism, trade and investments. "We assessed the broad progress achieved under different pillars of our bilateral engagement, including our partnership in defence and security. "India and Tajikistan live in an extended neighbourhood that continues to face multiple security challenges and threats.

S. Korea, Japan militaries directly exchange intelligence on N.K. for first time
Yonhap News Agency, Staff reporter, 2016 12 16
Seoul - **South Korea and Japan on Friday directly exchanged classified information on North Korea's nuclear and missile programs for the first time in line with their intelligence-sharing pact** which came into force last month, the defense ministry said. Defense ministry spokesman **Moon Sang-gyun** told reporters that the exchange was made during a meeting between the two countries' senior defense officials held in Seoul in conjunction with a three-way security dialogue which also includes the United States. "Under the recently-signed **General Security of Military Information Agreement (GSOMIA**), Seoul and Tokyo have shared intelligence on Pyongyang's nuclear and missile programs for the first time since the pact's signing last month," he said.

Spy agency produced documents detailing alleged surveillance of justices: sources
Yonhap News Agency, Staff reporter, 2016 12 16
Seoul - A **media executive's bombshell allegation about the state surveillance of senior judicial officials was based on documents written by South Korea's top spy agency**, government sources said Friday. **Cho Han-gyu**, former president of the local daily Segye Ilbo, claimed during a parliamentary panel on Thursday that the Park Geun-hye administration carried out illegal surveillance of senior judicial officials including Supreme Court chief justice Yang Seung-tae. On Friday, the presidential office denied the allegations as groundless. The sources, however, said the documents revealed by Cho carried watermarks used at only a limited number of state organizations, including the **National Intelligence Service**. The testimony came during the parliamentary hearing on corruption involving President Park Geun-hye and her confidante Choi Soon-sil.

N. Korea resumes encrypted numbers broadcast after 4-day break
Yonhap News Agency, Staff reporter, 2016 12 16
Seoul - **North Korea's state radio station resumed broadcasting mysterious numbers Friday after a four-day break that could be some kind of coded message to its agents operating in South Korea**. Radio Pyongyang, the Korea's state-run radio station, started broadcasting messages at 1:15 a.m. (Seoul time), calling out a series of pages and numbers before repeating them one more time. The radio announcer "gave review work in metal engineering to No. 27 expedition agents." The content was different from what has been transmitted this year. Since June 24, 18 of such encrypted numbers broadcasts have been

discovered, with the latest one broadcast Sunday. Broadcasts of mysterious numbers are considered a **kind of book cipher that was often used by North Korea to give missions to spies** operating in South Korea during the Cold War era. Spies could decode numbers to get orders by using a reference book, although **many intelligence officials believe this form of sending orders to be totally outdated**. Many have said the broadcast may be some sort of psychological strategy aimed at sparking internal confusion within South Korea.

FBI team was in Kolkata to get information on IS plan to hit US interests
Times of India, Neeraj Chauhan & Bharti Jain, 2016 12 16
New Delhi - The **Federal Bureau of Investigation (FBI) team's visit to Kolkata last week to question arrested Islamic State (IS) terror group operative Mohammad Masiuddin, alias Musa**, was essentially to gather more information on his Syria-based handler **Shafi Armar**, alias Yousuf al Hindi, and his alleged plans to harm US interests. According to top sources in the Indian security establishment, US agencies have been tracking the activities of Armar, who they suspect is in touch with radicalised American youth either looking to join or already recruited by IS. They also suspect Armar may be planning to target US interests and American citizens in India and elsewhere. After several hours of questioning Musa last Thursday, the seven- member team of expert FBI investigators shared their assessment on the IS operative with the **National Investigation Agency**.

Maj Gen Asif Ghafoor appointed DG ISPR
Pakistan Dawn, Dawn Report, 2016 12 15
Islamabad - **Major General Asif Ghafoor has been appointed as the new director general (DG) for Inter-Services Public Relations (ISPR).** He is presently commanding a division in Swat and will replace Lt Gen Asim Bajwa as DG ISPR. Lt Gen Bajwa was posted as Inspector General Arms at GHQ. Maj Gen Ghafoor was a part of the artillery regiment and also served in the military operations directorate, military sources said. The posting of officers with a track record in internal security and counterterrorism as the CGS and the ISI DG respectively also reinforces this impression.

Return to Table of Contents/ Retour à la table des matières

Africa / Afrique

Why SSS wrote separate reports to Presidency, Senate on Magu
The Premium Times, 2016 12 20
Abuja— The **actual trigger for the State Security Service (SSS) to have written the report upon which the Senate rejected Ibrahim Magu's nomination for the top job at the anti-graft EFCC has been uncovered**. At a hurriedly arranged press conference about the same time the Senate was ending a closed-door session on Thursday, the spokesperson for the Senate, Abdullahi Sabi, announced that Mr. Magu's nomination by President Muhammadu Buhari as EFCC chairman had been rejected. He cited "available security report" for the rejection. On Monday, the Senate Leader, Ali Ndume, claimed the Senate did not reject Mr. Magu's nomination but only suspended discussions on the matter until the SSS' concerns are resolved. PREMIUM TIMES' ongoing investigation into the procedural issues involved in the handling of Mr. Magu's nomination showed **the State Security Service actually turned in two reports on Mr. Magu. Both, though signed by one official, Folashade Ojo, on behalf of the Director General, Lawal Daura**, are contradictory, having different conclusions.

S Sudan spy kicked out of city flat wins right to return

Pretoria News, 2016 12 19
Pretoria—The South Sudanese refugee who had been battling with his country's embassy in Pretoria for more than a year feared for his life after being evicted from his flat. **Valentino Chan** filed an urgent application in the high court in Pretoria to be allowed back into the flat he was renting for his safety after the locks had been changed without his knowledge. In court documents filed on December 9, Chan said he had been living peacefully in the West Park flat since April until he was forced out last month. Chan **was the applicant in the matter lodged against Frans Oupa Makhafola, Little Manhattan Central Development Trust and the ministers of the State Security Agency and Defence**. Chan claimed that since August 2015 he was employed by the South Sudan embassy in South Africa. **He was to go on a secret fact-finding mission to spy on Dr Riek Machar**, the former president of South Sudan and rebel leader seeking asylum in South Africa.

«Le partage du renseignement, clé de la lutte antiterroriste»
El Watan (Algérie), Cherif Lahdiri, 2016 12 18
Oran, Algérie - Faire taire les armes d'ici 2020. C'est objectif de l'Union africaine (UA) pour qui **«le terrorisme est la préoccupation majeure du moment». Tel est le défi exprimé lors du 4e Séminaire sur la paix et la sécurité en Afrique qui s'est ouvert hier à Oran**. C'est la quatrième fois consécutive que ce rendez-vous annuel, qui a été institutionnalisé, il y a deux ans, par le Conseil de sécurité de l'Union africaine, a lieu en Algérie. Oran abrite, durant trois jours, ce séminaire impulsé par l'Algérie qui réunit une soixantaine de participants de 14 pays africains mais aussi des invités venus d'Europe et d'Asie. Dans son allocution d'ouverture des travaux, le ministre d'Etat, ministre des Affaires étrangères et de la Coopération internationale, Ramtane Lamamra, a plaidé pour «une **meilleure coordination des approches et pour davantage de mutualisation des moyens d'autant plus que le nombre de crises et conflits en Afrique représentent les deux tiers des questions à l'ordre du jour du Conseil de sécurité**».

Return to Table of Contents/ Retour à la table des matières

Americas / Amériques

'Assange' Doc Suggests Russia Knew In Advance Ed Snowden Would Spy on NSA
Heat Street website, Louise Mensch, 2016 12 14
New York - **Senior Russian intelligence officers from Cuba visited the head of Ecuadorean intelligence in Quito, days before Edward Snowden stole a tranche of top-secret files from the National Security Agency in the United States**. A classified document held by **SENAIN, Ecuador's spy agency**, in its embassy in London, reveals that Colonel Alexander Kazalupov of the FSB, and his deputy, one Igor Lebedev, were given a letter of credentials by the then Russian Ambassador to Ecuador, Yan Burliay, introducing them to the head of SENAIN in Ecuador's capital. The short letter is dated April 4th, 2013, and confirms a meeting on the same day at ten o' clock in the morning. Diplomatic language is used in the short note, and the Ambassador states the meeting is "in order to address issues of bilateral cooperation". The note is a record of a meeting between Russian and Ecuadorean spies in Quito, Ecuador.

Return to Table of Contents/ Retour à la table des matières

Today's News / Actualités
April 26, 2016 / le 26 avril 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Le ministre Marc Garneau attendu de pied ferme à Lac-Mégantic ce soir
C'est un moment que plusieurs Méganticois attendent avec impatience : le nouveau ministre des Transports du Canada, Marc Garneau, ira à la rencontre des citoyens de cette municipalité grandement éprouvée par une tragédie ferroviaire en 2013. Marc Garneau tient ainsi une promesse faite aux Méganticois dans la foulée du plus récent budget déposé par le gouvernement Trudeau. Le ministre doit rencontrer le maire Jean-Guy Cloutier en après-midi ainsi que la Coalition des citoyens et organismes

engagés pour la sécurité ferroviaire. En soirée, une rencontre publique aura lieu au Centre sportif et la population sera invitée à poser des questions au ministre Garneau. Radio-Canada

Les projets de Barrette inquiètent les ambulanciers
Les ambulanciers paramédicaux de la région de Mégantic craignent que les intentions exprimées la semaine dernière par le ministre Gaétan Barrette n'entraînent de nouveaux délais pour la population.Jeudi dernier, le ministre de la Santé et des Services sociaux a annoncé des mesures de sa réforme des services préhospitaliers d'urgence. Ces nouvelles politiques font suite aux rapports Ouellet, intitulé Urgence d'agir, et Robillard, qui scrutait l'ensemble des programmes gouvernementaux. Le ministre Barrette croit pouvoir récupérer 110 millions $ en appliquant certaines recommandations. La Presse

Salon du commerce à Lac-Mégantic
Le salon du Commerce organisé par Lac en fête Mégantic ce déroulera ce week-end. L'événement a pour but de rassembler les commerçants locaux de la région de différents secteurs tel la rénovation, la construction et l'aménagement extérieur. Il sera de retour dès vendredi au Centre Sportif Mégantic. Les portes ouvriront le vendredi à 18h00 jusqu'à 21h00. Le samedi de 13h00 à 21h00 et le dimanche de 11h00 à 16h00. O97.3

DiNapoli to feds: Strengthen safety measures for oil trains
State Comptroller Tom DiNapoli has written to the head of the federal Department of Transportation urging the feds to increase oil train safety measures. "Any train accident involving crude oil or other hazardous materials creates the risk of significant human trauma and disruption to communities,"DiNapoli wrote in a seven-page letter to USDOT Secretary Anthony Foxx. "The possibility of an accident on the scale of the Lac-Mégantic (Quebec) tragedy is not only a significant hazard to New York residents and environmental resources — it is also a financial threat. Times Union

Time for Quebec to allow pipeline
A letter to the editor states, "TransCanada's Energy East pipeline would be one of the biggest infrastructure projects in Canadian history, crossing six provinces and traversing 4,600 kilometres. Roughly two thirds of it would make use of underused natural gas pipe that's already in the ground, with new pipe being built through Quebec and New Brunswick. Quebec is now having more studies to discover if the energy east pipeline is safe enough to transport oil from Alberta to eastern Canada... Have they forgot the train derailment in Lac Megantic, Que. where this town was nearly destroyed and many lives were lost from exploding oil tankers? Instead of Canada using our own country's oil and supporting our fellow countrymen, they would rather support a dictatorship that treats its people very poorly..." Charlottetown Guardian

Four fires in Northeast Region so far
There is currently one active fire in the region, says the Ministry of Natural Resources and Forestry in a news release. Hearst 1 is under control at five hectares. The forest fire hazard will continue to move north as the snow melts. So far this season we have seen four fires in the Northeast Region, one in Parry Sound and two in North Bay. Sudbury.com

Evacuation order lifted near Fort St. John
A fire 50 kilometres northwest of Fort St. John has calmed down enough for people to go home. On Monday afternoon, at around 2 p.m., the Peace River Regional District lifted an evacuation alert for the Beatton Airport Road fire. The fire is 7,035 hectares in size and 30 per cent contained, but the Beatton Airport Road is now open. Kelowna Now

NATIONAL SECURITY / SÉCURITÉ NATIONALE

PM should lead charge to wipe out killer terrorists
An opinion piece states "They were evil barbarians even before the savage slaying of an innocent Canadian. Prime Minister Justin Trudeau is now "outraged" at the beheading of John Ridsdel in the

Philippines, but what did he have to say a month ago when the radical Islamic killers threatened their hostage. Nothing. In fact, Trudeau was at the White House socializing with President Barack Obama as Ridsdel cried out at gunpoint "to the Canadian prime minister and to the Canadian people in the world: Please, do as needed to meet their demands within one month or they will kill me, they will execute us." They were true to their word. "Canada condemns without reservation the brutality of the hostage takers and this unnecessary death," Trudeau said Monday. "This was an act of cold-blooded murder and the responsibility rests squarely with the terrorist group who took him hostage." The PM needs to explain why he didn't name the terror group or its affiliations. Abu Sayyaf has long been affiliated with al-Qaida and, in recent months, flying ISIS flags. What should have been considered was a military extraction exercise led by Canada's crack JTF2 counter-terrorism team with air support from our now idle CF-18 Hornets. These killers should be wiped out." Postmedia (Toronto Sun, Winnipeg Sun, Ottawa Sun, Edmonton Sun)

Live-tweeting a terrorist attack: How the public's posts can help in an emergency
When she heard about the shooting, Cpl. Wendy Stewart wanted to be on Parliament Hill. She wanted to protect her colleagues, her friends and her city. Like many RCMP members in Ottawa on Oct. 22, 2014, her first thought was to rush downtown.Instead, she got to work. Minutes earlier, the nation's capital had been peaceful. At the National War Memorial, three sentries from the Ceremonial Guard stood watch nearby — among them, 24-year-old Cpl. Nathan Cirillo. The calm was broken with the thunder of bullets. Michael Zehaf-Bibeau, a 32-year-old seeking retaliation for Canada's military involvement in Afghanistan and Iraq, approached Cirillo and fatally shot him twice in the back. Zehaf-Bibeau fled to the Hill only blocks away and ran inside Centre Block, where he exchanged fire with a squad of RCMP tactical officers and the Sergeant-at-Arms of Parliament. Moments later he was dead, ending the most vicious attack on Parliament in more than 50 years. From start to finish, the entire attack lasted less than ten minutes. Stewart's job was to wade through the information deluging social media, hoping to find any information that could help during the attack — watching what police call the open source, everything from Twitter to Instagram. "As soon as we heard about the shooting, we were doing social media searches," says Stewart. "Immediately, we went on the sites to see what we could find — seeing if anyone was talking about it online. Immediately, we were finding information. Before it was on the news, we found it on Twitter." (…) Stewart and Cpl. Judy Montreuil spent hours together poring over the data at the RCMP's Protective Investigation Unit (PIU) — watching the shock and terror of those downtown, scanning through grainy cellphone footage, clicking through graphic images from the war memorial. By using specific hashtags and geolocation tools, analysts were able to build a rough picture of what was happening downtown. Out of the Internet's noise and chaos, they managed to find a handful of important leads — crucial information for the members tasked with securing downtown. RCMP

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Jonathan Nicola to remain in custody, review board determines
Jonathan Nicola will remain in custody as he's considered a flight risk, an Immigration Refugee Board determined Tuesday. His next detention hearing is scheduled for May 24, but he could have an admissibility hearing as early as this week to determine whether he will be allowed to stay in Canada or be sent home to South Sudan. Nicola is accused of entering the country using false information on his passport from South Sudan. Canada Border Services Agency officials allege he came to Canada in November 2015 on a student visa to study in Windsor until January 2017. When he entered the country his passport and visa application listed his birth date as November 1998. But when he applied for a U.S visitor visa in April, his fingerprints matched an individual who'd already applied for a visa with a birth date in November 1986, the CBSA alleges. If the allegations are proved, that would make him 29, not 17, as his documentation suggests. CBC News, CTV News, Windsor Star

Coach of Canadian teen impostor Jonathan Nicola: Doubts overcome by documents
In the aftermath of the Jonathan Nicola scandal, anyone and everyone who has come into contact with the 30-year-old South Sudanese refugee has been put under the microscope as the general public struggles to understand how no one learned Nicola was 13 years older than he claimed to be. No one has received more of that wrath than Catholic Central basketball coach Peter Cusumano, who not only

coached the player but also put him up in his home. In the lone interview the coach has provided since Nicola was detained when trying to cross the U.S. border, Cusumano defended his own role in the incident, insisting that he agreed to help and coach Nicola because he had copious official paperwork stipulating that he was a 17-year-old athlete fleeing South Sudan. "He'd been vetted twice by government officials and arrives with all his documents," Cusumano told The Windsor Star, which held a conversation with the coach. "Is the school supposed to call Canadian Border Services and tell them they got it all wrong? We have over 400 kids here (Catholic Central) who were born outside the country. We don't have the resources to deal with that. "What's been tough to take are the insinuations that I knew his age all along. If that was the case, I'd be an idiot for taking him to the U.S. embassy to get a visa, knowing he had false documents. USA Today

Jacobus Van Nierop, 'horror dentist,' found guilty in France

A French court has found a Dutch dentist guilty of assault and fraud and sentenced him to eight years in prison. Dentist Jacobus Van Nierop, 51, showed no signs of emotion when the court in the central town of Nevers returned its verdict Tuesday. The court barred him from practising dentistry for life. About 100 people had issued complaints against Van Nierop, ranging from having multiple healthy teeth removed, pieces of drills left in their gums and teeth or abscesses and misshapen mouths after he did work on patients. Van Nierop was accused of causing "mutilations" or "permanent disabilities" to scores of patients from 2009 to 2012 and of overcharging patients and billing them for imaginary procedures. (…)The Dutchman eventually fled to New Brunswick, and was arrested in Nackawic, about 60 kilometres west of Fredericton, where he had been living for about eight months. Then the RCMP officers and members of the Canada Border Services Agency arrived, Van Nierop was in the bathroom and refused to come out. The officers forced their way in and found him sitting on the toilet, covered in blood. It appeared he had tried to commit suicide, according to a 2014 immigration decision. He was extradited to the Netherlands and then deported to France. CBC News, Radio-Canada, The Guardian (St. John's Telegram), L'Actualité

Demands for change to Canada's immigration detention system mount in wake of deaths

Nearly 80 detainees at Central East Correctional Centre in Lindsay, Ontario ended a hunger strike over the weekend that was initiated last Thursday April 21. The strike had been an effort to draw attention to indefinite immigration detention and recent inmate deaths. The detainees -- all racialized, undocumented men -- have two main demands: end immigration detention and "end indefinite and maximum security imprisonment, overhaul the judicial review process, and improve prisons conditions." According to the End Immigration Detention Network, the strike concluded after the Canadian Border Services Agency (CBSA) promised to provide updates and answers to these issues in two weeks. There have been at least 13 deaths in Canadian immigration detention since 2000 -- most of which have had minimal explanation or understanding. The most recent death, which occurred on March 13 2016, was of Francisco Javier Romero Astorga, a 39-year-old Chilean father of four. Since his death, Astorga's family has been very active in seeking answers and justice within Canada's immigration system. Rabble

FDFA reports March land border and airport statistics

The Frontier Duty Free Association (FDFA) has released the latest duty-free sales statistics, provided by the Canadian Border Services Agency for March. The national land border duty-free sales figure of C$9.5m ($7.5m) represented a 10.38% sales increase compared to March 2015. Sales between January and March increased around 12% compared to the same period in 2015. Sales at land border duty free shops for January/ March 2016 equaled $25.8m. Airport duty-free store sales for March totalled C$32.7m, an 8% drop compared to March 2015. Sales between January and March rose 7% compared to the same period in 2015. Canadian airport duty-free shops from January to March equalled $96m. DFNI Online, Moodie Davitt Report

Revealed: winners of Canada's senior public service awards

The winners of this year's senior public service awards of excellence in Canada have been revealed today. High-ranking public servants have been recognised for their management skills in four categories, including leadership, innovation and partnership, in an annual competition organised by the Association of Professional Executives (APEX). (…) The career contribution award, which recognises a senior official who has brought recognition to the public service or to their department or agency over a federal public

service career spanning at least ten years, went to Norm Sheridan, executive director, Greater Toronto Area, Canada Border Services Agency. Global Government Forum

Le Canada menace une femme et son fils de les renvoyer en Algérie
Adel, 17 ans, est né à Montréal. Il n'y a jamais vécu. Avec sa mère, Nadia, il a été exilé de force en Algérie en l'an 2000 et abandonné dans des conditions d'extrême pauvreté par un père qui voulait se débarrasser d'eux. Quinze ans plus tard, lui et sa mère viennent enfin de regagner le Canada, mais leur cauchemar n'est pas fini. Nadia a perdu sa chance de vivre ici. Les autorités canadiennes veulent la renvoyer en Algérie. Nadia Chikhi n'avait presque rien mis dans ses valises : des cadeaux pour sa famille en Algérie, deux robes pour elle et deux habits pour son bébé. Et c'est tout. Elle n'avait pas besoin de grand-chose. Elle ne partait que pour une semaine. Puis retour prévu dans son logement de Saint-Léonard avec mari et enfant. Elle devait commencer un nouvel emploi dans une garderie du quartier la semaine suivante. Elle ne s'y est jamais présentée. Il a fallu à la femme, aujourd'hui âgée de 46 ans, et à son fils 15 longues années pour regagner Montréal. (...)Adel est citoyen canadien, mais sa mère est sous le coup d'un interdit de territoire. Elle a perdu sa résidence permanente parce qu'elle n'a pas passé le nombre de jours requis par la loi en sol canadien. Elle s'adresse maintenant à la Cour fédérale en tout dernier recours. (...)En 2008, nouvelle lueur d'espoir : Nadia a reçu une lettre du Canada. « J'ai pensé que j'allais enfin avoir de l'aide. » On lui disait que sa demande de résidence permanente était en voie d'être accordée et qu'elle recevrait bientôt un visa pour le Canada, obligatoire pour les citoyens algériens qui souhaitent venir ici. Le hic : Nadia n'avait pas demandé sa résidence permanente. Elle la détenait déjà. En fait, tout ce qu'elle aurait eu à faire, c'était de demander un titre de voyage. Elle ne le savait pas. (...) La femme fait l'objet d'une mesure de renvoi, une épée de Damoclès au-dessus de sa tête et de celle de son fils. La Presse

U.S. fugitive for more than a decade arrested in Toronto
A man wanted in the United States for more than a decade is under arrest in Toronto. Delroy McGowan allegedly fled from the U.S. in 2004 while facing charges in an investigation involving firearms and serious drug offences, Toronto Police said Tuesday. McGowan was convicted in absentia and faces up to 60 years in prison, police said. Police said they believe McGowan fled to Jamaica, where he is a citizen, before allegedly entering Canada under a false name. A story featuring McGowan as a top 10 wanted fugitive in 2014 generated information that led to his arrest last week, police said. McGowan is being held in custody pending his extradition to the U.S. Canadian Press (Edmonton Sun, Ottawa Sun, Calgary Sun, Toronto Sun, Winnipeg Sun)

Americans flock to Canada, lured by the low-loonie discount
Americans are flocking to Canada at a pace we haven't seen in years, helping to pump up the retail and tourism industries. No, they're not Trump refugees, but rather shoppers enjoying the automatic discount from the low loonie. Over the course of the last two years through to February, noted BMO Nesbitt Burns, the number of American visits north has surged 20 per cent. That's more than two million for the first time in eight years, said BMO senior economist Sal Guatieri. (...) One of the gauges of cross-border shopping are same-day trips, which Mr. Rangasamy's research shows is now on the rise from the U.S. at the fastest pace in six years. Globe and Mail, CTV News

Ex-Kent State professor accused of trying to have sex with boy arrested in Louisiana

A former Kent State University professor accused of meeting a teenage boy for sex in an elementary school parking lot is back in police custody, five months after he was stopped at the Canadian border trying to leave the country. Willie Harrell, 44, was booked in the Summit County Jail about 1:30 a.m. Saturday. He was arrested March 22 in Orleans Parish, Louisiana. He waived his extradition hearing the next day and was sent back to Akron April 15, according to Orleans Parish Magistrate Court records. He is scheduled for a May 2 appearance in front of Summit County Judge Amy Corrigall Jones. Harrell faces a fifth-degree felony charge of importuning (…) Harrell was stopped trying to cross the border of Detroit, Michigan and Windsor, Ontario, according to court records. Harrell told Canadian authorities that he was trying to leave the country to avoid prosecution in his pending case in Summit County Common Pleas Court, according to a court filing by prosecutors. Harrell also had a device in his car that blocked GPS location tracking, according to court records. He was released to U.S. Border Patrol agents several hours later. Cleveland (2016-04-25)

Broadcast media / Médias télédiffusés

Jonathan Nicola, the high school basketball player who may be almost 30 years old, faced his second detention review hearing in front of the Immigration and Refugee Board of Canada. He will remain in custody until his next court date. He remains detained due to the flight risk and he has a history of using fraudulent documents. (CKLW-AM Windsor, 11h01)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Cybersecurity Alliance forms to help Canadian infosec groups work together
IT security professionals in Canada often form groups to share information with members, but rarely outside the group. Now they're coming together in a national network to broaden information sharing and best practices across industries. The Canadian Cybersecurity Alliance was quietly launched earlier this month with a goal of marshalling more resources to stand up to online attackers. So far 50 groups have agreed to participate in the alliance (see below for a partial list). The alliance is led by a 12-person national council co-ordinated by Gilles Racine, a member of Bell Canada's information security response team. IT World Canada (2016-04-25)

The shifting sands of cybersecurity
An ounce of prevention is worth a pound of cure, so the saying goes, and while it may seem trite, for in-house counsel who have to deal with the aftermath of a cyberattack or data breach, that recommendation overwhelms all others. When intellectual property and customer information falls into the wrong hands, how well prepared the organization is for such an eventuality will determine the ramifications. While it would appear that most organizations in Canada have a handle on the technological aspects of cybersecurity, there is still a ways to go when it comes to pre-emptive planning in case of a data breach and involving in-house counsel so they can contribute.. Canadian Lawyer Magazine (2016-04-25)

Spy Chief Complains That Edward Snowden Sped Up Spread of Encryption by 7 Years
On Monday blamed NSA whistleblower Edward Snowden for advancing the development of user-friendly, widely available strong encryption. "As a result of the Snowden revelations, the onset of commercial encryption has accelerated by seven years," James Clapper said during a breakfast for journalists hosted by the *Christian Science Monitor*. The shortened timeline has had "a profound effect on our ability to collect, particularly against terrorists," he said. When pressed by *The Intercept* to explain his figure, Clapper said it came from the National Security Agency. "The projected growth maturation and installation of commercially available encryption — what they had forecasted for seven years ahead, three years ago, was accelerated to now, because of the revelation of the leaks." Asked if that was a good thing, leading to better protection for American consumers from the arms race of hackers constantly trying to penetrate software worldwide, Clapper answered no. "From our standpoint, it's not … it's not a good thing," he said. Intercept; Washington Times

LAW ENFORCEMENT / APPLICATION DE LA LOI

Sask. man wins RCMP contest to name puppies
The RCMP have announced the winners of their national Name the Puppy Contest, and among the winners is Battleford, Sask. man, Lucas Anthony. Of the 16,000 entries, Anthony was one of 13 winners choosing the name Jett for one of the puppies. During this year's contest, all the names were required to start with the letter J. The winning entries include the names: Jango, Jolt, Jade, Jorgia, Jade, Jix, Jett, Jax, Juno, Java, Jinx, Jazz and Jake. The winners will each receive a certificate and a photo of the puppy they named. CBC; StarPhoenix

Quebec's independent investigation unit beset by delays
The Quebec government's planned independent bureau to investigate shootings, serious injuries and deaths involving a police officer is faced with another round of delays. The province approved a proposal three years ago to create the Bureau des enquêtes indépendantes, but it's still not operational. The bureau's latest targeted opening date was April 29. But Madeleine Giauque, a former Crown prosecutor was named its director in late 2014, told a parliamentary committee last week she would need more time to ensure the new unit can also handle allegations of sexual assault against police. The decision to add that investigative element to the bureau was made following allegations of abuse against police in Val-d'Or last year. The most recent delay to the bureuau comes following a string of police shootings, including the death of a 60-year-old man in Hochelaga-Maisonneuve on Monday following an intervention by Montreal police. The Sûreté du Québec, which took over the investigation, said officers were were called to the apartment block to check on someone in psychological distress and that the man had a knife. Provincial police say a stun gun was used in the police operation and the man was also struck by at least one bullet. Earlier this month, Sandy Tarzan Michel, 25, was fatally shot by a member of the local aboriginal police force in Lac-Simon. CBC

Murder charge laid against father after Carbonear fire
Harbour Grace RCMP have charged the father of the five-year-old girl who died in a house fire in Carbonear this past weekend with first degree murder and arson. Trent Butt, 37, will make a court appearance on Tuesday. The girl's body and Butt were found in their burning home early Sunday morning. Butt was transported to hospital, where police say he remains in serious condition but he is expected to survive. Court records show Butt faced three assault charges against his wife in the past, but all were dismissed. RCMP are not releasing the name of his daughter at this time, but will provide an update after Butt's court appearance. CBC News; Guardian; Brandon Sun

La GRC recherche un deuxième suspect armé et dangereux à Steinbach
La Gendarmerie royale du Canada (GRC) est à la recherche d'un deuxième suspect, qui aurait participé à une entrée par effraction à Steinbach, le 18 avril dernier. Jean Pierre Gagnon, 32 ans, est considéré comme étant armé et dangereux. Il fait face à plusieurs accusations liées à des actes violents et à l'utilisation d'une arme à feu. Il est le deuxième suspect qui aurait participé à l'entrée par effraction survenue à l'avenue Brandt, au cours de laquelle une personne a fait feu en se disputant avec l'un des résidents. Personne n'a été blessé lors de l'incident, mais la police croit que ces individus visaient précisément cette résidence et ses habitants. La GRC indique que Jean Pierre Gagnon aurait des contacts à Winnipeg et à Sainte-Anne. Elle demande à quiconque aurait de l'information de communiquer avec elle pour tenter de retrouver l'homme. Les autorités demandent particulièrement aux résidents de Winnipeg et du sud-ouest de la capitale manitobaine d'être à l'affut. L'autre suspect, Harley William Delorme, 24 ans, a été arrêté jeudi dans une résidence de Winnipeg. Radio-Canada

RCMP arrest Caleb Head; man wanted for attempted murder
RCMP say they have arrested Caleb Head after an attempted murder over the weekend near Carrot River. Mounties say Head was wanted on many charges after an alleged assault on the weekend. Mounties were called to the First Nation in the Carrot River area after a woman was found outside a home in the community early Sunday morning. Police says Head was arrested late Monday night in the community of Red Earth First Nation. The investigation is continuing; however, it is anticipated Head will make his first appearance in Provincial Court at 10:00 a.m. on Wednesday, April 27, 2016 in Nipawin, Saskatchewan. 620 CKRM

Mississauga murder victim ID'd as GTA rapper
A Toronto man shot dead in Malton on the weekend is a GTA rapper named Sizzlac who recently released a new video on YouTube, according to friends and fans. Peel Regional Police identified Mississauga's third murder victim of 2016 as Mustafa Omar, 29, of Toronto. Friends have been paying tribute online to Omar, known to many as Sizzlac, saying he was born and raised in "one of the most notorious blocks in Toronto, Jamestown Rexdale." He recently released a video on YouTube called "Realest in the 6." Homicide detectives in Peel continue to investigate the fatal shooting. Omar died early Saturday morning after gunshots rang out at a townhouse complex in the area of Goreway Drive and Morning Star Drive in Mississauga around 5:30 a.m. Omar was shot multiple times, police said. Peel Region Paramedics rushed him to hospital but he was pronounced dead there. Three others were also shot. One has been released from hospital while the other two suffered non-life threatening injuries. Neighbours have identified the home where the shooting occurred as a "party house" and have called police to complain about noise and illegal activity at the home. Hamilton Spectator

Coquitlam RCMP officer's disciplinary hearing may never see light of day
R.C.M.P. have adjourned a disciplinary hearing for an officer seen in online photos wearing his force issued boots and not much else. It has been four years since Coquitlam Corporal Jim Brown was suspended with pay. Now there is new information on why the case may never see the light of day, and what the long-time officer has been up to while collecting a paycheque. Brown's disciplinary matter has been one of several that have left the Mounties with a tarnished image. In 2012, bondage pictures emerged of Brown in sexually explicit poses with a woman. They were posted by Brown on a personal account on the "bondage, BDSM & fetish" community Fetlife, which he believed would be private. The pictures ended up being released to media, which subsequently sparked an internal R.C.M.P. investigation and Brown was put on paid leave. CKNW

White Butte RCMP along with Regina Police investigate B&E in Pense
A break-in in the town of Pense has RCMP looking for two men who made off with compound bows valued at nearly 5-thousand dollars. It happened overnight Sunday when someone reported a B&E at the residence. RCMP say two men forcibly entered a residence around 3:15 a.m. allegedly using a firearm looking for money and property. As well as the two compound bows, the thieves took off with an unknown amount of cash. There were two people inside the home at the time of the offence – a man received minor injuries while a woman was not physically injured. The two individuals are described as First Nations men: one was 5'9" – 5'10", 180 lbs, short brown hair, fair skin, 24 – 28 years old. 620 CKRM; CJME

Sûreté du Québec probe role of stun gun in fatal police shooting
Quebec provincial police are investigating why a stun gun and a firearm were used in an intervention Monday that led to the death of a 63-year-old man. André Benjamin, 63, was pronounced dead in hospital after police were called earlier in the day at an apartment in Hochelaga-Maisonneuve.
The Sûreté du Québec said a stun gun was deployed by an officer and that Benjamin was also struck by at least one bullet. "At this point, it would be irresponsible to come up to a conclusion on if it [the stun gun] did not work, or if there is a problem, or exactly what happened," Allard told CBC Montreal's Daybreak on Tuesday. "I think as we go through the investigation we'll have a lot more details that will follow." Allard said that Montreal police officers were called to the apartment block to check on someone in psychological distress. Benjamin had a knife, he said. Allard wouldn't go into details about what transpired next, saying they are still interviewing witnesses and gathering evidence. Montreal police haven't commented on the incident since it was handed over to the SQ. CBC

RCMP investigate alleged kidnapping west of Edmonton
A suspect has been arrested and RCMP are investigating after a woman was kidnapped near Evansburg, Alberta. On Monday evening, a police presence could be seen at the western edge of Alberta's capital by 103 Avenue and Winterburn Road. RCMP wouldn't say how but did confirm the scene is connected to their investigation. A man was also seen being taken into custody at that location. According to police, the vehicle the suspect was driving in was stopped after a spike belt was deployed on a road in Parkland County. Mounties said they believe the kidnapping incident originated west of Evansburg, which is about

110 km west of Edmonton. They said they believe it involved a man and woman who knew one another. Police said the woman is accounted for and in good health. Global News

Broadcast media / Médias télédiffusés

City officials blame a turf war between alleged gang members for a shooting yesterday in the community of Williams Lake. The RCMP is not linking this directly to a turf war. The Minister of Public Safety in B.C. is saying it's not a gang war, it's simply local rivalries. (CBC News, 9h15 ET)

CTV News reports 13 puppies born at the RCMP Police Dog Service Centre were named following a contest. Rough Transcript

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Elders use culture to heal Indigenous inmates from sexual violence
Elder Amy Victor of the Stó:lo Nation is no ordinary grandma. Five days a week she drives from the Cheam reserve to Abbotsford. B.C., where she willingly walks through the gates of the Fraser Valley Institution for Women. But the 74-year-old elder is not a prisoner or a guard. Her unique position, spiritual advisor, allows her to help Indigenous women heal the damage wrought by sexual abuse using a simple, potent formula: traditional teachings, Indigenous medicines, indomitable spirit. Indigenous women make up a disproportionate number of federal inmates in Canada. Many are survivors of a history of sexual violence before they arrive in prison. As one prison counsellor put it, "The women didn't even know it was possible not to be abused." (…) Incarceration rates for Indigenous women continue to climb. Canada's correctional investigator stated that the system is failing Indigenous peoples and culturally-appropriate alternatives are needed. Victor guides Indigenous inmates toward "the good path" by reintroducing cultural practices most of the women were denied or never knew due to Canadian assimilation policies. Victor says many women grew up in foster care and don't have a connection to their parents or grandparents. "Being disconnected from the culture caused them to be lost," she says. Only a fraction of Indigenous offenders identified with First Nations spirituality upon entry to the prison, according to a 2000 Corrections Canada study. (…) Despite challenges, some early results show improvements for Indigenous inmates involved in "Aboriginal-specific" programming. Indigenous offenders who participated in Pathways units had a 17 per cent rate of re-offense compared to 35 per cent in standard units. Inmates and staff at Healing Lodge facilities were also less likely to be involved in violent incidents and more likely to complete parole after release. These practices mark a slow shift from standard correction conventions. CBC News

« Je ne suis pas raciste, mais... »
Le 7 avril sur les ondes de CHOI FM (1), l'animateur de radio André Arthur, qui n'en est pas à ses premiers propos controversés, a déclaré que selon lui, Haïti est un pays « sans avenir, peuplé de voleurs, inventeur du sida ». Ses propos racistes faisaient aussi suite à une avalanche de commentaires xénophobes, particulièrement via la section des médias web du Québec, après la mort le 4 avril de Jean-Pierre Bony, Haïtien d'origine tué par une balle de plastique tirée à la tête par un policier de Montréal lors d'une perquisition. Il faut savoir qu'au Québec, dès qu'on ose faire allusion au spectre du racisme, on vous accuse immédiatement de faire du « Québec bashing » ou de jouer à la victime. Nous semblons collectivement plus enclins à nier aveuglément son existence plutôt que d'être fier d'amorcer un dialogue afin de développer des outils pour lutter contre celui-ci (…) Le plus alarmant, comme l'indique une étude réalisée par l'université McGill, c'est que le premier facteur déterminant une plus grande présence policière dans une ville n'a rien à voir avec le taux de criminalité qui y sévit, mais dépend uniquement du nombre de minorités racisées et de populations autochtones qui y vivent. Ces décisions de nos élites politiques non seulement entérinent que la répression policière est justifiée du seul fait de la race, ce qui en soit rend légitime la violence envers les communautés racisées, mais en plus, elles ne peuvent faire autrement que de judiciariser et d'incarcérer massivement des citoyens principalement à cause de la couleur de peau. D'ailleurs, en 2013, le rapport de l'enquêteur correctionnel Howard Sapers révélait qu'au cours des dix dernières années, la population carcérale autochtone a augmenté de 46,4 % ; celle

des Noirs, de 80 % ; tandis celle des femmes a plus que doublé, particulièrement celle des femmes autochtones. Presse gauche

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

La violence en baisse dans les écoles du Québec, selon une étude
Les agressions à caractère violent et l'intimidation sont en baisse dans les écoles du Québec. *L'Enquête nationale sur la violence à l'école 2013-2015*, dont les résultats sont dévoilés mardi à Québec, révèle des changements notables dans les comportements des élèves, particulièrement au primaire. Les insultes, les bousculades, les menaces sur le chemin de l'école et les propos à caractère homophobes étaient moins fréquents chez les élèves du primaire en 2015 qu'ils ne l'étaient deux ans auparavant. Une différence selon le sexe est toutefois observée. La violence sociale et les insultes sont en diminution chez les filles du primaire, mais pas chez les garçons, selon l'étude menée par des chercheurs de l'Université Laval. Au secondaire, les diverses formes de violence subies par les élèves sont restées stables de 2013 à 2015. Les statistiques laissent néanmoins entrevoir un nombre moins élevé d'insultes et de vols, notamment. (…) Même si le phénomène de cyberintimidation n'a subi aucune hausse entre 2013 et 2015, la proportion de jeunes possédant un téléphone cellulaire a augmenté de façon importante. En 2013, 61 % des jeunes du primaire disaient posséder un téléphone cellulaire, comparativement à 76 % en 2015. Au secondaire, l'augmentation est tout aussi importante : 77 % des jeunes possédaient un téléphone en 2013, comparativement à 88 % en 2015. Les élèves du secondaire rapportent aussi être plus nombreux à avoir accès à Internet sans la surveillance d'un adulte, tant à la maison (96 %) qu'à l'école (53). Radio-Canada, Journal de Québec

Region's public health department calls for 'real time' information on drug use
The Region of Waterloo Public Health Department wants access to real time information when it comes to monitoring and surveillance of opioid use, and in particular, overdoses. Right now, region health officials can access numbers from 2014, and the data from 2015 won't be available until later this year or possibly next year. That's a problem for Chris Harold, the manager of information and planning with the region's health department. "We often can't tell challenges or problems sweeping through the community until well after the fact," Harold told CBC's The Morning Edition. "So in many cases … we won't know the roll or if the number of deaths related to drug overdoses in particular opioids is increasing until well after the fact. This consistent, real time monitoring will help us give more relevant information so we can respond in a timely manner." The latest drug of choice and concern for officials is fentanyl. "We are aware that fentanyl is in the community … police issued an alert that fentanyl was present in the local drug supply in March," Harold said. The synthetic opiod narcotic, which is used as a painkiller, comes in pills or patches. The drugs being picked up by officers on the streets include both prescriptions and bootleg versions. CBC News

Stress post-traumatique : les agents des services correctionnels du N.-B. veulent être inclus dans la loi
Les agents des services correctionnels du Nouveau-Brunswick demandent que le stress post-traumatique soit reconnu comme une maladie liée à leur travail. Le gouvernement reconnaît déjà cette maladie pour les pompiers, les policiers et les ambulanciers. Pourtant, les agents correctionnels disent eux aussi vivre des situations parfois très difficiles, qui se comparent à ce que peuvent vivre des policiers ou des ambulanciers. Maurice LeBlanc est agent des services correctionnels et vice-président de la section locale du syndicat canadien de la fonction publique. Il travaille au Centre correctionnel régional du Madawaska depuis de nombreuses années et connaît des confrères touchés par le stress post-traumatique. « On a des gens qui ont découvert des détenus décédés ou qui étaient pendus. Suite à ces incidents, ils ont lâché la "job", explique M. LeBlanc. Ils n'en pouvaient plus, ils ne pouvaient pas revenir au travail, ils ont juste démissionné parce qu'ils ne pouvaient plus faire le travail. » Il souhaiterait que le stress post-traumatique soit reconnu par Travail sécuritaire NB. Radio-Canada (2016-04-25)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

#MMIW : au nom des femmes autochtones disparues ou assassinées
La création d'une commission d'enquête nationale sur les femmes et les filles autochtones disparues ou assassinées a été l'aboutissement de plusieurs années d'efforts pour Sheila North Wilson. Celle qui a réussi à mobiliser une nation grâce au mot-clic #MMIW connaît bien les défis qui attendent les jeunes filles des réserves autochtones qui partent vers les grandes villes, car elle a dû traverser elle-même de nombreuses épreuves. Sheila North Wilson a grandi à Oxford House, une réserve située à environ 960 km au nord de Winnipeg qui est réputée pour ses conditions de vie déplorables. Or, son enfance est remplie de beaux souvenirs. « Je pensais qu'on était riches, mais c'est juste que nos parents s'occupaient très bien de nous », se remémore-t-elle. Elle a tout de même vécu des moments sombres. À compter de l'âge de six ans, elle a été agressée sexuellement à plusieurs (…). « Les policiers ne prenaient pas les histoires de ces femmes au sérieux ou ils ne poursuivaient pas certaines pistes, explique-t-elle. Je sentais que je pouvais en faire plus si je m'impliquais directement dans la cause. » Elle quitte son poste de journaliste et devient relationniste à l'Assemblée des chefs du Manitoba. Mais elle découvre une réticence chez les chefs - surtout des hommes - d'aborder publiquement la question des femmes disparues. En juin 2012, un événement galvanise la communauté des Premières Nations du Manitoba : un homme se rend à la police et avoue avoir tué trois femmes autochtones. Les leaders autochtones et les intervenants sur le terrain manifestent ensemble. C'est aussi à ce moment que Sheila a créé le mot-clic #MMIW - Missing and murdered indigenous women (femmes autochtones assassinées ou disparues), qui a depuis été repris plusieurs millions de fois sur les réseaux sociaux. « Ce jour-là, nous avons commencé à demander une commission d'enquête nationale. » Mais le gouvernement Harper rejette l'idée d'une telle commission d'enquête. (…) Le 8 décembre 2015, Justin Trudeau annonce la mise sur pied d'une commission d'enquête nationale sur les femmes et les filles autochtones disparues ou assassinées. Pour les familles des victimes, les attentes sont grandes : changer des stéréotypes qui existent depuis des centaines d'années et faciliter l'intégration des jeunes autochtones dans les grandes villes. Sheila North Wilson espère aussi que la commission d'enquête réussira à redonner aux filles et aux femmes disparues leurs voix, au profit des jeunes filles d'aujourd'hui et de demain. Radio-Canada

Windsor Public Library To Honour Missing and Murdered Indigenous Women With Faceless Dolls Product
The Windsor Public Library will be hosting a special project to bring awareness to the cases of close to 1200 missing and murdered Indigenous women and girls in Canada during the week of May 16th to 22nd. In coordination with the Can-Am Indian Friendship Centre and the Métis Nation of Ontario, the project will consist of a series of workshops during which we are inviting community members to help create faceless dolls out of felt. Each doll represents one of the cases of murdered or missing women to help give a voice to these missing mothers, sisters and daughters. Windsorite

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

NIL

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

'Immense' pressure on Philippine military in manhunt for terrorists who killed Ridsdel

The Philippine military came under increased pressure Tuesday to rescue more than 20 foreign hostages after their Muslim extremist captors beheaded a Canadian man, but troops face a dilemma in how to succeed without endangering the remaining captives. Abu Sayyaf gunmen beheaded John Ridsdel on Monday in the southern province of Sulu. Ridsdel's head, which was placed in a plastic bag, was dumped by motorcycle-riding militants Monday night in Jolo town in impoverished Sulu, a densely forested province about 950 kilometres south of Manila, where the Abu Sayyaf and allied gunmen are believed to be holding 22 foreign hostages from six Western and Asian countries. "The full force of the law will be used to bring these criminals to justice," the Philippine military and police said in a joint statement. About 2,000 military personnel, backed by Huey and MG520 rocket-firing helicopters and artillery, are involved in the manhunt for the militants, who are believed to be massing in Sulu's mountainous Patikul town, military officials said. (…) A large-scale offensive could displace many villagers and draw attention to the longstanding security and social issues in the vote-rich south, homeland of minority Muslims in the largely Roman Catholic nation. Associated Press (National Post); Globe and Mail; National Post

Broadcast media / Médias télédiffusés

CBC News interviewed Zachary Abuza, professor at the National War College regarding Abu Sayyaf. Militants are believed to be holding 22 hostages from six different countries, including one more Canadian, Robert hall. They don't have a very clear stated political goal. Rough Transcript

INTERNATIONAL

The impact of jihadist beheadings: Is terror propaganda brutalizing us all?
Since the headline-grabbing murder of American journalist James Foley by ISIS militants in August 2014, the world has been regularly confronted with a modern form of an ancient, horrifying method of execution. British and American aid workers, Japanese and American journalists, Kurdish and Syrian soldiers, Egyptian and Ethiopian Christians and an alleged Russian spy were among those who followed in Foley's wake: their gruesome beheadings documented on camera and disseminated as propaganda to a global online audience. Canadian John Ridsdel, held by the Philippines-based, ISIS-allied jihadist group Abu Sayyaf since he was abducted in September, is the latest victim to be murdered in this way. CNN

9 Islamic extremists investigated over plan to kill
German authorities are investigating nine Muslim extremists on suspicion they planned to kill two people over disagreements in their interpretation of Islam. Prosecutors in Bremen say 10 premises in the northern German city were searched early Tuesday following tips about the planned crimes. Some 200 police officers were involved in the morning raids. Associated Press (Metro News, Yahoo! News)

Moment suicide bomber detonates in Paris cafe shown on French TV
French television has shown the moment when one of the suicide bombers detonated in a Paris cafe as part of the multiple attacks five months ago. Ibrahim Abdeslam, 31, was captured on a security camera as he carried out one of the attacks on November 13, which killed 130 people across the French capital. The disturbing footage shows the bomber walking into the busy bar at 9.40pm on the Friday night. Abdeslam walks towards an empty table, before looking down and covering his face with his left hand. There is then a flash behind him and a puff of white smoke as he detonates. Telegraph UK

Iraqis Reportedly Warn Sweden of ISIS Terror Plot
Iraqi intelligence services have reportedly warned Sweden of an ISIS terror plot in Stockholm. "Seven or eight" terrorists are planning an attack in the capital against civilians, according to local newspaper Expressen, citing sources. Swedish police are assessing the information, according to a police statement. "This information is deemed to be of such nature that it cannot be dismissed," police said, adding that they were working closely with national and international partners. The threat level has not been raised in Sweden and remains at "an elevated level." Swedish media are reporting that police are reconsidering security measures for the 70th birthday of Sweden's king next weekend. ABC News

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Radio-Canada
Le ministre Marc Garneau attendu de pied ferme à Lac-Mégantic ce soir http://rc.ca/L8rt33

Transport_gc
#ICYMI: Minister Garneau to participate in the #LacMégantic meeting tonight at 6:30 at the Centre Sportif #RSW2016 ow.ly/3zGpl0

Transports_gc
Rappel: Le min Garneau au centre sportif de #LacMégantic ce soir à 18h30 #SSF2016 ow.ly/3zGpl5

TrainsMagazine
Canada transportation leader to address Lac-Megantic community on rail safety trn.trains.com/news/news-wire…

LeDevoir
#LacMégantic Le ministre Garneau attendu de pied ferme ledevoir.com/environnement/…

KelownaNow
#Evacuation order lifted near Fort St. John @BCGovFireInfo #fireseason #BC #provincialnews kelownanow.com/watercooler/ne…

DRDC-RDDC
#CAUSE4 TMRW! Partners test how #tech is used to enhance response activities on both sides of border #DRDC_CSS @dhsscitech @Safety_Canada

NATIONAL SECURITY / SÉCURITÉ NATIONALE

RCMP
Read how the RCMP used social media to respond to the 2014 Parliament Hill attack. http://rcmp.ca/-yfB http://www.rcmp-grc.gc.ca/en/gazette/live-tweeting-a-terrorist-attack?tw

Mubin Shaikh
SneakPeek 2moro @Hedayah_CVE
@UN_CTED - I discuss Trials, Citizenship&Pass revocation, PeaceBonds etc. #cdnpoli

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Nicholas Keung
Jonathan Nicola, the 29-yr-old man posing as a teen in Windsor high school, says he's coached to lie. More to come

Chantal Desloges
Windsor high school player detained by CBSA after reports he's nearly 30 http://www.theglobeandmail.com/news/national/cbsa-arrests-man-allegedly-posing-as-high-school-basketball-player-inwindsor/article29713729/?utm_source=twitter.com&utm_medium=Referrer:+Social+Network+/+Media&utm_campaign=Shared+Web+Article+Links …

Maureen Revait
Detention review hearing by CBSA has decided to keep Jonathan Nicola in detention due to possible flight risk #sx

Nick Brancaccio
Stephen Fields Catholic School Board arrives at CBSA hearing for Jonathan Nicola, the Catholic Central student.

La Presse
Le Canada menace une femme et son fils de les renvoyer en Algérie

LAW ENFORCEMENT / APPLICATION DE LA LOI

RCMP Depot
RCMP announces winners of Name the Puppy Contest http://www.rcmp-grc.gc.ca/depot/news-nouvelles/2016/20160426-name-the-puppy-nomme-le-chiot-eng.htm … #namethepuppy

Rob Williams
RCMP #namethepuppy winners: Jango, Jolt, Jade, Jorgia, Jude, Jix, Jax, Jett, Juno, Java, Jinx, Jazz & Jake. #yeg

620 CKRM
#RCMP unveils winning names in their #NamethePuppy contest #yqr #SK http://bit.ly/21eemep

Charles Adler
#Nenshi not conservative. No #RCMP investigation. No prosecutor saying a deeply disturbed public demands justice.

Gary Dimmock
Mountie kept camera trained on his son when doing homework. Boy wouldn't do work.

Gary Dimmock
The father pulled son out of school in Sept. 2012, and 'homeschooled' him. I thought it was good for him but he didn't want to do the work

Gary Dimmock
UPDATE: 'I always felt rejected by my son': ex-Mountie tells court during child-torture trial

Gary Dimmock
Asked about neighbour's claim his son wasn't dressed properly for winter. Ex-Mountie denies it. 'I don't know where she came up with that'

Gary Dimmock
Asked about son's claim dad put box over his head to make him feel like he was in jail. 'This is not true. I don't live in a military house'

Gary Dimmock
Ex-Mountie back on stand. On life's stress, he just said: "I had wide shoulders but I'm not God. I could only do so much. I was drained"

Gary Dimmock
Mountie says his boy's 'vindictive, manipulative mind' was 'exhausting'

Gary Dimmock
Mountie claims under oath that his son acted like a vulgar street kid with no conscience. He told me he wanted to lie, steal and misbehave.

Gary Dimmock
Mountie is now branding his son a liar, recounting a lifelong trail of fabricated stories.

Gary Dimmock
The Mountie flatly denies his son's version of their Florida trip. Was he tied up and starved? "That's not true!"

Gary Dimmock
It was a Florida vacation nowhere near ordinary, according to the boy, who said he was tied up in hotel while family hit the beach.

Gary Dimmock
Mountie on trial for torturing + starving son has resumed his testimony. Talking about 2012 Florida trip.

Gary Dimmock
Mountie who terrorized 11-year-old son in basement takes stand in own defence.

Catherine Lathem

Dates of family photos are important to establish timeline. The boy says he was chained in basement for 6mths before feb 2013 @ctvottawa

Catherine Lathem
Looking at pictures he's confused about the dates. What year and what time of year. @ctvottawa #ottnews

Catherine Lathem
Showing the court a picture of his son "a beautiful shot. He's a hunk. He was my model, I dressed him up" @ctvottawa #ottnews

Catherine Lathem
Dad: "it only made him (son) smarter and better to manipulate all these people" @ctvottawa #ottnews

Catherine Lathem
The RCMP officer says his son with "vindictive mind" was only happy when he got what he wanted @ctvottawa #ottnews

Catherine Lathem
Dad: "if I don't have any morals, if I was able to shut my eyes and look the other way then I was the perfect Dad" @ctvottawa #ottnews

Catherine Lathem
Describing his son "there was something in him that always made him behave like a street kid. Vulgar" @ctvottawa #ottnews

Catherine Lathem
Said son had no morals & told him "I want to be able to steal, to lie, to touch anybody I want and not get in trouble" @ctvottawa #ottnews

Catherine Lathem
Dad says "no he met with my brother. We raked leaves. We played ping pong. Neighbors saw him playing outside " @ctvottawa #ottnews

Catherine Lathem
Defence asked your son claims he was chained in basement during that time (fall 2012) @ctvottawa #ottnews

Catherine Lathem
Now showing family photos of son playing outside in the fall of 2012. The crown previously disputed the date of that picture. @ctvottawa

Catherine Lathem
The RCMP officer and father is on the stand showing family photos of the Florida trip. Some pictures include his son. @ctvottawa #ottnews

Catherine Lathem
Dad: "his imagination continued so wildly" when asked about his sons imagination "it's hard to know what is true and what is not true".

Catherine Lathem
Dad about Florida trip "this was not true. The sad part was I thought I was making memories with him" @ctvottawa #ottnews

Catherine Lathem
The boy alleges his dad and stepmom left him tied up and starved while family hit beach. Dad: "it's not true at all" @ctvottawa #ottnews

Catherine Lathem
Officer talking about 2012 family trip to Florida. Staying in lrg 6bdrm beach home: says son was "living like a king" @ctvottawa #ottnews

Catherine Lathem
Back in court for RCMP officer testifying in his own defence. On trial for chaining 11yo son in basement for months @ctvottawa #ottnews

Mercedes Stephenson
Follow @CatherineCTV for tweets from court as RCMP officer testifies in own defence in child abuse case (his son). Warning it is disturbing.

Claire Neary
Police pleas for surveillance-technique secrecy 'self-serving and weak,' judge says - @Colinfreeze

Craig Forcese
Police pleas for surveillance-technique secrecy 'self-serving and weak,' judge says

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Rachel Browne
Kinew James inquest postponed indefinitely after coroner gets 8,000 new docs:

John Howard Society
#JohnHowardSociety addresses #solitaryconfinement in recent @globeandmail article

JohnHowardSociety
The misuse of solitary confinement is torture. So why does it still happen in Canada?

John Howard Society
Reform solitary confinement: Alternatives - Therapeutic communities, nonviolence + behavioral training https://shar.es/1eXEDO via @projo

PUBLIC SERVICE / FONCTION PUBLIQUE

Rabble.ca
"Privacy concerns" have been used too often by the Canadian government as a powerful pretext for inaction or silence http://buff.ly/1Sxn6qB

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Rachel Browne
Kinew James inquest postponed indefinitely after coroner gets 8,000 new docs:

John Howard Society
#JohnHowardSociety addresses #solitaryconfinement in recent @globeandmail article

JohnHowardSociety
The misuse of solitary confinement is torture. So why does it still happen in Canada?

John Howard Society
Reform solitary confinement: Alternatives - Therapeutic communities, nonviolence + behavioral training https://shar.es/1eXEDO via @projo

PUBLIC SERVICE / FONCTION PUBLIQUE

Rabble.ca
"Privacy concerns" have been used too often by the Canadian government as a powerful pretext for inaction or silence http://buff.ly/1Sxn6qB

OTHER / AUTRES

Matthew Fisher

Got to know murdered Canadian hostage John Ridsdel during past few years. My brief retrospective on a good man.

Stewart Bell
The cowardly murder of a Canadian in the Philippines:

David Akin
Good piece from @leeberthiaume on Canada, kidnappings and what we do in...
http://www.canada.com/news/canadian+government+98very+directly+involved+negotiating+john/11876430/story.html ...

INTERNATIONAL

AFP News Agency
#BREAKING Number of foreign fighters entering Iraq, Syria plummets: US general

CNN International
Another beheading by jihadists. Is this wave of decapitations brutalizing us all? http://cnn.it/1rwRpY5

Stewart Bell
Moment suicide bomber detonates in Paris cafe shown on French TV | via @telegraphnews
http://www.telegraph.co.uk/news/2016/04/26/moment-suicide-bomber-detonates-in-paris-cafe-shown-on-french-tv/ ...

Stewart Bell
"They were working day and night to promote homosexuality." AQ branch claims killing of LGBT magazine editor in Dhaka. @siteintelgroup

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

Sent to:

Today's News / Actualités
April 27, 2016 / le 27 avril 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Taxpayer money used to protect Ottawa from Lac-Megantic lawsuits
The federal government used taxpayer money to shield itself from lawsuits related to the deadly Lac-Megantic rail disaster -- but it's refusing to say how much it paid. Ottawa denies any legal responsibility for the fiery 2013 oil-train derailment that killed 47 people, even though it was released from liability by contributing to a $460-million settlement fund for victims and creditors affected by the crash. At least two of the other 24 other settling parties accused of wrongdoing connected to the accident have disclosed

how much it cost them to avoid potential damages and legal fees. So far, the Liberal government is staying mum. "That's a classified amount, but we made a contribution because we felt that it was important," Transport Minister Marc Garneau said Wednesday in Toronto when asked about the settlement. "We don't acknowledge that we had any responsibility; however, we did want to make a contribution because of the impact of this terrible tragedy in Lac-Megantic." Canadian Press (CTV News)

Tragédie de Lac-Mégantic - John Giles se veut rassurant
Le grand patron de la compagnie de chemin de fer a rencontré la population de Lac-Mégantic pour dire que les citoyens n'ont plus à avoir peur. Le président du Chemin de fer Centre du Maine et du Québec, John Giles, comprend l'inquiétude qui hante les citoyens de Lac-Mégantic, mais il croit que leur méfiance va s'apaiser avec le temps. La tragédie de juillet 2013 découle d'une gestion défaillante de la MMA et d'un manque d'application des procédures de sécurité. Plus de dix millions ont été invertis dans la réfection des rails. TVA Nouvelles

Ottawa to consult rail industry on safety recommendations: Garneau
The federal government will consult with industry stakeholders before deciding whether to require railways to install fail-safe train controls, even as carriers in the United States work toward a 2020 deadline to begin using the technology that Canada's transportation investigator says saves lives. Marc Garneau, Canada's Transport Minister, said he will hold discussions with stakeholders before acting on any of the 60 recommendations made in a review of the country's transportation laws commissioned by the previous government. The recommendations include requiring tougher tank car standards for certain dangerous goods, installing in-train video and voice recorders, and taking steps to adopt positive train control (PTC), which can override mistakes by train and track crews. The technology can automatically slow or stop a train in danger of a head-on collision with another train, if a track switch is aligned incorrectly or a train is travelling too fast. Canada's rail investigator, the Transportation Safety Board, said the technology would have prevented the 2012 derailment of a Via Rail passenger train in Burlington, Ont. The train entered a crossover track at 67 miles an hour (108 kilometres an hour), exceeding the speed limit of 15 miles an hour, derailed and struck a building. Three crew members died and 45 people were injured. Globe and Mail

NATIONAL SECURITY / SÉCURITÉ NATIONALE

The propaganda wing of ISIL has recruited several Canadians, former CSIS official says
The propaganda wing of ISIL, known for its gory videos and exploitation of social media, has recruited several Canadians into its ranks, a former senior counter-terrorism official told a security conference Wednesday. Andy Ellis, who recently retired from the Canadian Security Intelligence Service, where he was Assistant Director of Operations, said not all of the roughly 100 Canadians who have converged in the region are active in combat operations. “Many of the Canadians, for example, found their way into the propaganda wing of Daesh,” the 30-year-veteran of CSIS said, using another name from ISIL, in a speech at the Royal Canadian Military Institute in Toronto. “I would argue that would be equally as dangerous, maybe more, than someone who is joining the military wing. A lot of these young Western adherents to Daesh are put on the frontlines and die very quickly. Someone who is working in the propaganda wing can hurt us over and over and over again.” National Post

How Islamophobia is shaping young Canadian Muslims
(…) The majority of young Muslims in Canada feel Muslim first and Canadian second, an Environics Institute survey released Wednesday suggests. Some experts suggest that's because young Muslim Canadians feel a strong societal pressure to have to answer for violence perpetrated by extremists in the name of Islam and are struggling to reclaim their Muslim identity for themselves. Among young respondents who said their citizenship and their faith were important parts of their identity, 61 per cent said being Muslim was the most important part of their identity and six per cent said being Canadian was the most important. Twenty-six per cent said both were important (...) Many young Muslims in Canada feel saddled with a responsibility to have to answer for violent attacks carried out in the name of Islam, said Toronto-based legal scholar Azeezah Kanji. "Being a securitized population under suspicion in Canada is really the dominant experience that we've had," Kanji said. CBC News

Un présumé sympathisant terroriste devra rester détenu
Un homme de 23 ans faisant face à une accusation liée au terrorisme s'est vu refuser une libération sous caution, mercredi, à Brampton en Ontario. Kevin Mohamed devra donc demeurer derrière les barreaux, mais les détails de la décision sont frappés d'un interdit de publication. L'ancien étudiant en génie avait été arrêté le mois dernier parce que l'on craignait qu'il ne commette un acte terroriste. La Gendarmerie royale du Canada (GRC) l'avait alors accusé d'avoir participé ou contribué aux activités d'un groupe terroriste sur une période de deux ans. La police affirme que Kevin Mohamed a commis les offenses en Ontario - notamment à Whitby, Mississauga et Waterloo - entre le 24 avril 2014 et le 25 mars 2016. Presse canadienne (La Presse)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

International emergency system experiment conducted this week
Officials from both sides of the St. Clair River have been taking part in an experiment this week to test technologies designed to help Canadian and U.S. officials communicate during an emergency. Sarnia and Port Huron were chosen for the fourth annual Canada-U.S. Enhances Resiliency Experiment (CAUSE IV) that began Tuesday and was scheduled to be completed at noon Thursday. Philip Dawe, with Defence Research and Development Canada's Centre for Security Science, said 55 participants, on both sides of the border, were involved, along with 20 observers... Locally, the experiment involved Lambton County, the City of Sarnia, Canada Border Services Agency, Bluewater Health and the Blue Water Bridge. Sarnia Observer

Family of Calgary mother isolated in France raising pressure on Ottawa for help
A Calgary man vows to intensify pressure on Ottawa to come to the aid of his sister - known internationally for her stand against homegrown radicalization - who has been exiled in France. Jean-Marc Boudreau said his sister, Christianne, has brought comfort to so many families that have lost children to radical militant groups after her own son, Damian Clairmont, was killed while fighting with terrorists in Syria. But the mother is unable to continue "serving the world for the beautiful cause of peace" because she is stranded in a small town in France after she and her youngest son, Luke, were forced to surrender their passports... The mother suspects the passport dispute has less to do with Luke's application and more to do with her widely publicized criticisms of the Canadian government's efforts to address homegrown radicalization. Calgary Herald

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

SWIFT confirms additional cyberattacks on its messaging system
The Society for Worldwide Interbank Financial Telecommunication (SWIFT) has issued a warning to its customers that its financial messaging system has undergone repeated attacks similar to those that lead to $81 million from a Bangladesh bank. SWIFT has since issued a mandatory security update for its software that will help customers "identify situations in which attackers have attempted to hide their traces, whether these actions have been executed manually or through malware," according to bankinfosecurity.com. SWIFT would not release any details concerning these attacks or what companies were involved, but the organization did note that the attacks were all similar and that the attackers were able to compromise the targeted banks computer networks and obtain valid credentials to create and send messages, bankinfosecurity.com reported. On April 25 SWIFT confirmed it was aware that malware was targeting its system when $81 million was stolen from a Bangladesh bank in March. SC Magazine

FBI says it won't disclose how it accessed locked iPhone
The FBI says it won't publicly disclose the method that allowed it to access a locked iPhone used by one of the San Bernardino attackers. In a statement Wednesday, FBI official Amy Hess said the FBI does not "have enough technical information" about the software vulnerability that was exploited to make it public. An unidentified third party approached the federal government last month with a method that it said could

get into the phone used by Syed Farook, who along with his wife killed 14 people in the December attacks. The method proved successful. Hamilton Spectator

LAW ENFORCEMENT / APPLICATION DE LA LOI

'I thought the devil's inside him': Mountie in child-torture trial had priest perform exorcism on 'possessed' son

The Mountie on trial for child torture enlisted his brother — a priest — to perform an exorcism on his "possessed" 11-year-old son. "I thought the devil's inside him. I saw his eyes and heard his voice," the Mountie told court Wednesday morning. The chilling detail was revealed under questioning by lawyer Anne London Weinstein, who is defending the Mountie's wife, also on trial for confining the boy and failure to provide necessities of life. It's not clear when the exorcism was performed, but it was sometime before September 2012, and before the Mountie allegedly started torturing and starving his son in their darkened Kanata basement. The Mountie, suspended without pay, has also admitted to burning his shackled, naked son with a BBQ lighter as a form of punishment for misbehaving and refusing to do homework. Postmedia News (National Post)

English-only RCMP officers on Parliament Hill spark complaints

The Royal Canadian Mounted Police is not meeting its obligation to offer services in both official languages on Parliament Hill, according to a preliminary report stemming from four complaints last year. Yvon Godin — who at the time was NDP MP for the New Brunswick riding of Acadie–Bathurst and official languages critic — complained that RCMP officers were not able to provide service in French. With security on his mind following the Oct. 22, 2014 shootings, Godin noted that when he said, "Bonjour" to RCMP officers on the Hill, the response would be, "I don't speak French," he told Radio-Canada. "I thought this made no sense," he said. "As official languages critic, I started a little investigation (...)" The Office of the Commissioner of Official Languages found in an April 2016 report that the complaints — dated Feb. 15, May 27, June 5 and June 8 in 2015 — were founded. As a federal institution, the RCMP is required to offer services in both French and English on Parliament Hill, according to the *Official Languages Act*. CBC News; Presse canadienne (L'actualité)

Opitciwan police back on the job next week

One month after Opitciwan's police force was disbanded, 22 officers will be back on the job next week in the remote First Nation. The local department was disbanded on April 1 as negotiations over a renewed funding agreement between Opitciwan's band council, the federal and provincial governments fell apart. At issue was Quebec's refusal to help pay for the department's $600,000 deficit — a sum it had previously agreed to fund, according to Opitiwan's band council. For Opitciwan to continue paying its police officers as of April 1, the council would have had to divert money from other services like health care and education. Given that the community struggles with some of the highest unemployment levels in Quebec, band chief Christian Awashish says redirecting funds wasn't an option. As Awashish met with representatives from Quebec and Ottawa, the Sûreté du Québec assumed policing duties in Opitciwan at a cost of about $100,000 per week. Opitciwan's locally-run police force operated on less than half that budget. Montreal Gazette; CBC News

'Despicable act': Senior robbed at gunpoint inside Richmond home

Mounties are searching for a man who robbed a Richmond senior at gunpoint inside her own home Tuesday. The RCMP said the robber entered the 80-year-old woman's residence through an unlocked garage door shortly after 5 p.m. The man then pulled out a handgun, demanded the victim's purse and car keys, and then fled in her vehicle. "This despicable act was particularly brazen, especially given the time in which it took place. We are doubling down our efforts in tracking down those responsible for this crime," Cpl. Dennis Hwang said in a statement. CTV News

RCMP puppies trained in Alberta named in annual contest - 13 future police dogs all given names starting with 'J'

Try reading this without saying "aww." Thirteen cute and cuddly pooches set to become police dogs for the RCMP now have names, after nearly 16,000 children from across the nation submitted their picks for

the annual "Name That Puppy" contest. All names had to start with the letter "J." The 13 winners will each receive a certificate, a photo of the puppy they named, a plush German Shepherd toy dog named Justice and an RCMP cap. CBC News

RCMP withdraw pay from one suspended Woodstock officer - Only other N.B. Mountie currently suspended without pay was convicted of impaired driving

The New Brunswick RCMP say they have now withdrawn pay from one of the two Woodstock officers suspended from the detachment. RCMP spokesperson Const. Jullie Rogers-Marsh said the move happened at some time after February 16. Rogers-Marsh said the second officer remains suspended with pay, but did not reveal to CBC News whether the force is trying to remove pay from that member. The RCMP had said in February that they were pursuing suspension without pay for both officers. The two are still subject to a criminal investigation and a Police Act investigation. Four of the Woodstock RCMP's 29 officers were suspended last fall for alleged discreditable conduct. CBC News

Halifax shootings prompt meeting of justice minister, mayor, police - Diana Whalen says there are 'no simple solutions,' highlights programs she says are working

Nova Scotia's minister of justice met with the Halifax's mayor, chief of police, and RCMP Wednesday to discuss improving public safety in the wake of four deadly shootings in the region in the past month. Diana Whalen called it a "starter meeting" aimed at addressing the recent gun violence. She said the two levels of government and the two police services meet regularly one-on-one, but this was their first opportunity to sit around the table as a group. "There are no easy answers," Whalen said, "no simple solutions, and I think the community knows that. They understand that as well as, or better than, we do. "We want to work together. We want to make sure that we're leveraging as many of the resources that we can. But the answer lies in all of us putting our heads together … and it's a long-range plan. It's not something you can do in a snap." CBC News

RCMP confirm Troy Napope's remains found

RCMP confirmed on Wednesday that the human remains located on April 20 near the Saskatchewan Penitentiary belonged to those of Troy Napope. The Office of the Chief Coroner held an autopsy on April 22 to confirm the identity of the remains. The RCMP Underwater Recovery Team located human remains during a planned search in a rural area west of the Saskatchewan Penitentiary in Prince Albert. Prince Albert Daily Herald; Star-Phoenix; CBC News

RCMP investigating bridge fire as suspicious

A day after a trestle bridge near Mayerthorpe was destroyed in a fire, police confirmed the blaze was considered suspicious. On Wednesday, Mayerthorpe RCMP said the fire on the CN Rail trestle bridge, located on the northwest edge of the town, was being handled as suspicious. Police said provincial fire investigators, along with CN Rail officials were at the scene and trying to determine what caused the fire to assist the RCMP investigation. Officials said RCMP were called to the fire on Tuesday, at about 1:20 p.m. – Mayerthorpe RCMP said the bridge fire is the fifth fire they had been called to in the last ten days. CTV News

Nova Scotia RCMP charge Amherst woman with fraud

Nova Scotia RCMP have charged 54-year-old Rhonda Charmaine Kelly of Amherst with fraud and uttering forged documents following a 20-month investigation. Kelly is facing several charges including one count of fraud over $5,000 and nine counts of uttering forged documents. She appeared in Amherst Provincial Court April 25 and is due back on June 23. The RCMP received a complaint in July 2014 of a possible fraud in the amount of several hundred thousand dollars against the Nova Scotia Department of Economic and Rural Development and Tourism. Chronicle-Herald

Bondage cop steps down

A B.C. Mountie has left the RCMP over a controversy involving explicit bondage photos. Photos of Coquitlam RCMP Cpl. Jim Brown posted on a sadomasochism website made the Mountie the subject of three separate investigations in 2012. He was suspended with pay for alleged professional misconduct when the photos were first brought to the attention of the RCMP. Brown is seen wearing his RCMP boots in various bondage photos. CTV News has learned that Brown's disciplinary hearing was cancelled and

the commanding officer of the RCMP in British Columbia said Brown submitted his discharge papers, which were "immediately" signed. "His career with the RCMP is over," Dept. Comm. Craig Callens said in a statement. Castanet

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

What It's Really Like to Spend Time in a Canadian Prison
An opinion piece states "I'd heard the horror stories about prison. I'd seen the TV shows, movies, and news reports about the rampant violence, race-based wars, and sexual abuse that occurs behind the walls. I heard the advice from friends on how to survive in jail. Some say to find the biggest guy on a range (what inmates call a cell block) and pick a fight with him immediately. Some say to keep your head down and stick to yourself. Some say to go into protective custody. But above all, don't drop the soap. So when I spoke to my lawyer for the first time and heard I was facing over two years in prison, I was scared—two years and over in Canada means time in a federal penitentiary... So when I got to Millhaven Institution's Assessment Unit in Bath, Ontario, I felt like I was starting over again. Right out of the gate it was culture shock. My tattoo was photographed and sent to the Security Intelligence Officer to investigate any gang ties. They had me write down any emergency contacts they might need to know. They instantly put $80 of my personal money on hold until my release—but I knew that would happen." Vice News

Yukon study finds high levels of FASD in the justice system
A Yukon study has found people in the territory's justice system are much more likely to have fetal alcohol spectrum disorder than the general population. Health Canada estimates about one per cent of Canadians have the disability. According to preliminary findings of a Department of Justice study, the prevalence within the Yukon justice system is about 17.5 per cent. FASD is a disability caused when a mother consumes alcohol during pregnancy. People with FASD can have developmental disabilities, problems with memory, and difficulty with sequencing events and understanding consequences... Reports on FASD and the justice system are few and far between. In 2006-2007 a study by Corrections Canada found a 10 per cent rate in federally sentenced men. Yukon News

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Fewer crimes committed in Montreal in 2015, report shows
Montreal's overall crime rate dropped in 2015, but the number of violent incidents took a disquieting upturn last year, statistics released by the Montreal police force reveal. And as the number of cyclists has surged, so has the number of those who suffered serious injuries, a statistic police said could be linked to an increase in the number of bike paths. Crimes against individuals, which include homicides, attempted murders, sexual assaults and robberies, rose by 4.5 per cent over 2014, with 19,435 cases reported. The number of attempted murders leaped 48 per cent to 111 cases in 2015, compared with 75 in 2014. Sexual assault cases also saw a large increase, up 17 per cent to 1,299 cases in 2015. "We have to say that, in general, we are satisfied, because the overall crime rate dropped by 2.5 per cent," said Claude Bussières, assistant director of corporate services for the police force. Montreal Gazette

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Simone Sanderson was a police informant before murder: family
There were numerous accusations laid against Winnipeg police by a private investigator looking into the murder of Simone Sanderson. Among them, that there is a police cover up in part because Sanderson was a police informant. The 23-year-old was found murdered nearly four years ago. On Tuesday, police

charged a man with second-degree murder. It's a man the family say they told police about over a year ago. APTN News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

NIL

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

RCMP investigating killing of Canadian hostage by militants in Philippines
The RCMP is conducting a criminal investigation into the murder of hostage John Ridsdel in the Philippines. A senior official says the Mounties are relying on the extraterritorial provisions of the Criminal Code in pursuing the overseas investigation. It means the perpetrators, if found and charged, could one day face justice under Canadian law. The official spoke with The Canadian Press on condition of anonymity given the sensitivity of the ongoing hostage case. Ridsdel, 68, of Calgary, was beheaded earlier this week after a large random demand from his captors, members of the Abu Sayyaf militant group, went unmet. Canadian Robert Hall, abducted with Ridsdel from a marina in September, is still being held along with several others. Canadian Press (CP24; Toronto Star); Presse canadienne (L'actualité)

Headless torso discovered on Jolo Island may be Canadian kidnap victim, Philippine army says
The headless torso of a Caucasian man that may be Canadian kidnap victim John Ridsdel was discovered Wednesday on Jolo Island, Colonel Noel Detoyato, the chief Philippine army spokesman told Postmedia Wednesday. Prime Minister Justin Trudeau confirmed Monday that Ridsdel's severed head had been found that day after a ransom deadline set by Abu Sayyaf for the freedom of the mining executive and three other hostages had passed. The group, which claims to be allied with Islamic State in Iraq and the Levant, had demanded more than $8 million for each of the people they had kidnapped near Davao City last September and have been holding 600 kilometres to the west of there since then in the jungles of Sulu province. Postmedia News (National Post)

INTERNATIONAL

NIL

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

Karen Ahmed
@NoFlyListKids so many kids on the #Canadian list. #fix this @RalphGoodale @JustinTrudeau

OpenMediaOrg
Tell @openmediaorg what to say to @ralphgoodale about #C51:
http://ow.ly/4naDV5 #C51withGoodalepic.twitter.com/ZPCcK2RltP

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

AndyBlatchford
Feds won't say how much was paid to protect Ottawa from Lac-Megantic lawsuits http://www.montrealgazette.com/business/feds+wont+much+paid+protect+ottawa+from+lacmegantic+lawsuits/11881078/story.html … #cdnpoli

tvanouvelles
Tragédie de Lac-Mégantic: John Giles se veut rassurant http://bit.ly/1SQU0rC

RT_com
Huge fire destroys trestle bridge in #Canada, 17th fire in 6 days http://on.rt.com/7b6k

NATIONAL SECURITY / SÉCURITÉ NATIONALE

metromontreal
Terrorisme: un homme reste détenu en Ontario http://bit.ly/1TeJx3t

PostmediaNews
The propaganda wing of ISIL has recruited several Canadians, former CSIS official says http://ow.ly/8JRk3s

LAW ENFORCEMENT / APPLICATION DE LA LOI

Canadian Politics News
English-only RCMP officers on Parliament Hill spark complaints http://ift.tt/1pG6dlf

Frazer Snowden
Watch CTV #reddeer news tonight for a story on the RCMP's newest fuzzy recruits and the training ahead for them.

nvanrcmp
Out with CN Police, WVPD, ICBC for Rail Safety Week. Please pay attention at all RR Crossings. Know RR Safety Tips!

nationalpost
'The devil's inside him': Mountie in child-torture trial had priest perform exorcism on son http://natpo.st/1YUhw5t

mtlgazette
Opitciwan police back on the job next week https://t.co/2iO3fHYa1r

Lactualite
Les agents étaient incapables de fournir des services en français #GRC http://www.lactualite.com/actualites/agents-unilingues-anglophones-au-parlement-la-grc-a-enfreint-la-loi/ …

620ckrm
RCMP confirm body found in slough near Prince Albert is Troy Napope

TheTorontoSun
Mountie enlisted priest brother to perform exorcism on his "possessed" 11-year-old son. http://ow.ly/4naUzm

ctvottawa
Mountie's story under attack by Crown in child abuse trial, @CatherineCTV reports #ottnews http://ctv.news/lAy2M9Z

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

CSC_SCC_en
We are on Flickr! Check out our photo & video https://t.co/JklsWTSCV2

SCC_CSC_fr
Nous sommes sur Flickr! Allez voir notre collection de photos et de vidéos https://t.co/vicp9JOx6r

CTV_PowerPlay
To discuss the massive overrepresentation of indigenous peoples in jails across Canada, Correctional Investigator Howard Sapers. #cdnpoli

CTV_PowerPlay
ICYMI: Correctional investigator compares effect of prisons to residential schools when it comes to Indigenous youth https://t.co/lX9W8ncjA2

vicecanada
What it's really like to spend time in a Canadian prison: http://bit.ly/1SB5Lgp

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

APTNNews
Simone Sanderson was a police informant before murder: family - APTN National News
http://aptn.ca/news/2016/04/27/simone-sanderson-was-a-police-informant-before-murder-family/

OTHER / AUTRES

The Globe and Mail
WATCH: Amnesty International urges Justin Trudeau to cancel Saudi Arms deal http://trib.al/ZI7pZWS

CP24
RCMP investigating killing of John Ridsdel by militants in the Philippines http://www.cp24.com/news/rcmp-investigating-killing-of-canadian-hostage-by-militants-in-philippines-1.2877602 …

metromontreal
Otages aux Philippines: la GRC ouvre une enquête #polcan http://bit.ly/1Stghtt

INTERNATIONAL

LP_LaPresse
Séisme en Équateur: le Canada offre 900 000 $ de plus en aidehttp://bit.ly/1SKJJdk

Independent
Isis has terror cells 'operating in England' https://t.co/GDG8vykzW0

Blogs

We're meeting with Minister Goodale on C-51, and we want you to make sure your voices are heard: What should we say?
Alright OpenMedia community, we need your help! On Thursday, May 5, OpenMedia will be meeting in person with Canada's Minister of Public Safety and Emergency Preparedness, Ralph Goodale to discuss Bill C-51. This is where you come in: We need you to tell us what you want us to say! You have been at the heart of this campaign from the very start. Over 300,000 people have spoken up against this dangerous and ineffective bill. Protests and rallies have been held across the country. Tens of thousands of emails have been sent to MPs. Artists, business leaders, law professors, civil society groups, academics, and experts have all spoken out against this reckless legislation that jeopardizes our rights and freedoms. Open Media

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

Today's News / Actualités
May 17, 2016 / le 17 mai 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Fort McMurray Wildfire / Feu de forêt à Fort McMurray

Canada gov't says confident Alberta can fight widening fires
The Canadian federal government has full confidence in the ability of Alberta to fight a resurgent wildfire in the oil sands region and has not received any additional requests for help, **Public Safety Minister Ralph Goodale** said on Tuesday. **Goodale** told reporters that it was not a good sign that the fire is attacking oil sands facilities and said that the fire would have dampening effect on the economy. Reuters

Other/Autre

Ontario health workers demand end to 'inhumane' immigration detention process

A group of doctors, nurses and health-care providers have signed an open letter urging the province to stop allowing immigration detainees with health concerns to end up in Ontario prisons. The letter, signed by more than 140 medical professionals, was mailed Tuesday to Community Safety and Correctional Services Minister Yasir Naqvi. Concerns have been raised after two men detained by the Canada Border Services Agency (CBSA) died in separate incidents this spring in Ontario and a 24-year-old man died while being held at the Edmonton Remand Centre. The group behind the letter is calling on Queen's Park to end what they call a "worrisome practice," claiming the transfers of vulnerable people with health issues to provincial prisons is "adversely impacting the health of a very vulnerable population in our province." (…) The letter detailed the many harms those in custody can be exposed to while detained, from illnesses such as tuberculosis, HIV and Hepatitis C to the possibility of being assaulted or injured. "Refugee claimants and other migrants are especially vulnerable to the toxic stress of incarceration, as many have already experienced prolonged and repeated trauma, including torture, in their countries of origin," the letter stated. (…) On Monday, a CBSA spokesman confirmed immigration detainees are not provided with written reasons for transfers. "Detained individuals can speak to a CBSA officer about any aspect of their detention," said CBSA spokesman Travis O'Brien. "The officer is available by phone for any facility and also conducts regular site visits." In the letter, the group also mentioned how these placements have a "profound and debilitating impact" on those dealing with suicidal thoughts because they are sometimes placed in complete isolation or solitary confinement. (…) On Sunday, **Public Safety Minister Ralph Goodale'**s office released a statement saying they are concerned with the recent deaths in government custody and said the federal government is reviewing the detention program. CBC News

OPINION: New bill just a start to protect the rights of transgender people
An editorial states, "On Tuesday, Justice Minister Jody Wilson-Raybould tabled new legislation to better protect the human rights of transgender people in Canada. Timing the announcement to coincide with the International Day Against Homophobia, Transphobia and Biphobia, the proposed legislation would add "gender identity" and "gender expression" as prohibited grounds of discrimination to the Canadian Human Rights Act, along with the hate crimes provisions of the Criminal Code. In doing so, the goal of the legislation is to redress the extraordinarily high rates of discrimination, harassment and violence experienced by transgender people across the country. (…) After the photo opportunities are over on Tuesday, however, Ms. Wilson-Raybould and others in the Liberal cabinet must do more than simply pay lip service to transgender human rights. They need to get to work on a range of federal laws and policies. Take, for example, the legal regulation of transgender women in federal prisons – a portfolio overseen by the **Minister of Public Safety and Emergency Preparedness, Ralph Goodale**. In prisons across Canada, transgender women who have not undergone gender-affirming surgery are forced to be housed in men's institutions. Prison administrators know that placing transgender women in men's facilities is likely to make them vulnerable to violence and sexual assault. Administrators often place them into solitary confinement – a practice that has devastating mental-health consequences. While Ontario and British Columbia recently enacted policies to remove surgical requirements, the federal government has failed to show the same leadership." Globe and Mail

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fort McMurray Wildfire / Feu de forêt à Fort McMurray

Fort McMurray firefighters facing extreme fire conditions - 'We had to pull the firefighters off the line because it was so dangerous out there'
Heavy smoke, limited visibility and an unpredictable fire is making life dangerous for firefighters north of Fort McMurray. "Yesterday the fire was showing extreme behaviour and lots of smoke in the air," said wildfire information officer Travis Fairweather Tuesday. "We had to pull the firefighters off the line because it was so dangerous out there." The 285,000-hectare fire that destroyed whole sections of Fort McMurray earlier this month, forced the evacuation of 8,000 oilsands workers Monday. Most of the workers involved in the evacuation work at 12 plants for Suncor and Syncrude, located between Fort McMurray and Fort MacKay. "Those facilities have some fire treatment in place that will hopefully prevent them seeing too much impact from the fire," Fairweather said. "Any time you see a fire getting close to

anything, it's a scary situation." The fire slowed overnight as temperatures cooled but as the day heats up, the fire is expected to speed up. CBC News

Canada wildfire threatens Fort McMurray again as further 12,000 people evacuated
At least 12,000 people have been asked to evacuate oil sand camps close to the Canadian town of Fort McMurray after a fresh wildfire began to shift to the north. According to the BBC, more than 8,000 people were urged to leave the area on Monday night, in addition to 4,000 people who had already been issued with evacuation orders. Suncor Energy Inc was among several operators which confirmed on Tuesday that it had been forced to shut down operations as a precautionary measure. A spokesman said there had been no damage to the company's assets and that fire defences were in place around the facilities. Suncor and Syncrude Canada also confirmed they had evacuated workers from the area. "Suncor has enhanced fire mitigation and protection around all of its facilities," one Suncor official told AFP. UK Telegraph; Radio-Canada International

Fort McMurray: le feu menace les installations des pétrolières
Les incendies de forêt qui font rage dans le nord de l'Alberta menacent maintenant les installations de l'industrie pétrolière près de Fort McMurray, ont annoncé les autorités, mardi. Tard lundi soir, un avis d'évacuation obligatoire a été diffusé pour les quelque 8000 personnes résidant dans des campements au nord de Fort McMurray. La zone touchée, qui commence à environ 50 kilomètres au nord de Fort McMurray et s'étend jusqu'au sud de Fort MacKay, comprend les infrastructures de Syncrude et Suncor ainsi que celles de plusieurs autres compagnies. Scott Long, de l'organisation de gestion des urgences de l'Alberta, avait déclaré lundi soir que l'évacuation concernait les installations du secteur pétrolier et gazier, affirmant que Fort McMurray n'était pas visé. Selon John Archer, un porte-parole du gouvernement albertain, le brasier n'était pas trop près des infrastructures de Syncrude et Suncor, mais les autorités avaient tout de même décidé d'évacuer les gens lundi soir par mesure de précaution et pour ne pas avoir à lancer une telle opération à 2 h du matin. Presse canadienne (La Presse)

Nearly $1B of oilsands production lost due to Fort McMurray fire - report
A new assessment of the economic impact of the Fort McMurray wildfires says close to $1 billion of oilsands production has been lost. The Conference Board of Canada estimates that the fire in northeastern Alberta resulted in a loss of 1.2 million barrels of oil per day for two weeks, translating into $985 million in lost gross domestic product. That represents about 0.33 per cent of Alberta's projected GDP this year and 0.06 per cent of Canada's projected GDP. Twelve oilsands operations were shut down and several more curtailed output this month because of the wildfire that closed pipelines and forced the evacuation of more than 80,000 people from the area. Canadian Press (Edmonton Journal)

Safety commission says no danger from radiological devices after Alberta wildfire
The Canadian Nuclear Safety Commission says there is no risk to the public or the environment from radiological devices that could have been affected by the wildfire in Fort McMurray. The commission sent two radiation safety specialists to the oilsands city last Thursday after getting a request for assistance from Alberta's provincial emergency operations centre. Those specialists have completed field verifications and confirm that the devices stored in about 20 locations are OK. The equipment, including radiography cameras used to check welding work and portable gauges to measure density of roadways, is all in packaging designed to survive building or vehicle fires. The specialists were also asked to check a radioactive waste site just south of Fort McMurray that is under the control of Atomic Energy of Canada. Canadian Press (CFJC)

Fort Chipewyan firefighter says trying to save Fort McMurray homes was 'heartbreaking' - 'We worked very hard to save whatever we could,' says Kerry Antoine
Kerry Antoine says her mind was made up long before she got the call May 3 to help fight the Fort McMurray wildfire. "I knew the day I became a volunteer firefighter, this was what I wanted to do, even though it takes putting my life at stake," she said. "That's what firefighters do. We train for this stuff." For the past six summers, Antoine has been helping fight fires in Fort Chipewyan, Alta., 200 kilometres north of Fort McMurray. On May 3, the day the wildfire spread into Fort McMurray, Antoine was at work. Her brother's neighbourhood was one of the first to fall under a mandatory evacuation order. "I was so worried about my brother who was living in Abasand. My brother had just got off a night shift so I knew he was at

home sleeping and his kids were at work and his spouse was at work." When she wasn't calling her brother to make sure he was getting out, she was calling her local fire chief asking how soon they would be sending volunt eers to help. "It's just heartbreaking. There's no other words to explain it. Those are our neighbours; Fort McMurray is our neighbour," she said. CBC News

Fort McMurray fire won't devastate economy, says new report
Despite the Fort McMurray wildfire causing widespread devastation and shutting down about half of all oilsands production, a new report suggests the impact to the provincial and national economy will be minimal. The Conference Board of Canada expects the fire will translate into a .33 per cent loss to Alberta's projected GDP for 2016 and just a .06 per cent share for the Canadian economy. The report, released on Tuesday, assumed most of the oilsands producers will return to full production by the end of the month. In addition, the loss of work in Fort McMurray will be offset by increased economic activity elsewhere in the province. "Families have moved temporarily to other areas, mostly within Alberta, and they will spend on food and accommodations and other services - with much of the spending covered by insurance, donations or government transfers," states the report. "At the national level, the impacts will hardly be noticeable." CBC News

Broadcast Media / Médias télédiffusés :

CBC News provides live coverage of a news conference by Alberta premier Rachel Notley providing an update on the wildfire situation. Rough Transcript

CBC News interviewed Travis Fairweather, Wildfire Information Officer, on the situation with wildfires in Alberta. Rough Transcript

Other / Autre

Mandatory evacuation caused by intense wildfire near Fox Creek, Alta. dropped
UPDATE: Tuesday, May 17, 2016, 9:42 a.m. MT The Little Smoky area evacuation order has been rescinded. A two hour evacuation notice is in effect for the Town of Fox Creek and residents previously evacuated from the Little Smoky area. A mandatory evacuation order was dropped Tuesday morning for residents in northwestern Alberta whose community has been threatened by a wildfire. About 200 residents in the Municipal District of Greenview, south of the Hamlet of Little Smoky between Township Roads 650 and 664 and Range Roads 210 and 215 on both sides of Highway 43, were allowed to return home but remain on a two hour evacuation notice. The evacuation notice was also in effect for the Town of Fox Creek and Little Smoky. Global News

Heavy rain expected later this week in the Peace Country
Peace Country residents are being advised to brace themselves for a major moisture event, which could also see a return to more seasonable overnight low temperatures. The season's first large scale cold low is heading this way from the coast of Alaska and both Environment Canada and the Weather Network agree it is likely to result in a significant two to three day total precipitation post, beginning Wednesday night. How significant however, seems difficult to determine as estimates are running from 30, to more than 60 millimetres or one, to more than two and half inches. The Weather Network, before it revised it this morning, had posted an overnight long range forecast calling for 53 to 67 millimetres of rain, with more than half of it on Thursday, but has now essentially cut it in half to just over 30. Energetic City

Caddy Lake fire shrinking, evacuation orders lifted in Whiteshell, northwest Ontario - Fire detected May 5 in Whiteshell Provincial Park forced dozens to leave area
Cottagers and year-round residents are heading back to their properties in Caddy Lake, West Hawk Lake and Ingolf, Ont., after officials from the Manitoba and Ontario governments lifted forest fire evacuation orders at 8 a.m. Tuesday. Two forest fires straddling the Manitoba-Ontario border, first detected May 5, forced dozens of evacuations. One burned in the Nopiming Provincial Park area east of Beresford Lake and into Ontario, while the other fire was in Whiteshell Provincial Park, northeast of Caddy Lake, and northwestern Ontario. Bill Benson and his wife had three hours to gather their belongings and get out 10

days ago. He has been staying on the south side of West Hawk Lake, across the lake from his property, watching the fire puff clouds of smoke into the sky nearby. CBC News

Feux de forêt et qualité de l'air : toujours des préoccupations en Saskatchewan
Le risque de feux de forêt est de nouveau extrême sur une bonne partie de la Saskatchewan cette semaine alors qu'Environnement Canada maintient son avis concernant la qualité de l'air pour le nord de la province. La province indique que le risque d'incendie est particulièrement élevé dans l'ouest de la Saskatchewan, près de la frontière albertaine. Le risque augmente ailleurs également en raison des températures chaudes et de la faible quantité de précipitations attendues au cours des prochains jours. L'interdiction de faire des feux à ciel ouvert dans plusieurs parcs la semaine dernière perdure jusqu'à ce que les conditions s'améliorent. Radio-Canada

Saskatchewan summers could be even hotter, drier in future
A prairie climate think-tank says Saskatchewan should brace itself for hot, dry weather in years to come. Over the next 30 years, research from the Prairie Climate Centre shows the number of 30+ C days in an average summer is expected to almost double. By 2080, at current carbon emission rates, that number could quadruple. "That just transforms the climate of the prairies," said Danny Blair, Director of Science for the Prairie Climate Centre. "Even if we significantly reduce our carbon emissions, there's a really important change coming to the prairie climate." The centre has created an online tool called a climate atlas that shows how climate is expected to change on the prairies. The website allows people to track climate data down to the Rural Municipality level. "Saskatoon's summer climate, under our current really bad emissions scenario, will have summers like that of Colorado and New Mexico," said Blair. While the amount of rain and snowfall is expected to increase in the winter and spring, summers are expected to get much drier. That is expected to have consequences on everything from forest fires to agriculture. CBC News

NATIONAL SECURITY / SÉCURITÉ NATIONALE

NIL

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

U.S. Customs Brokerage Leader, Carmichael International Service Expands To Canada
Carmichael International Service, a division of APL Logistics and one of the largest customs brokerage, trade compliance and consulting specialists in the United States, today announced that it will expand its full suite of services into Canada. The expansion will cover all major entry points into Canada. With this move, Carmichael will offer seamless assistance to importers throughout the USA and Canada. The move marks Carmichael's first expansion outside of the U.S. in the company's 55-year history. The expansion will be facilitated through the Kintetsu World Express (KWE) office network in Canada. KWE is the parent company of APL Logistics. "We are excited to offer our full suite of customs brokerage and trade compliance services and expertise to Canadian customers," said Todd Boice, President of Carmichael International Service. "This milestone event will establish a full-service Canadian footprint and network right out of the gate. Our whole team is looking forward to the single-source synergies and conveniences that this expansion will offer to North American shippers." Carmichael's Canadian Customs Brokerage operation will initially serve clients at border crossings and major airports through dedicated offices operated by KWE in Canada. Key offerings include: 24-hour/6-day a week coverage; compliance and transaction validation; classification; Non-resident importer (NRI) programs; documentation; duty payment processing; regulatory compliance; and electronic entry preparation, filing and release. All of these services feature full electronic integration with CBSA's ACROSS system. And all can either be used solely in Canada or integrated with Carmichael's U.S. or global service offerings. Ajot

Canada: Immigrant Children In Canada Outperform Canadians
Immigrants play an important role in bridging gaps in the labour market, both short and long-term. Statistics now confirm that the children of immigrants outperform children from Canadian-born parents in

educational attainment thus adding another important benefit that immigrants bring to Canada. These findings are outlined in a Statistics Canada paper entitled 'Educational and Labour Market Outcomes of Childhood Immigrants by Admission Class' and reveals that children of immigrants graduate high school at a rate of 91.6 per cent, against 88.8 per cent of children who are third generation or more. At university, the gap increases, with 35.9 immigrant children graduating against 24.4 per cent from the established Canadian group. In educational terms, third generation Canadians are also bettered by every class of refugee in both the high school and university graduation categories. Only when it comes to average earnings does the third-generation Canadian group rank on top, at $46,100 compared to $42,900 for immigrants. Mondaq

Canadian Border Equally Vulnerable as Mexico
The U.S.-Mexico border is a hotbed for controversy regarding illegal immigration, but immigration officials have become equally as worried with the Canadian border. Border Patrol officials have expressed concerns about the amount of people trying to get into the U.S. through Canada as well as the drug smuggling. “Its definitely less secure, its longer and there are far fewer agents that are assigned to the Canadian border,” says Shawn Moran, spokesperson fro the National Border Patrol Council. “You have large areas that go largely unpatrolled for long stretches of time,” he says. “So if someone were to cross the Canadian border in a remote area, it could take several hours for a border patrol agent to get out there and be able to check, and hopefully apprehend that person.” Moran says radical Islam also is a real threat along the northern border, pointing to an arrest made back in 2000. “Border Patrol agents were the ones that stopped the 'Millennium Bomber' who crossed through Port Angeles, Washington,” he says. “So we know there is several hundred radicalized Canadian citizens, and that is a concern to us, that they would try to come to the United States and conduct attacks here.” KTRH

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

New Documents Show How Canadian Cops Use Secret Phone Surveillance Technology
New court documents are shedding more light on the controversial use of mobile phone surveillance technology by Canadian police, the second such case to emerge this year. In the new case, court documents recently filed in a Toronto court show that the Royal Canadian Mounted Police (RCMP) used a device commonly known as a Stingray, or IMSI catcher, during a pair of criminal investigations into organized crime in early 2014. However, lawyers for the accused have argued that police misrepresented the nature of the device when seeking permission for its use by failing to disclose its range, its ability to pinpoint the location of phones, and potential for interference with 911 calls. In a hearing that was originally slated for Tuesday — but postponed — the defense will seek more information about the IMSI catcher's capabilities and operating manual, the device's effect on non-targeted phones, and a copy of the non-disclosure agreement (NDA) between the RCMP and the device's manufacturer. Notably, crown lawyers have argued the NDA prevents the RCMP from disclosing further information about the device, its capabilities, and how it used. "This is despite the fact that the agreement in place — likely akin to the ones in place with American law enforcement agencies — is almost surely unconstitutional," the defence lawyers write. The existence of the highly secretive technique has been known in the US for years, but Canadian police have attempted to keep details about the technique secret. It is only in the past few months that information detailing the use of IMSI catchers by police in Canada has come to light. The RCMP have frequently been in court in recent years, fighting to keep a lid on its high-level surveillance tactics. Last month, VICE News revealed details of how the police agency obtained the global encryption key for all consumer-grade BlackBerry phones, and used it to bust a mafia murder plot in Montreal. Vice News

Case involving first documented use of 'stingray' technology in Toronto goes to trial

On Feb. 21, 2014, Detective Shingo Tanabe swore an affidavit in hopes of getting a warrant. Feuding gangs had been shooting in the streets, so he told a judge some powerful surveillance was in order. He suggested the Asian Assassinz gang could be dismantled only if Toronto Police could get a read on its shifting array of mobile phones. Police teams shadowing suspects needed a machine that mimicked a cellphone tower, he argued, capable of capturing data from all phones in a given radius. The document acknowledged some risks. Such as possible inadvertent interference with bystanders' data or 911 calls. Or, even that police could run afoul of Canada's radio laws. Yet, "investigators require a means to covertly identify the numbers of these mobile devices without alerting the subjects of the investigation," Det. Tanabe wrote. The sworn statement, obtained by The Globe from court documents, reveal the first documented use of police "stingray" technology in Toronto, the country's most densely populated metropolis. Across North America, this mobile-phone-targeting device - also known as an "IMSI catcher" - is being revealed as controversial and indiscriminate, but judges have endorsed the police legal logic in this case and others. Like other law-enforcement agencies in North America, Toronto Police have never publicly confirmed using an IMSI catcher. The force last year fended off a freedom of information request from a journalist by arguing before a tribunal that any such disclosure "would quickly lessen its effectiveness" or even "jeopardize the safety of law enforcement officials operating such devices." (…) The RCMP appears to have pioneered police use of such devices in Canada, and it is not clear how much latitude municipal forces have to use them. The Toronto Police affidavit materials suggest a Mountie expert was brought in to operate the machine in Toronto. Globe and Mail

Courtroom sealed as undercover officers testify at murder trial

An Edmonton court will take extraordinary steps today to protect the identities of five undercover RCMP officers set to testify at a first-degree murder trial. Had the police force had its way, the public and the media would have been banned from hearing what the officers have to say. The case involves Shawn Wruck, who is accused of murdering his girlfriend, Shannon Collins, in 2007. It took the RCMP years to lay charges. Wruck was arrested in 2013 after he allegedly confessed his crime to undercover officers in a so-called "Mr. Big" sting. That makes the officers' testimony in this case is crucial. Mr. Big sting operations involve police posing as criminals in an attempt to obtain a confession from a suspect. The target is often told a confession is the only way they can join a fictitious criminal organization. Last Friday, a federal Crown prosecutor representing the RCMP served 11th-hour notice to the judge and the lawyers involved in the case that she would apply Monday morning to have the courtroom sealed during testimony from all five undercover officers. Notice was also served to an Edmonton lawyer representing the media. CBC, Postmedia and CTV all opposed sealing the courtroom. "All of us find ourselves in what I would describe as an awkward situation," lawyer Fred Kozak told the court Monday. Justice Donna Shelley agreed, and appeared concerned about the short notice. "It could not have been a surprise to the RCMP that these officers were going to testify," she said. "It certainly could have been brought a long time ago." The RCMP requested the extreme measure to protect the safety of their undercover officers, concerned that suspects in other cases might attend the Wruck trial to expose their identities. CBC News

Woman's lengthy stay in Yellowknife RCMP cells unconstitutional, rules judge

A judge has ruled that a regular practice of the Northwest Territories justice system - holding women who are awaiting bail hearings in Yellowknife in RCMP cells - is a violation of the Charter of Rights and Freedoms. Women in custody awaiting court hearings in the city are often held in the RCMP detachment cells because there is no women's correctional facility in Yellowknife. On Friday, Judge Robert Gorin reduced a woman's 10-month sentence to eight months because of the charter violation. The woman had pleaded guilty to trafficking cocaine. She was kept in RCMP cells in Yellowknife for 12 days. "If she had been a male offender, in the normal course, she would have spent a day or two in RCMP cells," said her defence lawyer, Peter Harte. A man in the same circumstances would be housed at the North Slave Correctional Centre. Harte successfully argued that the extended stay in RCMP cells violated the woman's constitutional right to equal treatment under the law. "At North Slave Correctional Centre, you're not in solitary confinement - or close confinement as it's now called. You're in the general population, you get to watch TV, you get to go to the bathroom without having a camera watching you." The Crown had asked for a sentence of 15 to 18 months. CBC News

Dangerous new drug making its way north

Members of the Bonnyville RCMP Detachment are watching to see if the dangerous new opioid W-18 surfaces in the community. The drug first surfaced in the southern reaches of Alberta. It then appeared in Lethbridge, moved to the streets of Calgary and was finally identified in Edmonton last month. "I suspect it will continue to travel northward. I don't know when or the location but logically we can assume it will continue to travel north, though we haven't seen it yet," said S/Sgt. Luis Gandolfi. Gandolfi brought W-18 to the attention of town council last Tuesday. "It's a new trend we are starting to see in the province. It's my job to keep council informed," said Gandolfi. "(W-18) has been getting my attention so I wanted council to know that (Bonnyville RCMP) is aware of the issue." W-18 is a sister drug of Fentanyl. It is an opioid compound that can be pressed into pills. Fentanyl is 100 times stronger than morphine, and W-18 is 100 times stronger than Fentanyl. "It's like anything new. If there's something new, people want to try it if that's their lifestyle. (W-18) is the new kid on the block, a year ago it was Fentanyl," said Gandolfi. W-18 can be pressed into pills, or ingested as a powder mixed in with food or liquid. Doses are unreliable as they are manufactured by dealers. The first dose can be deadly. Gandolfi explained drug trends are slowly changing in the region. Methamphetamine is becoming more regular, as is cocaine. Bonnyville Nouvelle; Energetic City

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

NIL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Toronto gun violence must be addressed by entire city, Rexdale pastor says
A Toronto-area pastor says there's a feeling of hopelessness and helplessness in the city's Rexdale neighbourhood and it's a problem for the entire city to fix. On Sunday, a 35-year-old pregnant woman was shot and killed in a drive-by shooting while riding in the back seat of a vehicle in the area. Toronto police say Candice Rochelle Bobb shot was in the chest, but add she was not the likely intended target. Authorities say the 20-week-old premature baby is now in stable condition, but residents of Rexdale are still trying to cope with the reality of gun violence in the area. "I think the community is rightly feeling shocked and outraged," Sam Aragones, a pastor with the Rexdale Alliance Church, told host Matt Galloway Tuesday on CBC Radio's Metro Morning. (…)The pastor says he wants to see all three levels of government working to address issues plaguing the community, from a lack of resources and opportunities to a need for a stronger police presence. CBC News

Art installation seeks to unwrap human trafficking
Sarnia will soon be the latest community host to an interactive gift-box display highlighting the sordid reality of human trafficking. The Sarnia-Lambton Committee Against the Trafficking of Women and Children, along with a slew of partners, is bringing to the community a walk-in, seven-by-11-foot, steel GIFT (Global Initiative to Fight Human Trafficking) box. Outside, it's a pretty package, symbolic of the promises of wealth, travel and a better life that traffickers make to their would-be victims. But inside, stories and information unwrap the grim truth. Human trafficking includes people bought and sold for forced labour, sexual exploitation, organ harvesting, child soldiers and other purposes, according to the Sarnia-Lambton committee. "We still hear from people in our community, 'Really? Is that a problem in Sarnia?' And people have no idea that, yeah, it is happening here," said committee chairperson Michelle Batty. Sarnia may not be a likely destination site for human trafficking, but being a border community, Sarnia is part of the corridor along which people are trafficked from one destination to another, she said. Sarnia Observer

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

NIL

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Attentat commis à Paris en 1980: le suspect canadien sort de prison
Le principal suspect d'un attentat commis à Paris en 1980 contre une synagogue, l'attentat de la rue Copernic, a été remis en liberté avec un bracelet électronique, après un témoignage de son ex-épouse qui conforte son alibi et nécessite de nouvelles investigations. Trente-six ans après les faits, l'enquête est ainsi à nouveau relancée dans un dossier où les victimes avaient repris espoir après l'extradition fin 2014 d'Hassan Diab depuis le Canada, où il était un respectable professeur d'université en sociologie. Âgé de 62 ans, le Libano-Canadien est mis en examen en France, notamment pour assassinats terroristes, et considéré dans l'enquête comme l'auteur présumé de cet attentat perpétré devant une synagogue de l'ouest de la capitale. Bilan: 4 morts et une quarantaine de blessés le 3 octobre 1980, dans le premier attentat contre la communauté juive en France depuis la Seconde Guerre mondiale. Une juge des libertés et de la détention a mis fin jeudi à la détention provisoire du suspect et ordonné son assignation à résidence avec bracelet électronique, ont indiqué à l'AFP des sources judiciaire et proche de l'enquête. Le parquet de Paris a fait appel. Une nouvelle audience aura lieu le 24 mai. La Presse

Auditor general says leaks of spending review did not come from his office
Auditor general Michael Ferguson says a leak of his high-profile review of Senate spending couldn't have come from his office, pointing the finger back at the Senate as the source of the unauthorized release. Ferguson said his office hired an outside security firm to investigate his staff to see if any of them could have leaked the audit to journalists ahead of its public release in early June 2015. He told senators investigating the source of the leak that he is confident any information in the audit didn't come from his people, but said he can't be 100 per cent sure. It was that possibility that senators on the Senate's rules committee locked on to as they used the morning meeting to blame Ferguson's office as the source of the leak. This investigation is the second time in as many years that the Senate has looked into the leak of Ferguson's report, an event that senators argue violated their parliamentary privilege and the right to see the document before the public. In some cases, senators said they learned the details of the audit from reading media reports. Leaks to multiple media outlets, including The Canadian Press, made public the names of nine senators who would be recommended for referral to the RCMP for a criminal review, the total amounts owing for the 30 senators identified in the report as having problematic expense claims and the recommendations Ferguson made to overhaul Senate spending rules. Canadian Press (iPolitics); Ottawa Citizen

INTERNATIONAL

Surveillance de Salah Abdeslam: le travail de la police belge mis en cause
Le travail de la police belge dans la surveillance de Salah Abdeslam, seul survivant des commandos des attentats du 13 novembre à Paris, a été à nouveau mis en cause mardi par une télévision belge. Trois semaines avant les attaques qui ont fait 130 morts à Paris, Salah Abdeslam publiait le 23 octobre sur Facebook une photo où il pose avec l'emblème de l'organisation État islamique (EI), explique notamment

la RTBF, sans citer de source. La chaîne publique, citant un document confidentiel des autorités belges, indique par ailleurs que les enquêteurs belges disposaient d'informations sur des «échanges directs», début 2015, entre Salah Abdeslam et son vieil ami Abdelhamid Abaaoud, jihadiste notoire et alors futur organisateur des attentats de Paris. L'image d'un Salah Abdeslam revendiquant sur les réseaux sociaux ses liens avec l'EI n'avait pas échappé à l'Organe de coordination pour l'analyse de la menace (OCAM), mais «cela n'a, en son temps, entraîné aucune réaction ni du côté de la police, ni du côté du renseignement», selon la RTBF. Salah Abdeslam et son frère Brahim, originaires de Molenbeek, en région bruxelloise, avaient pourtant été signalés comme étant en voie de radicalisation dès janvier 2015. Agence QMI (Journal de Montréal, TVA Nouvelles)

Bombings in Baghdad kill at least 69

A wave of bombings struck outdoor markets in Shia-dominated neighbourhoods of Baghdad on Tuesday, killing at least 69 people, officials said — the latest in deadly militant attacks far from the front lines in the country's north and west where Iraqi forces are battling the ISIS group. The new, higher death toll comes after a bombing in the northeastern Baghdad neighbourhood of Habibiyah killed nine people and wounded 18 early on Tuesday afternoon. Police officials say the attack targeted a restaurant. In the largest attack of the day, a car bomb struck a crowded market in Baghdad's northeastern Shaab neighbourhood, killing 34 people there and wounded 75. Elsewhere in the Iraqi capital, at least 26 were killed. CBC News

Europe's Top Cop: It's 'Almost Certain' Terrorists Will Try to Strike Again

"The threat is alive and current. Another attempted attack is almost certain." For months, E.U. officials have faced criticism for failing to prevent the Paris and Brussels attacks, with many intelligence experts blaming the lack of information sharing. Away from the debate and out of the spotlight, the E.U's law-enforcement agency Europol has quietly tried to piece together the terror threats, working out of its sleek, modern headquarters in the small Dutch capital of The Hague. Europol has not escaped criticism, too: Some E.U. lawmakers fear some European officials want the organization to become a "European CIA." However, the organization is tiny by comparison to the CIA, with a staff of about 1,000 and a budget in 2015 of €94.4 million ($106 million). On May 13, exactly six months after the Paris attacks, the organization invited TIME into its fortress-like building to discuss the ongoing terrorist threat in Europe with Europol director Rob Wainwright. Wainwright's assessment is sobering, including that "several hundred" battle-trained European jihadists are likely plotting further major attacks, and that his agency is supporting some 50 ongoing terrorist investigations. Wainwright, who is British, is also convinced his country will be far less secure if Britons vote on June 23 to leave the E.U. in a so-called "Brexit." As for Europe as a whole, he says: "The threat is alive and current. Another attempted attack is almost certain." Time (2016-05-16)

Leaked NSA docs show details on Russian mobster, search for WMDs in Iraq, Guantanamo Bay 'Tiki Bar'

In-house newsletters from the clandestine National Security Agency have been released by an online news site -- part of the mountain of documents leaked by former NSA contractor Edward Snowden. The Intercept, whose founding editors were the first to publish documents leaked by Snowden, released on Monday the first batch of nine years' worth of the newsletters, which offer a behind-the-scenes glimpse into the NSA's work. The newsletters reveal efforts to eavesdrop on a Russian crime boss, the search in Iraq for possible weapons of mass destruction and help with interrogations at the U.S. military prison at Guantanamo Bay, Cuba. An article in the May 2003 newsletter describes how NSA spent "many months" obtaining the phone number of a Russian organized crime figure so his calls could be intercepted. The State Department asked the NSA for information on the boss of the Tambov crime network in Russia -- a figure known only as "Mr. Kumarin" -- and whether he had any ties to Russian President Vladimir Putin. The man later was convicted of fraud and money laundering and sentenced to 14 years behind bars. In a newsletter article published Dec. 22, 2003, an NSA liaison officer recounts a temporary duty assignment at Guantanamo Bay where the task was to provide intelligence to support Defence Department, CIA and FBI interrogations of detainees picked up off battlefields. The job entailed relaying information back to NSA, based at Fort Meade in Maryland. But sometimes, NSA would share "sensitive NSA-collected technical data" to help the interrogators. Associated Press (Calgary Sun, Winnipeg Sun, Edmonton Sun, Toronto Sun, Ottawa Sun)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fort McMurray Wildfire / Feu de forêt à Fort McMurray

CBCAlerts
#FortMcMurray fire grows to 354,000 hectares propelled by hot, dry weather conditions. Was estimated to be 284,000 hectares Monday. #ymmfire

CBCNS
Map showing growth of #FortMcMurray fire northwest of city, which led to evacuation of 8,000 oil workers overnight: pic.twitter.com/nPEzy4YU8u

CBCCalgary
Extreme fire behaviour making job dangerous for Fort McMurray firefighters http://ift.tt/1NwKGaa

CTVCalgary
WATCH LIVE NOW ~ Premier @RachelNotley provides update on northern Alberta wildfire and relief efforts https://t.co/nNdCTYZZIS

CityNews
Story: Explosion in Fort McMurray damages homes, fire destroys building http://ow.ly/YDOM300inoa

Other / Autre

GlobalNational
Fox Creek area evacuation order lifted. 2 hr notice still in place. #wildfires #alberta #yeg https://t.co/10PLGDnT2R

LAW ENFORCEMENT / APPLICATION DE LA LOI

rcmpgrcpolice
RCMP helps rescue 20 victims of #human trafficking through Operation Northern Spotlight. http://rcmp.ca/-5aH

RCMPNS
Police Week fact: #RCMPNS Police Dog Service has trained to travel by helicopter to access remote areas.

GRCNE
#Mardienvoiture – La Semaine nationale de la sécurité routière se déroule du 17 au 23 mai http://ow.ly/gK4N300i41y pic.twitter.com/BlEFfMwdig

PUBLIC SERVICE / FONCTION PUBLIQUE

natnewswatch
Auditor general says leaks of spending review did not come from his office | National Newswatch http://www.nationalnewswatch.com/2016/05/17/auditor-general-says-leaks-of-spending-review-did-not-come-from-his-office/#.VzsxB2ikM1F.twitter …

INTERNATIONAL

washingtonpost
NTSB expected to conclude that engineer in deadly 2015 Amtrak derailment lost track of where he was https://t.co/24KTo7iU6J

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

Today's News / Actualités
May 23, 2016 / le 23 mai 2016
09:00 - 18:00 ET

This collection contains news items that appeared online between 9:00 a.m. and 6:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 09h00 et 18h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

CBSA considers electronic tracking of detainees rather than holding them in custody
The Canada Border Services Agency is looking into tracking detainees electronically, rather than keeping them in custody. A government tender posted online this month asks industry for feedback on how to manage alternatives to detention, "including a community supervision program supported with electronic supervision tools," for people detained under the Immigration and Refugee Protection Act. In the criminal justice system, electronic supervision usually means using an ankle bracelet or something similar to track people via GPS or cellular data. It's used in several Canadian jurisdictions, including Nova Scotia and Ontario. The CBSA has the oft-criticized — and largely unchecked — power to hold non-Canadians in migrant detention centres indefinitely. There are usually about 600 "clients" in custody, according to the tender. With the government promising to increase oversight, the agency appears to be looking for ways to reform its practices. "Detention guidelines require CBSA officers to consider all

reasonable alternatives before detaining someone for immigration purposes and will consider all release proposals presented by or on behalf of the detainee," spokeswoman Wendy Atkin said (...) **Public Safety Minister Ralph Goodale** plans to convene an all-party parliamentary committee this year to look at the activities of CBSA and other security and intelligence agencies. ***"We will also be looking at where there are gaps or holes in the existing architecture," Goodale*** said in a scrum Wednesday. ***"One obvious one is CBSA, the border services agency that has no review mechanism whatsoever."*** Postmedia (National Post)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fort McMurray Wildfire / Feu de forêt à Fort McMurray

Notley gets kudos in handling Fort McMurray wildfire crisis, but hard work yet to come
Alberta Premier Rachel Notley is getting high marks for leadership in handling the Fort McMurray wildfire crisis, but political observers say the disaster remains a dicey political proposition with limited upside and a lot of downside. Political scientist Duane Bratt says the process of getting people back into their homes and getting aid and reconstruction money will tell the tale on how Notley will be remembered in the long term for her handling of the crisis. "On the political side ... if you handle it well, it's a short term blip," said Bratt, a political scientist with Mount Royal University in Calgary. "If you screw it up, it never goes away." About 80,000 evacuees begin returning in phases to Fort McMurray on June 1, almost a month after a raging blaze broke through the firelines and destroyed 2,400 structures, most of them houses. Canadian Press (Global News, Calgary Sun, Edmonton Sun)

Firefighters help their colleagues deal with stress of Alberta wildfire
There are small teams of Alberta firefighters travelling to Fort McMurray who aren't on the front lines of the wildfire that's been threatening the city, but are instead helping by listening to those who are. Patrick Jerome, a Medicine Hat firefighter, is a member of his department's Critical Incident Stress Management Team that recently travelled to Fort McMurray to assist crews deal with the mental effects of fighting such a large fire, which forced the evacuation of the city. Post-traumatic stress disorder is a known side-effect of emergency service work such as firefighting, and it's something that teams like the one Jerome is on work to prevent. "The fires that those guys fought is a lifetime of fires for a firefighter. It's just so much firefighting that they've done in so little time," said Jerome, speaking from Medicine Hat. "It's just so much. I can't believe what those guys went through." The four-member Medicine Hat team, which includes their chaplain, aren't mental health professionals but are trained in managing stress and draw from their own experiences. Canadian Press (Calgary Herald, Toronto Sun, Ottawa Sun, Calgary Sun, Edmonton Sun, Chronicle-Herald)

Evacuation order lifted for all Fort McMurray oilsands camps
A mandatory evacuation order has been rescinded for the remaining oilsands camps in the Fort McMurray area that were evacuated last week. Workers won't be able to return, however, until Alberta Agriculture and Forestry and Alberta Health Services complete fire and health inspections to ensure occupant safety. There is no timeline set for these inspections, but they are being completed as soon as possible, said Robin Smith, press secretary for the Regional Municipality of Wood Buffalo. CBC News; Global News; Bloomberg

Thousands of oilsands workers are losing pay while Fort McMurray fires shuts sites
While wages are continuing for many employees of oilsands companies forced off the job by Fort McMurray wildfires, thousands of tradespeople hired by contractors are off the payroll. "It's certainly an economic hardship. People have bills to pay, people make plans around when they expect the work will take place," Warren Fraleigh, executive director of the Building Trades of Alberta, said Friday. "Folks who have had a fairly lean winter (were) waiting for this work." He estimated 2,000 to 4,000 members of the trade union umbrella group lost their jobs after many oilsands operations were shut down or scaled back because of fire safety concerns. Postmedia (Financial Post, National Post)

Support for Fort McMurray spans the globe

News of the Fort McMurray wildfire has people around the world opening up their pocketbooks for displaced residents. The wildfire is now more than 520,000 hectares in size and remains out of control, but people across the globe are finding ways to help. Students at Hangzhou International School, a private K-12 school in China, are selling "Stay Strong For Fort Mac" wristbands to raise money for the Canadian Red Cross. They've already sold out of wristbands, and are in the process of ordering more. CBC News

Other / Autres

Feux de forêt : des ordres d'évacuations levées dans l'est du Manitoba
Les ordres d'évacuation ont été levés pour les régions de Nora Lake et Florence Lake, a déclaré le Service des incendies de forêt du Manitoba. Des pompiers travaillent encore près des routes environnantes. Ils peuvent à l'occasion retirer des arbres devenus dangereux, ce qui peut perturber la circulation automobile. Le gouvernement demande aux conducteurs de ne pas dépasser 20 km/h en raison du mauvais état des routes et de faire attention aux pompiers vêtus de gilets aux couleurs vives. Par ailleurs, il est encore interdit de faire des feux en pleine nature dans le centre et l'est du Manitoba. Certains feux de camp sont permis dans des structures désignées. Le Manitoba a enregistré 74 feux de forêt depuis le début de l'année. Radio-Canada; CBC News

Cottagers allowed back, but business slow to return in Caddy Lake
The wildfires along the Manitoba-Ontario border are hampering business in cottage country. Louay Alghoul, who owns Caddy Lake Resort in Manitoba's Whiteshell Provincial Park, said he's grateful the fire didn't touch his business but the situation has made for a slow start to the season. He's had 20 per cent drop in business compared to last year, but he's staying positive. If the rest of the summer holds out to be as nice as this weekend, in terms of the weather, Alghoul expects business to bounces back quickly. "We're ready for a really good season and it's starting beautiful," he said. CBC News

Possibility of funnel clouds today in Sask., Environment Canada says
Funnel clouds are possible in central and west-central Saskatchewan today, Environment Canada says. The weather agency issued a weather advisory for the Prince Albert, Martensville, Battlefords and Kindersley areas on Monday morning. It said a low pressure system spinning over southwest Saskatchewan will lead to the development of scattered showers and thunderstorms late this morning into this afternoon. As these storms develop, conditions will be favourable for funnel clouds. The threat of funnel clouds will decrease later this afternoon. CBC News; Radio-Canada; 620 CKRM

NATIONAL SECURITY / SÉCURITÉ NATIONALE

NIL

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

NIL

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

The fearless woman behind America's cyber rapid response team
Amid a torrent of cyberattacks and seemingly endless data breaches, the United States Computer Emergency Readiness Team, the government's premier cybersecurity monitoring unit, has never been busier. US-CERT, as it is known, protects the country's computer networks by analyzing malware samples, intrusion patterns, and other digital residue left behind by hackers, and then packages those insights into guidance for federal agencies and critical-infrastructure sectors (including the nation's most

sensitive shared resources, like power plants and hospitals). It deploys incident-response teams to the sites of massive cyberattacks (it worked with Sony in 2014 and the Office of Personnel Management in 2015), and it coordinates international cybersecurity efforts with other nations' CERTs. The mission of US-CERT, a Department of Homeland Security unit established in 2003, is to study active intrusions for lessons that can inform the design of more robust security systems. "One person's detection can be another person's mitigation," Ann Barron-DiCamillo, director of US-CERT, told the Kernel (…) As we see certain things trending, certain vulnerabilities—we put out a paper, I believe it was around this time last year, or maybe in the spring; I have to go back and look—and we partnered with our Five Eyes partners, so with CERT-UK, **Public Safety Canada,** Australia CERT, as well as the New Zealand CERT, and we looked across our domestic markets at what common vulnerabilities were we constantly seeing as far as incident-response activities and engagements, not only in our government space but also in our critical infrastructure and just general space of the Internet within our domestic markets. We came up with about 31 different CVEs, which are common vulnerability exploits. The Kernel

LAW ENFORCEMENT / APPLICATION DE LA LOI

Registre des armes: des policiers retraités le déconseillent
Le policier retraité du Service de police de la Ville de Montréal (SPVM) Marc Brisebois se souvient d'avoir toujours été reconnaissant pour toute information concernant les armes à feu qui apparaissait à son écran lorsqu'il devait aller patrouiller ou intervenir dans une résidence. M. Brisebois, qui a pris sa retraite en 2006 après 30 ans de carrière, a affirmé que ces renseignements permettaient de prendre des décisions plus rapidement, et que ses collègues et lui-même étaient heureux de les avoir. Vingt et un ans après la création du registre fédéral des armes à feu, qui a été aboli en 2012 par l'ancien gouvernement conservateur, le Québec travaille à mettre sur pied sa propre base de données sur les armes sans restrictions. La Presse Canadienne (La Presse); Canadian Press (Global News, iPolitics, Charlottetown Guardian, St. John's Telegram, Cape Breton Post)

Darryl Rondeau accused of pretending to be a Fort McMurray evacuee, bilking donations
A British Columbia man is facing charges for impersonating a Fort McMurray evacuee and allegedly taking advantage of people who were trying to help, police say. The RCMP says they received a complaint from Family and Community Support Services in Claresholm, Alta., because they believed a man and woman were pretending to have evacuated the wildfires. Police allege the man travelled to Claresholm and "took advantage" of people who thought they were helping wildfire victims. Canadian Press (National Post, Times Colonist, Vancouver Sun)

Woman pulled dead from water near Peggys Cove
A woman is dead after being seen in the water off of Peggys Cove, N.S., on Sunday afternoon. Peter Andrews, the On-Duty Division Commander for the Halifax Fire Department, confirmed they responded to a report of a woman spotted in the water around 1:40 p.m. local time. A local fishing boat pulled the body of the woman from the ocean and the crew attempted CPR. The boat transported her to the Government Wharf where emergency workers continued CPR, but the woman was pronounced dead. Peter Richardson, owner of Peggys Cove Boat Tours, said the woman was seen on the rocks at the popular tourist destination just moments before she ended up in the water. "There's a couple of people here that were standing close to her, but they saw her one minute and the next minute, she was in the water," Richardson said. CBC News; Chronicle-Herald

Moncton restaurant employee shot with pellet air gun in holdup, say RCMP
An armed robbery Sunday night at the Sun Sun Restaurant on Mountain Road in Moncton, N.B., has the local RCMP seeking the public's help. At 10:50 p.m. Sunday, "a man armed with a pellet air gun approached an employee out back of the Sun Sun Restaurant located at 979 Mountain Road and demanded money. During the incident, the employee was shot with the pellet gun." police said in a written release Monday. The employee was transported to hospital for treatment for non-life-threatening injuries, RCMP added. CBC News

Fusillade impliquant un policier : 10 accusations portées contre un Winnipégois
La Gendarmerie royale du Canada (GRC) annonce le dépôt de dix chefs d'accusation à l'endroit de Carl Devin Beaulieu à la suite d'un incident qui s'est soldé par une fusillade jeudi matin près de Portage-la-Prairie, dans le sud-ouest du Manitoba. Selon la GRC, un de ses agents a ouvert le feu sur Carl Beaulieu à la suite d'une « interaction » qui s'est produite près de l'intersection de l'autoroute Transcanadienne et de la route 240. Carl Beaulieu a été hospitalisé, mais on ne craint pas pour sa vie. M. Beaulieu fait face à de nombreuses accusations liées à la possession d'une arme dangereuse et à une conduite au volant imprudente. Radio-Canada

RCMP patrolling highways for Canada Road Safety Week
Officers increased presence during May long weekend as part of national strategy. RCMP Cst. Chris Gunn explains the various pieces of equipment inside his patrol car to premier Wade MacLauchlan before heading to a checkstop in Queens County. Police will be patrolling Island highways today as part of a national campaign to make roads safer in Canada. Officers choose the first long weekend of the "summer" from May 17-May 23 to hold Canada Road Safety Week. Charlottetown Guardian

Saskatchewan RCMP on lookout for missing man
Saskatchewan RCMP are asking the public for help in locating a missing 40-year-old man. Keith Leavens, of Lashburn, was last seen on the evening of May 17 when he left his mother's residence in Lloydminster. Maidstone RCMP believes he may have been in the Lloydminster area at around 9 p.m. CT on May 19. Leavens is believed to be travelling in his grey 2006 Pontiac Montana van, which may have Alberta licence plate BSL3619. Global News; StarPhoenix

Police seeking help in finding missing Royal Road woman
A 54-year-old woman from Royal Road has gone missing and the West District RCMP is asking for the public's help in locating her. Odila Marie Daigle was last seen leaving her home on Route 620 on Sunday at around 7 p.m., according to a written statement from the RCMP. Route 620, known as the Royal Road as it approaches Fredericton, runs between the capital city and the village of Stanley. CBC News

Teenager injured in Midnapore explosion
Members of the Calgary Police Service are investigating an afternoon explosion that sent a teenage boy to hospital. According to police, emergency crews were called to a location on Midridge Close Southeast early Monday afternoon after a male was injured by a homemade explosive device. CTV News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

NIL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NIL

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Liberals' pot plan looks for way to detect and deter drug-impaired driving
The man tasked with coming up with Canada's marijuana law has a proposal for dealing with one of the biggest issues facing legalization: prevention of driving under the influence of pot. While police can conduct field sobriety tests if they suspect a driver is impaired by any substance, there is no established breathalyzer equivalent in roadside policing to easily detect and measure impairment when it comes to driving while high. Liberal MP Bill Blair says oral fluids testing could be the roadside measure used by Canadian authorities to detect marijuana in a person's system. "The kits are currently used in Europe," Blair told CBC News in an exclusive interview. The oral fluids drug test is conducted with a small plastic stick. When the police officer suspects a driver has smoked marijuana, the officer would take the stick and swipe it over the driver's tongue. The saliva would then be mixed with the enzymes in the device. If a red line appears three minutes later it indicates there are drugs in the driver's system. The officer would then have the right to take the driver to the station for a full evidence test. CBC News

Tougher laws against drunk driving 'well overdue,' MADD Canada says
New laws aimed at getting tougher on impaired drivers could be in the works, following a meeting between Newfoundland and Labrador's Liberal caucus and the chief executive officer of MADD Canada. "It's been years since the provincial government has done anything major in the area of impaired driving. It's well overdue," said Andrew Murie, CEO of MADD Canada, about the meeting held earlier this month at Confederation Building (...)While in the province, Murie also met with the RNC and RCMP about introducing saliva testing for drivers impaired by drugs. Murie said instances of drugged driving are rising on the province's roadways. CBC News

PUBLIC SERVICE / FONCTION PUBLIQUE

With civil service shakeup, Trudeau brings youth, diversity to top jobs
Retirements of Ottawa's highest-ranked bureaucrats have accelerated under the Justin Trudeau government as the Liberals shuffle the leadership of the public service after years of management under Stephen Harper. The government has made a series of moves with its highest-ranked bureaucrats since coming into office last fall, most recently promoting senior officials who had worked on the Environment and Foreign Affairs portfolios. Ian Shugart, a bureaucrat who for a couple of years managed Environment Canada under Mr. Harper, and Daniel Jean, the Foreign Affairs deputy minister who has advised the Trudeau government on key files from refugees to Canada at the UN, both received promotions as about seven senior mandarins announced their retirements (...) Privy Council Clerk Michael Wernick, the head of the public service appointed by Mr. Trudeau in January, has been working on the appointments, recently promoting Louise Levonian to deputy minister of Employment and Social Development Canada. Ms. Levonian had been serving as an associate deputy for the department and prior to that was a senior Finance Department and tax policy official under the Conservatives. Mr. Jean, who had served as deputy minister of Foreign Affairs since 2013, was heading the department as the Trudeau government implemented key foreign-policy priorities after the election, including Canada's withdrawal from air strikes in Syria and Iraq and the resettling of 25,000 Syrian refugees. Mr. Jean, in his new position as national security adviser to the PM, takes on one of the most important public-servant roles in government, advising Mr. Trudeau on top-secret national-security issues. He replaces Richard Fadden who retired in March. **Malcolm Brown**, who served as special adviser to Mr. Wernick in the efforts to welcome the 25,000 Syrian asylum seekers, was also promoted in April, to deputy minister of **Public Safety (...)**The handful of deputies who have retired include Mr. Fadden, **François Guimont**, Colleen Swords, George Da Pont, Matthew King, Krista Outhwaite and Daphne Meredith. Globe and Mail

OTHER / AUTRES

Stéphane Dion urged to use Saudi arms deal to free Raif Badawi
Foreign Affairs Minister Stéphane Dion is being urged to use Canada's $15-billion combat vehicle deal with Saudi Arabia to seek clemency for imprisoned blogger Raif Badawi when he meets with senior members of the ruling monarchy in the Mideast country Monday. Mr. Dion expects to meet one-on-one with the powerful son of the Saudi King, 30-year-old Deputy Crown Prince Mohammed bin Salman, who

is the Defence Minister and also in charge of reforming the Saudi economy. Former Liberal justice minister Irwin Cotler, Mr. Badawi's lawyer, sat down with Mr. Dion before he left for Jeddah, Saudi Arabia, where he will attend a meeting of the regional Gulf Cooperation Council. "I told him the Saudis have been so criticized internationally they might be looking for a way out to refurbish their image somehow," Mr. Cotler told The Globe and Mail in an interview. Globe and Mail (2016-05-22)

INTERNATIONAL

'That is not the son I raised': How a British citizen became one of the most notorious members of ISIS

The last member of the group of British jailers who supervised the torture and killing of Western hostages held by the Islamic State has been identified as a 27-year-old Londoner who traveled to Syria in 2012. El Shafee Elsheikh, a British citizen whose family fled Sudan in the 1990s, was one of four jailers dubbed the "Beatles" by their prisoners because of their British accents. The cohort's most prominent figure was Mohammed Emwazi, better known as "Jihadi John," whose videotaped beheadings of American and British hostages became a global emblem of the Islamic State's brutality (…) Elsheikh was identified through a joint Post and BuzzFeed News investigation. His name was confirmed by a former U.S. counterterrorism official and other people familiar with British nationals in Syria. They spoke on the condition of anonymity to discuss an ongoing investigation. The FBI declined to comment. Elsheikh's family said he is still alive and living in Syria. He remains in touch with some friends and family — but not his mother, she said (…) Elsheikh, when he was 21, married an Ethiopian woman living in Canada but became frustrated when she was unable to move to London to be with him. The following year, the mother said, she started to noticed changes in her son after an older friend introduced him to the preaching of a West London imam known for his radical beliefs. Washington Post; Independent UK

Egypt official says plane didn't swerve, plummet as claimed

The head of Egypt's state-run provider of air navigation services says that EgyptAir flight 804 did not swerve or lose altitude before it disappeared off radar, challenging an earlier account by Greece's defence minister. Ehab Azmy, head of the National Air Navigation Services Company, told The Associated Press on Monday that in the minutes before the plane disappeared it was flying at its normal altitude of 37,000 feet, according to the radar reading. He says, "that fact degrades what the Greeks are saying about aircraft suddenly losing altitude before it vanished from radar." Associated Press (Globe and Mail, CBC News)

Bombs kill nearly 150 in Syrian government-held cities: monitor

Bombs killed nearly 150 people and wounded at least 200 in Jableh and Tartous on Syria's Mediterranean coast on Monday in the government-controlled territory that hosts Russian military bases, monitors and state media said. Islamic State claimed responsibility for the attacks in the cities that have up to now escaped the worst of the violence in the five-year-old conflict, saying it was targeting members of President Bashar al-Assad's Alawite minority. The Britain-based Syrian Observatory for Human Rights said 148 people were killed in attacks by at least five suicide bombers and two devices planted in cars. State media had said 78 people had been killed in what is Assad's coastal heartland. Reuters

Attacks in Yemeni port city of Aden kill at least 45 men waiting to join army

Suicide bombers targeting prospective army recruits killed at least 45 and injured many in the restive southern Yemeni city of Aden in two assaults, highlighting the obstacles to ongoing peace talks in Kuwait. The first attacker targeted applicants gathered outside the home of a military commander, Brig. Gen. Abdullah al-Subaihi, killing at least 25, according to witnesses and Yemeni officials (…)The second attack unfolded 10 minutes later outside an army base that also served as a recruitment center, killing at least 20, witnesses and officials said. Washington Post; Associated Press (Toronto Star)

Future of national security whistleblowing at stake in US inquiry

Former head of the CIA David Petraeus, in an interview published in the Financial Times on 6 May, was asked if Edward Snowden should be prosecuted. "Unquestionably," said Petraeus (…) "If Snowden had wanted to help that debate, he could have very easily been a whistleblower who could have gone to the

appropriate organization and offered his views. He didn't." It is a line that has been repeated by Barack Obama, Hillary Clinton and just about every other establishment figure asked about Snowden. Rather than a leak to the media, they argue, there were alternative routes: he could have taken his concerns to Congress or pursued the official internal route, through the inspector general's office. But a powerful new insider account undermines the idea that the inspector general's office offers whistleblowers a safe route. John Crane supervised the whistleblower-protection unit of the Pentagon inspector general, which has oversight responsibility for defense department components such as the National Security Agency. His story, told at length in Mark Hertsgaard's powerful new book Bravehearts: Whistle-Blowing in the Age of Snowden, suggests that an office meant to aid whistleblowing can put whistleblowers in danger. Guardian UK

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

HuffPost Canada
Notley gets top marks for handling of wildfire crisis http://huff.to/1TSaURk

BreannaKarstensSmith
Still hot and dry up in #ymm. Fire fighters putting out hot spots by the entrance to the city #ymmfire

Manitoba Gov News
For further general information on #Manitoba wildfires, go to http://www.gov.mb.ca/wildfire/ #mbfire

Manitoba Gov News
Evacuation orders for Nora and Florence lakes now lifted. Road conditions may be poor; recommended speed is 20kph. #Manitoba #mbfire

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Colin Freeze
This amounts to a relative bargain. Canadian police paid a terror mole $4-M back in '06 http://www.theglobeandmail.com/news/national/how-a-police-agent-cracked-a-terror-cell/article4285642/ ...)

Mukhtar Ibrahim
FBI informant says he was paid $100,000, most of it in cash, for secretly recording his fiends' conversations.

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

National Post
CBSA considers electronic tracking of detainees rather than holding them in custody http://natpo.st/1Vg02lc

LAW ENFORCEMENT / APPLICATION DE LA LOI

CTV Calgary
B.C. man charged after allegedly impersonating Fort McMurray wildfire evacuee

Global Montreal
Retired police officers warn #Quebec against starting costly gun registry

CTV Calgary
Teenager injured as homemade explosive device detonates in Midnapore http://bit.ly/1YT0iFK #yyc

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

The Globe and Mail
Fentanyl pushes heroin off the streets in Vancouver http://trib.al/XjGF98K From @GlobeBC

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Hannah Thibedeau
Oral fluids test proposed to detect stoned drivers as new pot law approaches http://www.cbc.ca/1.3591671 #cdnpoli #hw

PUBLIC SERVICE / FONCTION PUBLIQUE

Claire Wählen
Paging @Baxfacts: Privy Council Office says removing 'Action Plan' signs not Ottawa's job

OTHER / AUTRES

Stewart Bell
"My government has abandoned me," says Canadian held hostage by Abu Sayyaf.

INTERNATIONAL

CBC World News
EgyptAir didn't swerve before crashing, Eyptian authorities say http://ift.tt/1WdLYtu

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

Today's News / Actualités
June 4, 2016 / le 4 juin 2016
11:00 – 18:00 ET

This collection contains news items that appeared online between 11:00 a.m. and 6:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 11h00 et 18h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fort McMurray Wildfire / Feu de forêt à Fort McMurray

Re-entry delayed for Fort McMurray neighbourhoods hit hardest by wildfire
Dangerously toxic ash barred some Fort McMurray residents from re-entering some of the most badly damaged neighbourhoods of the city on Saturday. The Abasand, Beacon Hill and Waterways

neighbourhoods were originally scheduled to reopen on Saturday, the fourth day of re-entry. Residents from these areas were told last week they might have to wait until September, but they will now be given access to their properties on June 10. CBC News

Fort McMurray wildfire: Final day of re-entry for liveable neighbourhoods
The last of the Fort McMurray neighbourhoods considered safe enough for re-entry began to welcome back its residents Saturday, on the fourth day of the province's voluntary phased re-entry plan. People who fled the communities of Grayling Terrace and Draper, which make up Zone 4(b), were expected to join the thousands of people who arrived in the northern Alberta community earlier in the week after being forced out by a massive wildfire last month. As of 2 p.m. on Friday, the enormous wildfire remained out of control but was considered to be 56 per cent contained. It now covers more than 581,000 hectares including part of Saskatchewan. The province said 2,146 firefighters and support staff were battling the blaze with the help of 80 helicopters and 219 pieces of heavy equipment. While the gradual return of residents continued Saturday, there was still no timetable for re-entry into the hard-hit neighbourhoods of Abasand, Beacon Hill and Waterways, considered uninhabitable because of toxins and where debris is still being removed by the municipality. Global News

Fort McMurray business owners call for financial help in face of uncertain future
As Fort McMurray fire captain Ryan Pitchers battled the wildfire known as "The Beast" with all his might, he wondered, as a business owner, if his downtown pet food store would still be standing afterwards. "Is it going to burn down, is it going to be damaged or what's going to happen in the future?" Pitchers, a co-owner of Pet Valu, asked himself. As the fire began to retreat from the city, Pitchers spent his downtime with some friends rescuing two hedgehogs, a lizard and other animals from his store (…) But now, Pitchers has another rescue on his hands: his business. It's the weighty task facing many Fort McMurray business owners who were already struggling in a slumping economy. CBC News

Psychological challenges loom as large as reclamation tasks for Fort McMurray residents
Fort McMurray's scars are not just on the landscape, but in the psyche. Like many of Fort McMurray's returnees, Kenny St. Croix hoped he was emotionally prepared for the trip home. That's not how it turned out. "You think you're strong? You can't prepare yourself for that," St. Croix, 60, said Friday, recounting his experience staring at the remains of the Timberlea home he and his son shared. "Kinda tough. Kinda tough," he said, noting his daughter also lost her house in nearby Parsons Creek. "I'm trying to warn the kids before they come back. I took a video, and I sent it down to them, so I've kind of prepared them the best I can. But they'll still be shocked (…)"As a sign of the psychological hardships returnees are facing, about 275 people sought mental health support Thursday, including 114 one-on-one appointments, Alberta Health Services said. It's a significant number, especially for a town known for a tough work ethic and a reputation for shrugging off adversity. Residents may go through many phases of grief over the next few days and weeks as they think about what they've lost and feel anxiety about rebuilding their lives, said Marjorie Epp, a clinical supervisor overseeing community mental health at the temporary urgent care centre. Edmonton Sun (Calgary Sun)

Plus de 800 voitures abandonnées attendent d'être réclamées
En vidéo ci-dessus, revoyez les images saisissantes d'un résident de Fort McMurray forcé de fuir et de tout laisser derrière lui, le mois dernier. Plus de 800 voitures abandonnées il y environ un mois par les sinistrés de Fort McMurray attendent maintenant d'être réclamées par leurs propriétaires. Des remorques de la fourrière Mobster Towing ont travaillé sans relâche pendant des semaines pour remorquer les véhicules, a rapporté le *Edmonton Journal* vendredi. Les voitures ont pour la plupart été laissées sur le bord des routes, mais certaines ont été abandonnées en plein milieu des voies de circulation. Agence QMI (TVA Nouvelles)

Les incendies de Fort McMurray ont envoyé des cendres jusqu'en Suisse
Des cendres et de la poussière générées par les immenses incendies qui frappent l'ouest du Canada depuis un mois ont atterri en Suisse, selon des météorologues suisses. «Les feux ont injecté une quantité énorme de poussière dans l'atmosphère» dont la présence «est actuellement mesurée au-dessus de la Suisse», indiquent les autorités météorologiques suisses dans un rapport publié sur son site et repris dans la presse suisse vendredi. Agence France-Presse (TVA Nouvelles) (2016-06-03)

Other / Autres

'Cascadia Rising' earthquake drill to commence on June 7
A magnitude 9.0 earthquake along the Cascadia subduction zone and the resulting tsunami have devastated the Pacific Northwest. Telephone and Internet service is gone, leaving ham radio operators our only means of communication with the outside world. It is a frightening scenario, and probably the most complex and devastating disaster emergency services and public safety officials in the Pacific Northwest could ever face. KXRO explains that this scenario called "Cascadia Rising" will be played out starting June 7, and will last until June 10. Be aware that this is a drill, and it will be big. This drill is a simulation of a complete rupture of the Cascadia subduction zone (CSZ), causing a magnitude 9.0 earthquake situated 100-150 miles to the West of the Coastline in the Pacific Ocean. Emergency Operations and Coordination Centers (EOC/ECCs) at all levels of government and the private sector will be included in a simulated field response operation within their jurisdictions and with neighboring communities, state EOCs, FEMA, and major military commands, according to FEMA. Digital Journal; Express (UK); News Tribune

Russian Satellite for Defense Ministry Put Into Orbit
A Russian satellite for the needs of the country's Defense Ministry has been successfully put into orbit, the Russian Defense Ministry said on Saturday. "The launch [of the satellite] into orbit has been carried out in a normal mode," the ministry's press service told RIA Novosti. Earlier in the day, Russia launched the Rokot carrier rocket with the satellite from the Plesetsk space center in northwest of the country. The Rockot carrier, first launched from the Plesetsk spaceport in 2000, has so far put 65 satellites for various purposes into the orbit. Sputnik News; TASS; TeleSur

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Islamophobia runs deeper than failed Tory election tactics
An opinion piece states "Muslim Conservative Uruzurum Heer made headlines recently for castigating the Islamophobic campaign run by her party in the last election. "This party worked actively and aggressively against my people," Heer said, at the Conservative convention. "It didn't differentiate who Muslims were versus the enemies." The Harper-headed Conservatives certainly deployed a particularly crude form of anti-Muslim animus during the election: a continuation of their governing modus operandi. However, Islamophobia did not begin with Stephen Harper, and it will not end with his exit from power. It is very tempting to relegate Islamophobia to a past we have overcome or to a future we have avoided. It is too easy to project racism onto other times or onto other people: onto those like Stephen Harper or Donald Trump, who ostentatiously brandish anti-Muslim stereotypes as political weapons. It is far more difficult to confront the normalized Islamophobia that has permeated Canadian national security law and policy since the initiation of the War on Terror, under both Liberal and Conservative governments (…) Stereotypes about Muslim violence have sustained the War on Terror's project of violence since its birth. The War's dangerous excesses in Canada — an extra $92 billion allocated to national security spending in the decade after 9/11; expansion of state powers of surveillance, which have been used to monitor and stifle activists and dissenters; the proliferation and broadening of terrorism offences, to now include such vague crimes as "promoting or advocating the commission of terrorism offences in general" — have been justified by citing the supposedly excessive danger posed to Canadians by Muslim "terrorists." Toronto Star

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CBSA pilots new initiative in Manitoba with the Canadian Centre for Child Protection
The Canada Border Services Agency (CBSA) has announced that they will be working on a pilot project in Manitoba with the Canadian Centre for Child Protection (the Canadian Centre) to enhance officer knowledge and training for identifying situations involving missing, sexually abused and exploited

children. This Manitoba pilot project involves the CBSA and the Canadian Centre working together to better identify missing and abducted children, and those at-risk of exploitation, at the border. The Canadian Centre will provide support to officers with specific cases where they must intervene, such as abduction and family reunification or instances where children or youth may be at-risk of sexual exploitation. “Protecting and identifying missing children is a matter that is close to the hearts of our employees,” said Kim R. Scoville, Regional Director General, Prairie Region, Canada Border Services Agency. mySteinbach

Air Canada grounds Toronto family after passports are stolen
When Keethai Tharmaseelan's family had their passports stolen from their hotel room during an Arizona vacation last April, Air Canada assured them that their return tickets were enough to fly back to Toronto. They had no idea of the ordeal that awaited them. On their departure day, the family of four did make it through Phoenix airport security. But just before an Air Canada agent handed them their printed-out boarding passes, another agent came along - and told them it was "illegal under Canadian law" to travel back to Toronto without passports (...) Tharmaseelan's family isn't the first to be unexpectedly grounded thanks to mixed messages from Air Canada staff about missing passports. Last year, a Kelowna, B.C., woman who lost her passport on an Air Canada plane wasn't allowed to board a return flight from Philadelphia - even though, she told Global News, officials had repeatedly assured her she could. When Tharmaseelan called the Canadian consulate about her family's stolen passports, they told her to speak with her airline. An Air Canada rep told her that, because they'd purchased round-trip tickets, all of their information was still logged in Pearson International Airport's system. The Canadian consulate also told Tharmaseelan that Pearson would let her, her husband, and their two young children through, as long as security could verify their ID another way. Toronto Star

Canada's dairy farmers say diafiltered milk from U.S. costs them millions
Our wily neighbours to the south have figured out a clever way of not paying tariffs on a certain — let's say "controversial" — commodity, and Canadian dairy farmers say it's costing them hundreds of millions every year. The product in question is called diafiltered milk. Essentially, it's milk that's filtered, flushed with water, and then filtered a second time, with a few other steps along the way. The end product has a high concentration of protein, about 85 per cent, and very little of the fat and lactose that make up natural milk. The Canadian government allows it to cross the border without a tariff, because if it were dried into a powder, it would have the same amount of protein as the kinds of protein powders allowed to pass through tariff-free under trade agreements. CBC News

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

City of Moncton unveils memorial to slain Mounties
A commemorative sculpture was unveiled in Moncton Saturday on the second anniversary of the shootings there that left three RCMP officers dead. Constables Doug Larche, Fabrice Gevaudan and Dave Ross were killed as they responded to a call regarding a man carrying weapons. Newfoundland artist Morgan MacDonald was chosen to make the permanent monument, which has been placed in the heart of Moncton, in Riverfront Park on the banks of the Petitcodiac River. Among the speakers were RCMP Deputy Commissioner Dan Dubeau, local MP and government leader in the House of Commons Dominic LeBlanc, New Brunswick Premier Brian Gallant and former Moncton Mayor George MacDonald. The wives of the three slain Mounties, Nadine Larche, Rachael Ross and Angela Gevaudan, also spoke at the ceremony. The families got an early chance to view the finished memorial on Friday afternoon. CBC News; Global News; Radio-Canada; TVA Nouvelles; Canadian Press (The Guardian, London Free Press, Toronto Star); Kelowna Now; La Presse Canadienne (L’Actualité)

Des restes humains découverts à Rosthern
La Gendarmerie royale du Canada (GRC) enquête sur la découverte de restes humains sur une ferme près de Rosthern, au nord de Saskatoon. La GRC n'a pas indiqué quand la découverte a eu lieu, mais a souligné qu'un fermier a trouvé les restes et a contacté les policiers par la suite. Les causes de la mort et l'identité de la victime n'ont pas été dévoilées. Radio-Canada

Un entrepreneur québécois arrêté à Fort McMurray
Un Québécois de 33 ans a été arrêté en Alberta, pour avoir forcé le coffre-fort laissé derrière par un sinistré de Beacon Hill. La Gendarmerie royale du Canada de Wood Buffalo a arrêté l'individu jeudi, a rapporté Global News. Les policiers ont précisé que l'homme, dont l'identité n'a pas été révélée, devra se présenter en cour le 7 septembre prochain, à Fort McMurray, les accusations exactes portées contre lui n'ont pas été précisées. La GRC a précisé que le coffre était vide et qu'aucun autre item n'a été volé. Journal de Montréal; Agence QMI (TVA Nouvelles); Canadian Press (National Post)

Rescue crews call off search for missing swimmer in Fraser River
Rescue crews have called off a search for a missing swimmer in the Fraser River on Saturday morning. The man disappeared overnight in Surrey's Brownsville Bar Park located between the Pattullo Bridge and the neighbouring SkyTrain bridge. According to RCMP, a group of men were drinking on the beach when they decided to swim around the SkyTrain bridge pillar and back to shore. A 32-year-old Burnaby man was spotted going under the water and never came up. Divers were seen going into the water and a coast guard hovercraft was also on scene. RCMP say they were unable to locate the man after several hours of searching, and made the difficult decision to call off the search. Global News; Vancouver Sun

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Dispatches from an indefinite period in isolation
The guards led Richard Wolfe to the segregation unit in April, 2014. They stopped at cell five, considered the most luxurious because it was wheelchair-accessible and slightly larger than the others: 12 feet by 10, Richard guessed. As he stood at the door, he saw a bunk covered by a thin mattress. On one side of the room sat a stainless-steel toilet with built-in sink. Natural light filtered in through a skinny window about six inches high and two feet wide. For the next 21 months – though he didn't know it at the time – this would be his home (…) Over the next 91 weeks, Richard regularly wrote letters and made phone calls describing what it was like to be locked in segregation. His account provides a rare glimpse inside a prison regime that is controversial, little known and, according to prominent critics, counterproductive (…) As a founder of the Indian Posse, a large, primarily indigenous street gang, he was a high-profile inmate and a significant target for rival gangs. Although his brother died in 2010, and Richard said he himself had left the Indian Posse more than a decade ago, the Wolfe name remained notorious in Canadian prisons. And, because he faced a charge of sexual assault, the unwritten rules of prison subculture made him vulnerable to attack. Globe and Mail

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NIL

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

5 questions with Carolyn Bennett, minister of Indigenous affairs
She has been called the minister of reconciliation (…) She sat down with *Unreserved* host Rosanna Deerchild and answered questions about her new job, the history between Indigenous peoples and the

Canadian government and what she hopes an inquiry into missing and murdered Indigenous women will accomplish (…) *Let's focus in on the missing and murdered Indigenous women inquiry that the Liberal Party is set to launch. What was it like to go across the country meeting families and hearing their stories?* "I think having the three ministers — the Minister of Justice Jody Wilson-Raybould, and Minister [Patty] Hajdu is the Minister of Status of Women and myself — hear directly from the families who have been so frustrated over a decade, I think we learned a lot. It's very different than a report on your desk with a few quotes in the margin. "There are real regional differences coast to coast to coast, therefore the solutions are going to have to be different. The actual root causes of poverty and housing, sexism and racism in policing, child abuse, the child welfare system, these are common elements, deep, complex." *What do you hope to see come out of the MMIW inquiry?* "In listening to the families, they want justice. They want to seek justice and they want to stop the uneven application of justice that happens coast to coast to coast. They feel their loved ones' lives were less valued. They want healing for themselves and their families, but mainly every one of them wants to prevent this. They want this to stop. This tragedy has to stop." CBC News - Unreserved

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Legal cannabis lobbyist opposes illegal dispensaries
More than half of the 31 licensed marijuana producers in Canada are members of a lobby group called Cannabis Canada. Members of Cannabis Canada have been vocal in their opposition to illegal marijuana dispensaries, like the ones raided at the end of May in Toronto. The group talked to city authorities months before the police crackdown, warning them of the rapidly growing number of pot shops operating outside the law. *Out in the Open* talked with Cam Battley, who is the Chair of Cannabis Canada Advocacy Committee and senior vice president of one of the licensed producers of medical marijuana, Aurora. Cam said that he finds it difficult to understand the anger and shock of the Toronto dispensary owners whose shops have been raided. "They were warned multiple times. There were letters delivered to their landlords. Essentially, the police were saying, 'We will bust you if you don't stop operating.' And then they got busted and they pretend to be shocked. I find that perhaps a little bit disingenuous." CBC News - Out in the Open

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Is ISIS preparing for 'Plan B' as losses mount?
With recruitment down, its finances squeezed and having lost considerable ground, ISIS just may be in the throes of near defeat, according to some analysts. But whether the Islamic State is on its last legs or is still capable of waging an indefinite campaign, attention is now being focussed on just what happens on the so-called "day after." "The West should have no illusion that the Islamic State will simply slump into defeat," wrote Brian Michael Jenkins and Colin Clarke, both of the Rand Corporation, which specializes in insurgency and transnational terrorism. "Instead, it must focus on thwarting the group's Plan B." That the group has formulated such a contingency plan is still a subject of speculation, and expert opinions differ on how close it is to actual defeat. "After maybe years of really stunning success, I think the Islamic State has run into trouble," said Austin Long, assistant professor of international and public affairs at Columbia University and a former adviser to the multinational force in Iraq. CBC News

INTERNATIONAL

Tropical Rains, Possible Tornadoes Threaten Half of the US
From tropical rains to tornadoes, about half of the U.S. expected to see wet and at times severe weather this weekend, capping a week of scorching temperatures out West and flooding that killed nine soldiers when their military vehicle got caught in the rushing waters of a rain-swollen creek at Fort Hood, Texas. People along the Gulf Coast kept a watchful eye on a system over the Caribbean Sea that was forecast to bring 5 to 10 inches of rain to parts of Florida. The storm is likely to develop into a tropical cyclone. Associated Press (ABC News, National Post)

Exclusive: Seven police chiefs warn over Brexit terror risk
Leaving the European Union would be a "gamble" with Britain's security that would put the country at greater risk of terrorist attacks, an alliance of seven top police chiefs warns today. In an open letter, the former chief constables say it is "vital" to be able to share fingerprint data and criminal records with police forces across Europe to stop jihadists and criminal gangs. There is "no case" for putting Britain's security at risk by withdrawing from the EU, they warn. Telegraph UK

Unofficial ISIS Apps Pose Security Risks For The Islamic State Group
The Islamic State group has used social media platforms and apps as vehicles to spread information to its followers as well as aid in recruitment. The apps, while being viewed as a trustworthy source of intelligence, can also be exploited, according to a report from Motherboard. Recent alerts sent out through official channels of the terrorist organization, also known as ISIS or ISIL, warn of fake news apps filled with malware. ISIS' app portfolio includes Amaq Agency for news and al-Bayan for streaming radio. There's also an instructional children's app where letters of the alphabet are associated with various pictures of weapons. An English version of Amaq Agency has been released, while other news apps in French and Turkish have been developed by the group. International Business Times

Exclusive: Snowden Tried to Tell NSA About Surveillance Concerns, Documents Reveal
On the morning of May 29, 2014, an overcast Thursday in Washington, DC, the general counsel of the Office of the Director of National Intelligence (ODNI), Robert Litt, wrote an email to high-level officials at the National Security Agency and the White House. The topic: what to do about Edward Snowden. Snowden's leaks had first come to light the previous June, when the *Guardian's* Glenn Greenwald and the *Washington Post's* Barton Gellman published stories based on highly classified documents provided to them by the former NSA contractor. Now Snowden, who had been demonized by the NSA and the Obama administration for the past year, was publicly claiming something that set off alarm bells at the agency: Before he leaked the documents, Snowden said, he had repeatedly attempted to raise his concerns inside the NSA about its surveillance of US citizens — and the agency had done nothing. VICE News

Niger's defence ministry says Boko Haram kills 32 soldiers
Niger's defence ministry says Boko Haram extremists attacked a military post near the country's border with Nigeria, killing at least 32 soldiers. The ministry said Saturday that hundreds of Boko Haram fighters attacked the post Friday night, killing at least 30 Niger soldiers and two soldiers from Nigeria. It said 67 other soldiers were wounded. The military reclaimed the post Saturday morning. Associated Press (Boston Herald); Reuters

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

Ralph Goodale
En souvenir des vies et du service de 3 membres héroïques de la GRC, tombés à Moncton.

Ralph Goodale
Today remembering the lives and service of 3 heroic fallen RCMP officers in Moncton.

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fort McMurray Wildfire / Feu de forêt à Fort McMurray

CBCCanada
Toxic ash bars Fort McMurray residents from returning to hardest hit neighbourhoods http://ift.tt/1ZmBxSs

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Stewart Bell
Three convicted in ISIS recruiting network with ties to Edmonton. https://www.justice.gov/opa/pr/federal-jury-convicts-three-minnesota-men-conspiring-join-isil-and-commit-murder-syria …

Star Opinion
Commentary: Islamophobia runs deeper than failed Tory election tactics

LAW ENFORCEMENT / APPLICATION DE LA LOI

Alison Crawford
Senate appears eager to give Mounties broad range of issues to collectively bargain http://www.cbc.ca/news/politics/rcmp-bill-c-7-senate-1.3615807 … #canlab #cdnpoli #cdnlaw

Tonda MacCharles
Here's my beat colleague @alisoncrawford5 on Senate tackling the #RCMP union bill.

CACP ACCP
Police leaders throughout Canada salute retiring @RCMPNB Commander Roger Brown. #Leadership #integrity #empathy

CACP ACCP
City of #Moncton unveils memorial to slain Mounties - #RCMP Constables Doug Larche, Fabrice Gevaudan and Dave Ross

chronicleherald
RCMP commander retires after tragic and emotional post in New Brunswick herald.ca/shr

CBCNB
Sculptor hopes Moncton Mounties monument brings peace, healing cbc.ca/news/canada/ne…

CBCNews
Memorial to slain Mounties unveiled in Moncton http://www.cbc.ca/1.3615620

globalnews
Honouring the lives of three fallen Mounties: monument unveiled in Moncton. glbn.ca/McaM7p

chsjnews
Moncton RCMP Monument Unveiled bit.ly/25G1O5v #Moncton #NewBrunswick #RCMP

MetroNewsCanada
Monument uses personal touches to honour fallen RCMP officers in Moncton ow.ly/pUSQ300V1vy

Alison Crawford
'Doug's coming home': Widow welcomes memorial to slain Mounties

edmontonjournal
Edmonton RCMP raise Pride flag prior to weekend festival. ow.ly/dTvo300V1yB #yegpride

GlobalBC

RCMP, coast guard search for missing swimmer in Fraser River glbn.ca/02tEUb

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

John Howard Society
640 days, 4 walls + 1 tiny window: Richard Wolfe's dispatches from solitary: Stop this cruelty /via @globeandmail

INTERNATIONAL

Rachel Browne
Exclusive: Edward Snowden tried to tell the NSA about his surveillance concerns, documents reveal https://news.vice.com/article/edward-snowden-leaks-tried-to-tell-nsa-about-surveillance-concerns-exclusive … via @vicenews

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

Today's News / Actualités
June 27, 2016 / le 27 juin 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Tax question raised over Canada's border data sharing plan
As part of a new border information exchange with the U.S., Canada has proposed legislation that would see personal data collected when truck drivers and other motorists *exit* the country, as is currently done at border *entry* points. The Act to amend the Customs Act-Exit information was introduced to the House of Commons on June 15, making good on the March announcement from Prime Minister Trudeau and President Barack Obama that both countries would implement a system to exchange basic biographic entry/exit data, all while maintaining privacy safeguards. The information collected would primarily be found within the traveller's passport, and the traveller's record of entry in one country could serve as a record of exit from the other, the legislation suggests. ***"It's important that we have a clear picture of who is entering and exiting our country so we can ensure the efficient movement of legitimate trade and travel and keep our border secure,"*** announced **Minister of Public Safety and Emergency**

Preparedness, Ralph Goodale, who introduced the legislation. But news of the entry-exit data exchange has created some concern for those seeking clarification around federal tax implications. An individual could be subject to the U.S. Internal Revenue Service's "substantial presence test" if he or she spends more than 120 days in the country over the course of a year. In an interview with the *Toronto Star* on Saturday, Canadian Trucking Alliance president, David Bradley, said clarification is needed about whether simply dropping off a load south of the border could be considered as a day spent in the U.S. Today's Trucking

Welcome parliamentary oversight is not enough to fix security policy: Editorial
An editorial states, "The lives of Canadians have never been more transparent to the state's security apparatus, yet the security apparatus remains troublingly opaque to the people. That dangerous asymmetry was compounded by the Harper government's overreaching Anti-Terrorism Act, formerly Bill C-51, which introduced vast new powers for spy agencies last year and yet did nothing to make them more accountable. It was reassuring, then, to see the new Liberal government table Bill C-22 last week, an important first step toward accountability. The legislation would finally give to Canada what most of our allies already have: a parliamentary committee that provides democratic oversight of our national security establishment. (…) As welcome as Bill C-22 is, it could be better. **Public Safety Minister Ralph Goodale** said last week that the committee would have ***"the ability to look at any issue, any activity, any operation, any document."*** But that's not quite true. In fact, under the proposal, the prime minister and his cabinet would be allowed to withhold any information or veto any inquiry they deem to be "injurious to national security." This "Mack truck exception," as University of Ottawa law professor Craig Forcese calls it, makes it too easy for the ruling party to cover up politically inconvenient information. (…) Worse still, some national security organizations, such as the Canada Border Services Agency, escape independent scrutiny altogether. Fifteen people have died in CBSA custody since 2000, yet in the absence of any arm's-length oversight Canadians remain completely in the dark about the circumstances of those deaths. The parliamentary committee would be a good start here, but more integrated and robust access to information is needed. (…) The act compromises Canadians' privacy in unprecedented ways, criminalizes the "promoting" of terrorism, gives CSIS the power to perform the sort of dirty tricks it was created to pre-empt, and allows imprisonment of up to five years to prevent crimes that "may be carried out."" Toronto Star

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Chemawawin, Easterville to lift state of emergency after Manitoba forest fires
The state of emergency for Chemawawin Cree Nation and Easterville is expected to be lifted Monday afternoon after a rainy weekend helped combat forest fires near the Manitoba communities. The area about 400 kilometres north of Winnipeg has been under the state of emergency since last week as flames crept as close as 100 metres to homes. CBC News

Heavy rains over weekend cause damage, O'Connor Township declares State of Emergency
The city has so far received about 230 calls reporting flooding and damage as a result of heavy storms on the weekend. About 92 millimetres of rain fell on Thunder Bay over the course of Saturday. A portion of one lane of Fort William Road, north of First Avenue, will be closed while crews repair a washed-out shoulder. The work is taking place today. City crews will continue making other repairs around the city today, as well. Kerri Marshall, the city's general manager of infrastructure and operations, said it's important those who suffered damage due to the storm contact the city. CBC News

Whiteshell flood damage 'devastating,' homeowner says
Grant Fisette's home is in a precarious situation after the weekend downpour in the Whiteshell caused flooding and a landslide on his property. The province recommended people along parts of the Manitoba-Ontario border pack up and temporarily leave the area after torrential rains washed out a few major roads and threatened to do the same to others on Friday night. More heavy rain Saturday night created gaping holes on roads in West Hawk Lake and Falcon Lake, and on Sunday, the province again urged people to exit the area. Fisette's home is on Caddy Lake, about 140 kilometres east of Winnipeg. The lake has

risen so much that by Monday morning, there was 56 centimetres of lake water on the highway, he said. CBC News

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Cinq projets contre la radicalisation des jeunes

Québec mise sur cinq projets de tables rondes, de théâtre et d'actions communautaires pour lutter contre la radicalisation des jeunes menant à la violence. Environ 165 000$ seront injectés sur deux ans pour intervenir notamment auprès des jeunes issus de minorités racisées. En tout, 17 000 jeunes de partout au Québec participeront à ces projets, qui font partie du Plan d'action 2015-2018 pour lutter contre la radicalisation au Québec. Seulement six organismes ont répondu à l'appel de projets, parce que «peu d'organismes ont la capacité de porter des projets aussi complexes», croit la ministre de l'Immigration, de la Diversité et de l'Inclusion Kathleen Weil. «Il n'y a pas un jour qui passe sans qu'on entende parler d'islamisme, de racisme, de terrorisme. Nos animateurs observent une montée de l'intolérance dans nos écoles, particulièrement de l'islamophobie. C'est donc important d'aborder ces thèmes avec les jeunes», croit Marie-France Legault, d'Ensemble pour le respect de la diversité. Cet organisme présentera le projet Escale je prends ma place afin d'aborder ces thématiques sensibles auprès de jeunes de second cycle du secondaire partout au Québec. Journal de Montréal; Montreal Gazette

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Heading South to the United States? Plan Your Return
Travellers should plan to cross the border outside of peak traffic periods if possible to avoid delays. Travellers can also help speed up processing by ensuring that they have proper identification for everyone in their vehicle readily available upon arrival to Canada. Returning Canadians should have receipts for all purchases in hand," states Paul Loo, Acting Regional Director General, CBSA, Northern Ontario Region. Now that summer is officially here, the Canada Border Services Agency (CBSA) is making every effort to effectively manage the expected higher traffic volumes during this peak period. Net News Ledger

Brexit : quel type d'accord entre l'Union européenne et le Royaume-Uni ?
Voilà 43 ans que le Royaume-Uni et l'Union européenne sont engagés dans un mariage tumultueux. Lors du référendum de jeudi dernier, les Britanniques ont choisi le divorce, votant pour 51.9% en faveur du "Leave". (...) Un vaste accord commercial a été signé entre le Canada et l'Union européenne en 2009, le CETA (Accord économique et commercial global). Cet accord de libre-échange prévoit la levée des droits de douane sur de nombreux produits à l'importation et à l'exportation entre le Canada et l'Union européenne. Ce scénario permettrait au Royaume-Uni de négocier des accords bilatéraux avec d'autres pays comme les pays émergents et les Etats-Unis. Cet accord de libre-échange ne garantit cependant pas la levée des barrières douanières sur les services financiers. Si le Royaume-Uni choisit de se lancer dans cet accord de libre-échange, il devra par ailleurs négocier pendant plusieurs années : alors que les négociations durent depuis sept ans entre le Canada et l'UE, l'accord n'a pas encore été ratifié. France Bleu

Les producteurs de bois d'oeuvre du Québec réclament un coussin de 5 milliards $
Les producteurs de bois du Québec suggèrent à Ottawa de durcir le ton dans ses négociations avec les Américains. Ils sollicitent également un coussin financier pouvant atteindre jusqu'à 5 milliards de dollars afin de protéger les scieries et les emplois canadiens en cas de conflit prolongé. Ces scénarios ont été discutés lors d'une rencontre avec la ministre canadienne du Commerce international, Chrystia Freeland, à Montréal en début juin. Les négociateurs canadiens étaient d'ailleurs à Washington la semaine dernière. La question du bois d'oeuvre reviendra sur le tapis cette semaine, alors que le premier ministre Justin Trudeau accueille à Ottawa ses homologues américain et mexicain, Barack Obama et Enrique Peña Nieto. Les producteurs québécois, et certains de leurs collègues ontariens, croient qu'au lieu de conclure une entente avec les États-Unis, le gouvernement canadien devrait plutôt prendre la voie des tribunaux, devant l'Organisation mondiale du commerce (OMC). « Ce serait la première fois que le Canada s'en remettrait complètement à l'OMC et attendrait la décision finale, sans conclure d'entente bilatérale avec les États-Unis », avance le pdg du Conseil de l'industrie forestière du Québec, André Tremblay. Selon lui, une entente négociée « limite nécessairement l'exportation du bois d'oeuvre canadien vers les États-Unis », soit par des quotas ou des barrières tarifaires (de 15 à 25 %), « qui limite l'expansion de l'industrie ». Tandis que si le Canada remet le dossier entre les mains de l'OMC, André Tremblay espère « gagner un plein accès au marché américain », soit une situation complète de libre-échange. Radio-Canada

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Analyst: Brexit Cybersecurity Ramifications Could be Significant
After 43 years of inclusion, the UK has voted to leave the European Union in the historically unprecedented "Brexit" referendum vote. Aside from causing uncertainty in the world's financial markets and across the political landscape, the result has implications for cybersecurity too. While some cybersecurity pros say that Brexit will have little ill effect on the space, others aren't so sure. For one, Michela Menting, research director for ABI Research, noted that the UK will need to review its role Europol and the European Cybercrime Centre (EC3), which is the focal point in the EU's fight against cybercrime. "Organized online criminal activities are undeniably best tackled from a cooperative, supra-national perspective, and the UK's isolation that may result from Brexit would be an unwelcome development in the fight against cybercrime," she said. "Further to this, new cybersecurity information and

asset sharing structures will need to be put in place between the EU and the UK." Infosecurity Magazine (2016-06-24); SC Magazine; ComputerWeekly

Should the Careless Be Punished for Getting Hacked?
An opinion piece states "Nearly everyone with Internet access is harmed, at least indirectly, by digital criminals. Josephine Wolff, a professor at the Rochester Institute of Technology, believes cybersecurity policy would benefit from a debate about if and when it might be appropriate to punish careless computer users for their role in enabling those criminals. She writes: The question in my field (cybersecurity) that I think would most benefit from more vigorous, widespread debate is what degree of responsibility and liability individual Internet users should have for participating, unknowingly, in the perpetration of cybercrimes and data breaches. The (generally well-meaning) people whose computers are infected and become part of the large bots that spew phishing emails and ransomware, or who click on the links and attachments in those phishing emails and carelessly surrender their login credentials or the contents of their hard drives play an enormous and devastating role in many (perhaps most) of the major cybersecurity incidents that occur today." The Atlantic

LAW ENFORCEMENT / APPLICATION DE LA LOI

Complaints into RCMP conduct reveals dangers of being Mountie in the North
The dangers of being an RCMP officer in the North are being revealed in an unlikely place: public complaints into the conduct of Mounties. Complaints made in the last five years to the Commission for Public Complaints Against the RCMP about N.W.T. officers were obtained by the CBC through an access to information request. The Commission is an independent oversight body created to investigate public complaints about the RCMP's conduct. The majority of the complaints filed were for alleged "excessive use of force" by officers, which were most often during an arrest. However, investigations into many of those incidents revealed that RCMP officers had been physically assaulted by the complainants. In an excessive force complaint investigation in 2014, an intoxicated person punched an officer in the side of the head while the officer was trying to remove the person's shoes prior to putting them in a cell. While the officer was trying to handcuff the person, the individual grabbed the male officer's testicles, squeezed and twisted them. The officer then punched the person to get them to release his testicles. The individual then bit the officer on the leg. CBC News

Body recovered in Exploits River by search and rescue crew
A body has been recovered from the Exploits River, after police were called about an object in the water Monday morning. Roger Goobie of Exploits Search and Rescue said his group was called to help the RCMP, after police were notified of an object in the river around 5:50 a.m. The body was recovered from an area of the river adjacent to the weigh scales on the Trans-Canada Highway, on the eastern boundary of Grand Falls-Windsor. No further details have been released as of yet. CBC News

4 collisions en 5 minutes pour un homme qui est accusé de tentative de meurtre
Un homme de 21 ans de Bedford, en Nouvelle-Écosse, est accusé de tentative de meurtre après avoir heurté volontairement quatre véhicules en cinq minutes dans la région de South Harbour, au Cap-Breton. Vers 15 h dimanche, la GRC a reçu plusieurs appels pour signaler quatre collisions sur un tronçon de un kilomètre du chemin White Point. « C'est un événement inquiétant, raconte Andrew Joyce de la GRC. Il semble qu'il ait foncé volontairement sur un véhicule sport utilitaire et deux motos. Il a ensuite raté de peu un autre véhicule avant de frapper un garde-fou. » Heureusement, dit le policier, personne n'a été blessé sérieusement. L'accusé conduisait une fourgonnette Honda Odyssey lorsqu'il a d'abord heurté le véhicule sport utilitaire d'une femme de 49 ans qui avait un enfant de 5 ans à bord. La fourgonnette a fui les lieux de l'accident et a ensuite frappé un motocycliste et son passager. ICI Radio Canada

B.C. high school forced to close, postpone graduation amid threats
A high school in southeastern B.C. remains closed Monday as officials investigate a threat. Posts on the website of Mount Sentinel Secondary in South Slocan, about 25 kilometres west of Nelson, confirm a threat to the safety of students and staff was received last week. Officials decided to shut down the school and also postponed graduation ceremonies set for the weekend. An update posted Sunday and

attributed to Mount Sentinel vice-principal Shellie Maloff says the RCMP, Nelson Police, the Ministry of Children and Family Development and the school district's Violent Threat Assessment Team are investigating. The post urges parents and students to "continue to be vigilant" if attending any grad activities, parties or events where students might congregate. Canadian Press (CTV News)

Crash involving BMW and RCMP vehicle shuts down Hwy. 1
The Trans-Canada Highway was closed westbound for several hours overnight after a serious collision involving an RCMP vehicle and BMW sedan. Video taken at the scene shows a black SUV with severe front-end damage and a white BMW sedan with damage as well. Abbotsford Police say a Chilliwack RCMP vehicle was involved in the collision. Westbound lanes of Highway 1 near Sumas Road in Abbotsford were shut down as police investigated. Police have not confirmed whether a pursuit was involved in the accident, if anyone was injured, or if any arrests were made. CTV News

Opération Clemenza: les accusés sont tous libérés
Les huit individus arrêtés dans l'opération Clemenza de la GRC le 11 mai dernier, et qui étaient détenus depuis, ont tous été libérés lundi matin par la juge Linda Despots de la Cour du Québec en attendant la suite des procédures. Marco Pizzi, Erasmo Crivello, Frank Iaconetti, Riccardo Preterotti, Antonio Ciavaglia, Hansley Lee Joseph, Frank Albanese et Carmelo Marsala sont accusés de complot, trafic de cocaïne, importation de cocaïne et gangstérisme. Un interdit de publication nous empêche de dévoiler les détails de la preuve et les raisons données par la juge pour les libérer. La Presse

Un Américain arrêté après avoir envoyé des photos de lui nu à une policière
Une policière de la GRC en Nouvelle-Écosse a contribué à l'arrestation d'un homme du Missouri, aux États-Unis, qui sera accusé d'inconduite sexuelle avec un enfant âgé de moins de 15 ans. L'homme, qui vit à St. Peters, une localité à 2900 km de la Nouvelle-Écosse, fait face à huit accusations d'avoir envoyé des photos et des vidéos de lui nu à une policière qui se faisait passer pour une enfant de 12 ans. La policière en question est membre du Groupe provincial de lutte contre l'exploitation des enfants dans Internet de la GRC. Son identité est protégée en raison de ses fonctions au sein de cette unité. Elle a néanmoins accepté de parler de son travail au réseau CBC et de ce cas en particulier. « Séduisez-moi » La policière a donné une présentation sur le travail de son unité. Afin de démontrer l'étendue du problème devant un groupe, elle a utilisé son téléphone intelligent pour se brancher à un populaire site de clavardage auprès des enfants. Elle s'est identifiée en tant que jeune fille de 12 ans. « J'ai publié "ce site est bizarre LOL. Mais je m'embête. Séduisez-moi" », a raconté la policière à CBC. ICI Radio Canada

Broadcast media / Médias télédiffusés :

An incident involving an R.C.M.P. cruiser and another car forced the closure of westbound highway 1 lanes in Abbottsford for several hours overnight. Video from the scene shows a badly dented suv and a white BMW with damage as well. Abbottsford police say it was a Chilliwack R.C.M.P. vehicle that was involved in the incident. So far, police have not confirming any details or whether or not there was a pursuit. It's not clear if anyone was hurt or if any arrests were made. (CTV Vancouver, 8:30)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Remise en liberté de Dennis Oland: la Cour suprême se prononcera jeudi
La Cour suprême du Canada doit rendre sa décision jeudi quant à la remise en liberté de Dennis Oland qui en appelle du verdict de meurtre non prémédité prononcé à son endroit. Les avocats de Dennis Oland avaient demandé au plus haut tribunal une décision rapide sur sa demande de remise en liberté après qu'il eut été trouvé coupable du meurtre non prémédité de son père, l'homme d'affaires Richard Oland. La Cour d'appel du Nouveau-Brunswick avait rejeté cette demande en février dernier. Les tribunaux néo-brunswickois n'ont jamais accordé de libération conditionnelle à un accusé trouvé coupable de meurtre. Dans leur demande à la Cour suprême, les avocats d'Oland reprochent à l'instance précédente d'avoir imposé des standards élevés qui sont en porte-à-faux avec des causes similaires ailleurs au Canada. L'ex-conseiller financier avait écopé d'une sentence d'emprisonnement à perpétuité sans possibilité de

libération avant 10 ans, plus tôt cette année, après que son père eut été trouvé mort dans ses bureaux de Saint-Jean en juillet 2011. Presse canadienne (La Presse, Droit-Inc); Radio-Canada; Canadian Press (Toronto Star, Global News); CBC News

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NIL

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

National Aboriginal Day marks 20 years
Elders and outstanding community members were honoured, and lives lost remembered as National Aboriginal Day celebrations kicked off in Muskoseepi Park on Sunday. (…) A unique aspect to this year's celebrations was the fashion show featuring clothing designed by Tishna Marlowe. Marlowe said the show was a chance to use her platform as a designer to bring awareness to all the missing and murdered aboriginal women. "I have family and friends who are missing and/or murdered indigenous women," she said. After walking out in the clothes individually, the models did a second loop and had a moment of silence to honour all those lives lost. "Residential schools played a part in (the women's) upbringing and their lifestyle," she said. "The red dresses represent all the lost kids, babies and young women who didn't make it back from the residential schools. There's about 100 years of missing and murdered women. It goes back farther than people realize and we're only now starting to understand it... The numbers are so large it can't be ignored anymore. We as aboriginal culture and society have to make it stop. We can't completely end it but we can do something." Daily Herald Tribune

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Debate on marijuana shops operating in Toronto deferred until October
The debate around Toronto's pot shops will have to wait a few more months as the city has deferred official discussions about the matter until October. In a letter sent to the Licensing and Standards Committee last month, Mayor John Tory asked the executive director to work with the chief medical officer of health and police to review a possible regulatory framework for marijuana dispensaries. The group was asked to report back on their findings at today's meeting and but the report now won't be received until Oct. 25. Coun. Jim Karygiannis – who is on the committee -- was joined by Michael Price McLellan of the Toronto Dispensaries Coalition and medical marijuana patient and advocate Jesse Beardsworth Monday. They told reporters prior to the meeting at city hall that the crackdown on marijuana dispensaries was a "knee-jerk reaction to a couple hundred emails." CTV News

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

China reportedly tightens visa rules for Hong-Kong born Canadians
China appears to have quietly tightened its visa requirements for Canadian citizens born in Hong Kong who want to visit the mainland, requiring them to obtain two-year travel permits rather than the usual 10-year visitor visa. Ming Pao Daily, a Vancouver-based Chinese newspaper, published a report on June 19

that says as of June 2, Canadian nationals born in Hong Kong can no longer obtain a 10-year tourist visa and must instead seek a two-year travel permit. But there is no information announcing the change on the Chinese embassy's visa requirements web page, last updated on December 1, 2015, or on the Canadian government's travel advice and advisory page for China, last updated on June 1, 2016.Details are slim but the Canadian government says it has received a number of questions about the apparent change and is trying to gather more information from Chinese authorities. However, spokespersons from Global Affairs Canada declined to confirm whether they had received that clarification and would not confirm the details of the changes.(…) One Toronto-based visa services company said it has heard of the policy change and provided details on what they understand the changes to include, which matched and expanded on the information in Ming Pao Daily's initial report. iPolitics

INTERNATIONAL

EgyptAir: Paris ouvre une enquête pour homicides involontaires
Les autorités françaises ont ouvert une enquête pour homicides involontaires relativement à l'écrasement d'un avion du transporteur aérien EgyptAir en mai, tout en déclarant que rien ne permet pour l'instant de croire à un attentat terroriste. La porte-parole du bureau du procureur de Paris, Agnès Thibault Lecuivre, a précisé qu'il s'agit d'une enquête sur un accident, et non d'une enquête pour terrorisme. Elle a dit que les autorités ne favorisent « pas du tout » l'hypothèse d'un geste délibéré, mais le statut de l'enquête pourrait changer en fonction des preuves recueillies. Les enquêteurs ont décidé d'entamer l'enquête sur la base des éléments retrouvés jusqu'à présent et sans attendre l'analyse du contenu des deux boîtes noires, a-t-elle ajouté. La Presse; Toronto Star

Russia passes 'Big Brother' anti-terror laws
Russia's parliament has passed harsh anti-terrorism measures that human rights campaigners including the NSA whistleblower Edward Snowden say will roll back personal freedoms and privacy. The lower house of parliament voted 325 to 1 on Friday to adopt the "Yarovaya law", a package of amendments authored by the ruling United Russia party member Irina Yarovaya, who is known for previous legislative crackdowns on protesters and non-governmental organisations. Snowden, who has lived in Russia since receiving asylum in 2013, tweeted on Saturday that the "Big Brother law" was an "unworkable, unjustifiable violation of rights" that would "take money and liberty from every Russian without improving safety". Guardian UK (2016-06-26)

858 killed: Not a day in April passed without a terror attack
Habib Ullah chugged along a dusty road in rural Pakistan on his battered motorcycle, his wife, infant son and 7-year-old daughter hanging on — a family of farm laborers on their way to work the fields. A 60-year-old father of seven, Ullah was steering through the barren, mountainous district of Khuzdar, in Pakistan's poorest province. The family never reached the fields. One of the motorcycle's wheels struck a mine on Loop Leak Road. (…) It was April 12, 2016 (…) One day, six countries, 19 deaths. And it wasn't the deadliest day in April. That was a week later, on April 19, when terrorist attacks in five countries killed 71 people and wounded 391 others. To assess the scope and nature of terrorism in 2016, the Los Angeles Times sought to chart the worldwide toll of deaths and injuries in a single month (…) They confirmed 858 deaths in 27 countries. An additional 1,385 were injured (…)The number of terrorist attacks around the world actually decreased by 13% last year, according to the U.S. State Department, the biggest decline in more than a decade. But the reality is that terrorist attacks over the last 15 years have become more deadly, more indiscriminate and more wide-ranging. During April, not one day escaped bloodshed committed by terrorists. Los Angeles Times (2016-06-24)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

ON Drug Strategies
International Day Against Drug Abuse and Illicit Trafficking : Ministers @Puglaas @janephilpott @RalphGoodale http://news.gc.ca/web/article-en.do;jsessionid=ff60fea91d993e644abde519ca7ba06f7d1bd765a5a753276ea37d12647dad7f.e34Rc3iMbx8Oai0Tbx0SaxuPbxj0?mthd=index&crtr.page=1&nid=1090529 …

Lawrence MacAulay
Lots to discuss w/ my good friend @RalphGoodale. Just a few years of combined parliamentary experience in the room…

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

PreparedBC
Prevent wildfires. Follow #EmergencyMommy's campfire safety tips: http://ow.ly/1ioh301C5CB #BCWildfire

Oplopanax
#SAR Incidents in #BritishColumbia by month from 2003 to 2010

IAEMCdnCouncil
200-year loss scenario from flood in Canada could produce insured losses of $5.7 billion: Swiss Re

Public Safety Canada
#PTSD impacts public safety officers, families and friends, organizations, and communities. Don't suffer alone #PTSDAwarenessDay

Sécurité publique
#ESPT affecte les agents de sécurité publique, familles/amis, organisations et communautés. Ne souffrez pas seul #JournéesensibilisationESPT

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Stewart Bell
That makes 10 Canadians killed by terrorists in 2016: Burkina Faso (6), Jakarta (1), Philippines (2), Somalia (1).

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Google News CA
Ambassador Bridge still paying for tainted gas repairs

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NatlCyberSecAlliance
Register for a discussion about "The difference between security & privacy programs" feat. @PrivacyRef : https://www.eventbrite.com/e/are-you-cyber-prepared-registration-25935206902 … #CyberAware

LAW ENFORCEMENT / APPLICATION DE LA LOI

CBC North
Complaints into RCMP conduct reveal dangers of being Mountie in the North

Yellowknife NT
Complaints into RCMP conduct reveals dangers of being Mountie in the North
http://www.rightrelevance.com/search/articles/hero?article=b43826bb6ad1ccb9fa4b080a84e709f56d8955ff&query=n

orthwest%20territories&taccount=yellowknifentrr ...

VOCM News
RCMP Cruiser Collides with Truck on TCH http://vocm.com/news/rcmp-cruiser-collides-with-truck-on-tch/ ... #nltraffic

CTV Vancouver
BMW and RCMP vehicle smashed in crash on Trans-Canada Hwy. in Abbotsford

BC Government News
43 arrested as a result of investigations by @cfseubc. Learn more: http://ow.ly/8nlM301C0xh @bcRCMP #StopGunsGangsBC

Global BC
BASE jumper dies in B.C. after parachute apparently fails to deploy: RCMP

Embassy of Canada US
On June 29 Canada will host its continental partners in Ottawa for #NALS2016 http://bit.ly/1UzqKF8 HT @CanadianPM

Bruce A. Heyman
#USCanada flags for @CanadianPM's March visit to #WDC. Excited to see our flags together for #ObamaCAN & #NALS2016!

RCMP National Div
ICYMI: #NALS2016 Significant disruptions expected June 29. More info: @ottawacity, @OttawaPolice, #OttTraffic and #OttCircule

Ville d'Ottawa
Sommet des leaders n.-a. ˆ #Ottville le 29 juin. Fermetures de rue et retards #Ottcircule au c.-v. DŽtails http://ow.ly/sCZx301GbYk #SLNA2016 http://aka.ms/Twitter2BingTranslator

EastDistrictTraffic
Getting ready/training for the NALS visit to Ottawa . @OPSWestTraffic @TorontoPolice

Garda World
@GardaWorld in charge of security for the North American Leaders Summit meeting in Ottawa @JustinTrudeau #NALS

iPolitics
Presidents Obama and Peña Nieto are coming to town! Visit ottawa.ca for more info. on road closures. #NALS #Ottawa

Ottawa Police
ICYMI - Road closures/ Expect delays June 29 during #NALS2016 in downtown #Ottawa:http://ow.ly/aXXo301BzWP

OTHER / AUTRES

Canada in Mexico
#LIVE Watch the official welcoming ceremony for President @EPN via @PresidenciaMX http://ow.ly/LzmZ301FTZN

David Johnson
At the #Citadelle of #Quebec, I will officially welcome @EPN, President of #Mexico, to Canada. http://bit.ly/28QgBSH

Foreign Policy CAN
@MinCanadaFA greets Mexican Pres @EPN upon his arrival in Quebec City for his state visit & ahead of #NALS meeting

Canadian PM
Canada, the US and Mexico are strong partners in a wide range of areas that benefit our three countries. #NALS2016

Amnesty Canada

RT @CPAC_TV Live 1030ET: @AmnestyNow speaks about human rights issues in North America ahead of #NALS2016 http://spr.ly/6014BQN4j #cdnpoli

Reuters Top News
Adios, Three Amigos: Obama heads to last summit with Canada, Mexico: http://reut.rs/28Yk1mf

INTERNATIONAL

Ray Boisvert ISECIS
Preparing to crush growing internal / popular unrest against Putin: Russia passes 'Big Brother' anti-terror laws

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

Today's News / Actualités
June 28, 2016 / le 28 juin 2016
14:00 –20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

One million Canadians have donated to Red Cross campaign for Fort McMurray fire victims
More than one million Canadians have now donated to the massive Red Cross campaign to help Fort McMurray residents forced from their homes almost two months ago. The campaign is the largest and most successful in the organization's post-war history, said Conrad Sauvé, president and CEO of the

Canadian Red Cross. "This has been a real Canadian moment," Sauvé said Tuesday. "A tremendous Canadian moment. I think we need to recognize that, and I think everybody was touched throughout the country by seeing those images of Canadians fleeing this situation." The campaign has raised more than $136 million so far, and that total does not include matching funds from provincial and federal governments, Sauvé said. CBC News

Here's what life is like after the massive fire in Canada's Fort McMurray
More than a dozen people line up in the rain outside the only food bank in Fort McMurray, Alberta. Even as the downpour gets stronger, they wait in place holding green laminated numbered cards — most of them using this service for the very first time. It's Monday afternoon and since the food bank wasn't open over the weekend, this place is especially hectic as one team of workers take the green cards, and another team hurries in and out of the building with boxes of food to load into clients' parked cars. Over the last two weeks, since it reopened, the bank has fed some 3,000 people, displaced and put out by the raging wildfires that hit the town in May, prompting a state of emergency and a mandatory evacuation of the city — the longest in Canadian history — and wiped out entire neighborhoods. While climate change has been listed a factor for extremely dry weather and unruly forest fires in western Canada, Alberta wildfire investigators have said the Fort McMurray fires, also known as "The Beast," were likely caused by "human activity" and police have put a call out to people asking for any information. The police say they are treating the investigation as a criminal matter. VICE News

Crews battling three wildfires in wooded areas throughout Nova Scotia
The Nova Scotia government says crews are battling several wildfires in wooded areas throughout the province. The province says the largest is burning in Fenwick, just south of Amherst, and is approximately 12 hectares in size. Spokesman Brian Taylor says that fire has been contained and more than 50 crew members are working to extinguish the blaze. Taylor says another fire, one hectare in size, is burning in Lunenburg County, but it has been contained and there are no concerns. Canadian Press (St. John's Telegram, Charlottetown Guardian)

Forest fire burning outside community of Pollard's Point
Water bombers have been dispatched to a forest fire outside the community of Pollard's Point in White Bay. The province's fire duty officer, Basil English, said the blaze was reported around 3:30 p.m. and is burning about 15 kilometres outside of the community. CBC News

Kenora declares state of emergency
The City of Kenora declared a state of emergency on Monday following heavy rainfall and flooding that hit the northwest over the weekend. It's the second municipality in the region to do so after many parts of the region saw over 100 millimetres of rain. O'Connor Township, just outside of Thunder Bay had already declared a state of emergency on Sunday. A press release issued by the City of Kenora said the over 109 millimetres that fell on the city over a two day period led to more than 20 roads experiencing moderate to extensive damage. CBC News

Sandbag machine arrives in Whiteshell as flooding continues
People in the Whiteshell are watching the floodwaters continue to rise and have been told a sandbag-making machine is on its way. Grant Fisette, whose property borders Caddy Lake, said the lake level went up by about 10 centimeters overnight. Much of the hillside next to his home has already slumped away from heavy rains on the weekend that washed out roads. "I boated around last night and there's so much water damage and sheds on their sides around the lake and boat houses that are pretty much totally submerged," he said. CBC News

Calgary group urges flood-affected homeowners to appeal property tax assessments
A small group of Calgary homeowners impacted by the 2013 floods is encouraging others to appeal their property tax assessments, saying they shouldn't have to pay more in taxes until "big" flood mitigation measures are taken. The group, called "Still Paying for the 2013 Flood," is headed up by local political strategist Stephen Carter. He says homeowners in Calgary haven't yet seen the type of mitigation needed to justify an increase in property taxes. A dry dam for the Elbow River is planned for the Springbank area, though it is now undergoing a federal environmental assessment. CBC News

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Somali cabinet minister killed by car bomb the latest in growing number of Canadian terror deaths
Despite the risks, Buri Mohamed Hamza returned to Somalia to serve the country's struggling federal government, but on the weekend Al-Shabaab extremists struck his hotel with a car bomb, killing the former Toronto resident. The zoologist was the 10th Canadian to be killed abroad by terrorists in 2016, the worst year for such deaths since the Sept. 11, 2001 attacks, according to a terrorism database. Nine other Canadians have also died in Burkina Faso, the Philippines and Indonesia. "Overseas exposure of Canadians to terrorism seems to be up, markedly so," said terrorism researcher James O. Ellis. "The widespread travel and work of Canadians has exposed them to greater danger this year than we've seen in many recent previous years (...)" Ellis is a research affiliate at the Canadian Network for Research on Terrorism, Security and Society (TSAS), which maintains a database of known terrorism incidents. Excluding attacks on Canadian military personnel in Afghanistan, the database points to 2016 as the worst in 15 years. Canadians have not necessarily been targeted more than in previous years, but they have been falling prey to overseas extremist groups intent on killing Westerners, said Alan Bell, president of Toronto-based security firm Global Risk International Inc. National Post

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Two men denied entry into Canada at Pembina sparks underage sex investigation
Fargo Police are in the midst of an investigation into Corruption of a Minor and Luring a Minor By Computer after allegations surfaced of two men having sex with a 14-year-old Kennedy, MN girl. It involves U.S. Customs and Border Protection, the Department of Homeland Security and Canadian authorities. Valley News Live

Drugs, Weapons Seized At Ambassador Bridge
May was a busy month for customs officers at the Ambassador Bridge. On May 2nd, two non-residents made a wrong turn onto the Ambassador Bridge. Upon exiting the vehicle in secondary inspection, both occupants of the vehicle admitted that there were drugs in the vehicle. Both were placed under arrest and personal searches were conducted. An examination of the vehicle with detector dog assistance resulted in the seizure of 413.9 grams of marijuana wax butter, 916 grams of marijuana cookies, 148.9 grams of marijuana, 220 tabs of LSD, 1 tab of Xanax, and US$999. All of the drugs were seized, and a vehicle penalty assessment of CAN$1,200 was issued and paid by the travellers, who returned to the United States. Windsorite

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Things a Criminal Could Do With 9 Million Hacked Health Care Records
What can a fraudster do with medical records stolen from several health care organisations? Last weekend, a hacker advertised over 600,000 alleged records for sale on the dark web. Then on Monday, the same hacker listed around 9 million supposed health care insurance details. Those dumps included, among a few other tidbits, Social Security numbers, dates of birth, physical addresses, and victim's full names. Some also include details on health insurance, such as policy numbers, but their medical history isn't being sold, it appears. Motherboard

Mozilla made a game to teach you the basics of encryption
Sure, people will tell you that encryption is important to maintaining your online privacy, but how do you wrap your head around the concept? Mozilla wants to help. It's introducing a web-based game, Codemoji, that illustrates how ciphers work through emoji. Type in a phrase and Codemoji will both shift the letters and replace them with emoji. The challenge, as you might guess, comes when you get your friends to guess the meaning without turning to the Codemoji website. Engadget

LAW ENFORCEMENT / APPLICATION DE LA LOI

Explosion destroys home in Mississauga, at least 1 person seriously injured
Emergency crews are investigating after a massive explosion in Mississauga destroyed one home and left several others damaged Tuesday afternoon, with at least one person seriously injured. Peel Regional police, firefighters and paramedics responded to the call of an explosion at 4:20 p.m. on Hickory Drive near Willowbank Trail, in the Dixie Road and Rathburn Road East area. Heavy smoke was visible in the area, with debris scattered across the neighbourhood. At least four homes were damaged in the explosion and a small fire was also seen burning at the scene. Global News; National Post (Ottawa Citizen); CTV News; Canadian Press (Global News, Metro News); Huffington Post; ABC News; Torstar (Hamilton Spectator)

Man wanted by RCMP in Alberta arrested in northwest Ontario: OPP
Ontario Provincial Police say a 32-year-old man wanted by the RCMP in Alberta has been arrested. They say they were told by the RCMP that the man and a female companion were possibly in the Dryden, Ont., area. OPP say the man and woman were located on Highway 17 in Southworth Township, Ont., on Monday, and arrested the man on a charge of failing to comply with a recognizance. Police say Jason Masse was wanted by RCMP in Provost, Alta., on charges including assault with a weapon, pointing a firearm, forcible confinement, uttering threats, and possession of a weapon for a dangerous purpose. Canadian Press (610 CKTB, Kelowna Daily Courier); CBC News

RCMP support Pride in Steinbach, city council refuses to endorse
The first Steinbach Pride March has faced a number of challenges and concerns along the way to the July 9 date, now the city council is refusing to endorse the event. City council announced their decision in a media release Tuesday, “Council has not officially endorsed the July 9 Pride March. Steinbach residents will decide themselves whether they wish to attend this event.” The city announcement comes after Manitoba RCMP supported the march on Monday. D Division Commanding Officer Scott Kolody said he would attend the Pride March and Manitoba RCMP would “provide all required resources to ensure participants can walk in Steinbach knowing they are safe, secure and have the RCMP by their side.” Global News

Memorial in St. Albert will honour slain RCMP Const. David Wynn
The life and legacy of fallen St. Albert RCMP Const. David Wynn will be honoured with a special memorial and an endowment fund. The design for the memorial was unveiled near Lacombe Park Lake in St. Albert Tuesday. Benches will surround a plaque on a large rock next to the Sturgeon River. The memorial in the park is intended as a place for reflection. Mayor Nolan Crouse hopes it will be completed by October. Global News; Kelowna Daily Courier; Canadian Press (Chronicle-Herald, Metro News)

RCMP search for missing 15-year-old Gillian Mikayla Bruce
RCMP are asking for help to find a 15-year-old girl who ran away during a family visit to Winnipeg. RCMP were called after Gillian Mikayla Bruce from the rural municipality of Tache didn't show up to meet her ride back home. The teenager ran away during a family visit to Winnipeg on June 18, RCMP said. "While our investigation so far has confirmed that Gillian left on her own accord and likely does not want to be located, we are doing everything we can to confirm her well-being," RCMP Sgt. Bert Paquet said in a news release. CBC News; myToba

Sylvan Lake RCMP investigate attempted abduction of 13-year-old girl
Sylvan Lake RCMP are investigating after two men allegedly attempted to abduct a 13-year-old girl. Police said the girl was walking with friends near the Sylvan Lake library at around 11 p.m. Monday when she and her friends separated. Shortly after, the teen noticed a vehicle which was operating “in a suspicious manner,” so she hid in a nearby bush. Global News

RCMP investigating after shots fired into a home in Surrey
Police are investigating a targeted incident involving shots being fired into a home in Surrey on Tuesday morning. When Surrey RCMP arrived at the home in the 10100-block of 127 Street, they found bullet

holes in the front door and window. Police also found the family dog dead inside and it's believed the dog died of a gunshot wound. One person was in the home at the time of the incident but was not injured. Global News; Vancouver Province

RCMP rule sudden death as a homicide
An autopsy has determined that a sudden death in Onoway on June 26thwas a homicide, RCMP said. Glen Allen Abbott, 37, was found dead in his residence by RCMP officers. The RCMP Major Crimes Unit and the Stony Plain General Investigation are now handling this homicide investigation, and they are seeking the public's assistance to determine the victim's movements in the days leading up to his death. CTV News; Edmonton Journal; CBC News

Nanaimo RCMP seize weapons and drugs after searching 2 homes
RCMP in Nanaimo have seized a number of weapons along with quantities of various drugs after raiding two homes. Police were called to a home in the 500 block of Dundas Street on Monday last week after a report of a man with a rifle. They were then called to a home in the 400 block of Nicol Street three days later. Officers say there had been dozens of previous complaints about both locations and the homes had been the focus of the Street Crimes and Drug Unit for some time. CBC News

Property crime and fraud up: RCMP annual report
Property crime and reports of fraud have increased, according to an annual report from the New Brunswick RCMP. The report, RCMP in New Brunswick Annual Report 2015 released Monday says property crime rose by 15.4 per cent. In 2014, there were 16,880 reports of property crime, which includes arson, break and enter, fraud, possession of property obtained by crime, theft $5,000 and under and theft $5,000 and over and theft of motor vehicle. A year later, the number of reports grew by 2,610 to 19,490. But the most startling statistic in the report was that showing a 50 per cent increase in reports of fraud. "This is a significant increase, and one the RCMP takes very seriously," the reports states. CBC News

Firearms like AR-15 used in Orlando shooting tougher to get on P.E.I.
Weapons like the AR-15, which was used in the Orlando shooting earlier this month, are more difficult to obtain in Canada than in the U.S., according to P.E.I.'s director of public safety. Following the shooting, U.S. media coverage showed just how easy it was to obtain an AR-15 semi-automatic rifle in less than 10 minutes. "I think the gun culture in Canada is much different than the gun culture in the U.S. from what we see in media and what's reported," said Aaron Campbell. "The interest in the safety of the public is something that is well-considered under the federal Firearms Act to ensure that communities are safe." There are 1,297 restricted firearm licences on P.E.I. Weapons in the restricted category include handguns or rifles with shorter barrels. Non-restricted weapons, of which 4,608 are licenced on P.E.I., include shotguns and hunting rifles. CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Laval inmate, serving eight years, dies in hospital
An inmate of the Federal Training Centre, a multi-security level penitentiary in Laval, has died. Robert Harvey, 57-years-old, was serving an eight-year-sentence for several offences including robbery as well as breaking and entering. He had been serving since July 6, 2011. Harvey passed at the hospital of Archambault Institution in Sainte-Anne-des-Plaines. According to a report issued by the Correctional Service Canada, the police and coroner have been notified, and the circumstances of the incident will be reviewed. The inmate's next of kin have also been given notice of his death. Montreal Gazette

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Deadly W-18 drug found in Vancouver say police

The deadly drug W-18 has made its first reported appearance in Vancouver, according to police. Police found the synthetic opioid in pills seized from two men who were arrested in a break-and-enter incident in Vancouver's West End on April 8th. Officers initially thought one of the pills may have been a counterfeit oxycontin pill and sent it to Health Canada for analysis. Those results came back last Friday and revealed the presence of W-18 in those pills. Experts say W-18 is many times more lethal than fentanyl. Metro News; Global News

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Provinces studying terms of reference for inquiry on missing, murdered women
Prime Minister Justin Trudeau was the one who promised a national inquiry into missing and murdered indigenous women, but the provinces still need to sign off on the details. The recommendations that came out the Liberal government's consultations earlier this year were clear: the upcoming national inquiry should have the authority to make recommendations within provincial and territorial jurisdictions as part of a larger attempt to tackle what the inquiry will determine are the root causes of the issue. That authority does not come automatically, however, which is why officials at Indigenous and Northern Affairs Canada are having some back-and-forth discussions with the provinces and territories over the terms of reference, which sources said the federal government proposed in early June. Canadian Press (Winnipeg Free Press); CBC News

Families of 34 missing or dead Indigenous women demand 'proper' investigations
CBC News is investigating the deaths or disappearances of dozens of Indigenous women — all cases where the police said there is no evidence of foul play. But families say their loved ones may have been murdered and that the police investigations were riddled with problems. The Current speaks to three CBC reporters: Connie Walker, Geoff Leo and Angela Sterritt, to find out what their investigations have turned up so far. CBC News - The Current - Transcript

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

NIL

NORTH AMERICAN LEADERS SUMMIT / SOMMET DES LEADERS NORD-AMERICAINS

Operations for LRT tunnel secret for VIP visits to Ottawa
The city won't say if it will ever have to close the Confederation Line LRT tunnel during visits by a U.S. president or other VIPs after the $2.1-billion rail system opens in 2018. A city spokeswoman chalked it up to "security reasons" Tuesday after consulting with the Ottawa Police Service. Part of the 2.5-kilometre tunnel is under Queen Street, just a couple of blocks from Parliament Hill.] On Wednesday the city is closing downtown streets north of Albert Street as a security precaution while U.S. President Barack Obama meets with Prime Minister Justin Trudeau and Mexican President Enrique Pena Nieto. Obama will be addressing Parliament. OC Transpo is detouring a few bus routes away from the street closures in the core. Stephanie Carvin, an assistant professor of international affairs at Carleton University and a former national security analyst, said the city will need to consider how it will operate LRT during a visit by a VIP the stature of a U.S. president. "We might see an LRT shutdown during future visits. I wouldn't rule that out at all," Carvin said, noting the city will need to balance the importance of running the transit system with any security threats identified by law enforcement agencies. Ottawa Citizen

Last chance to wave goodbye to U.S. President Barack Obama in Ottawa
If you're hoping to catch a glimpse of outgoing U.S. President Barack Obama at the North American Leaders' Summit tomorrow in Ottawa, your best bet is late in the afternoon on Parliament Hill. Prime

Minister Justin Trudeau will host Obama and Mexican president Enrique Peña Nieto for the so-called Three Amigos meeting here in the capital, and the jam-packed itinerary means road closures and travel restrictions, mostly downtown. Obama is scheduled to arrive at the Ottawa airport at 10:15 a.m. However, the Ottawa Airport Authority says there will be no public viewing area, and it's reminding travellers about traffic reductions and road closures in the vicinity of the airport at the time of Obama's arrival. It's also recommending travellers get to the airport two to three hours before flights scheduled to depart mid-morning and in the early evening. CBC News

Trudeau, Mexican president stand up for free trade, take shots at Trump-style protectionism
The leaders of Canada and Mexico stood shoulder to shoulder on Tuesday, as they heralded a new era of friendship while taking subtle jabs at Brexit and Donald Trump's anti-trade rhetoric. Prime Minister Justin Trudeau and Mexican President Enrique Pena Nieto presented their united front outside the House of Commons, where they pushed reset on the country-to-country relationship by promising reciprocal action on visas and beef. "We've seen around the world many examples of protectionism, of stepping away from trade agreements and engagements like we're showcasing today," Trudeau said. "And I think it's important that allies and partners like Mexico and Canada work together to address the challenges we're facing together (...) As Trudeau and Pena Nieto, who will be joined by U.S. President Barack Obama for the Three Amigos summit on Wednesday, were proclaiming their new friendship, Britain's decision to leave the EU as well as the potential for a Trump presidency hovered over the leaders like a cloud. Many analysts have attributed Brexit to growing angst about the effects of globalization and free trade in the United Kingdom. Those sentiments have also manifested themselves in other parts of Europe as well as the United States. Postmedia (National Post, Ottawa Citizen); Toronto Star

Donald Trump's anti-Mexican talk offensive, worrisome, Mexico's foreign secretary says
Mexico's foreign secretary says everyone should be worried about the kind of anti-immigration sentiment coming out of the United States now, because it shows a lack of respect for countries that are supposed to be allies. "I think this kind of rhetoric and this kind of language is not only offensive or disparaging to Mexicans, I think it should be worrisome for anyone that believes that people have the same rights," Claudia Ruiz-Massieu told CBC News Network's Power & Politics. "You should not use stereotypes or negative categories to talk about countries and peoples that are your friends, your allies — and should be accorded the same respect as anyone else." CBC News

PUBLIC SERVICE / FONCTION PUBLIQUE

Public service unions go to court over federal payroll problems
A dozen unions representing federal government workers are today filing a notice of application in Federal Court to force the federal government to pay its employees properly and on time. Five months after the government launched its problem-plagued pay system called Phoenix, civil servants are still getting short-changed or not paid at all. The most recent wave of complaints comes from among 2,000 recently hired seasonal workers at Parks Canada. "Some of those seasonal workers started back as early as April of this year and they have yet to receive a pay cheque," said Chris Aylward, vice-president of the Public Service Alliance of Canada. CBC News

OTHER / AUTRES

With U.K.'s commitment to NATO questionable, Canada could pick up its security slack
Britain's decision to bolt from the European Union and the ensuring market turmoil, political infighting at Westminster and the EU's hardening position on the impending breakup talks have received massive global attention. But the first real earthquake since last Thursday's repudiation of Europe by British voters has occurred in the security realm on the distant eastern margins of the continent. It was Turkish President Recep Tayyip Erdogan's stunning volte-face in his dispute with Russian President Vladimir Putin over the shooting down of a Russian warplane last fall. Others security aftershocks are sure to follow, especially in Britain itself. Scottish nationalists who are bent on holding another referendum on independence want to get rid of the Royal Navy's multibillion-dollar nuclear deterrence force, based

entirely near Glasgow. This suggests an opportunity for Canada to show greater leadership in NATO, although there is little evidence that the Trudeau government wishes to do more than the bare minimum. National Post

INTERNATIONAL

IS believed to be behind Istanbul airport attack; Nearly 50 dead
A senior Turkish government official has told The Associated Press all initial indications suggest the Islamic State group is behind the attack at Istanbul's Ataturk airport. The official also said nearly 50 people were killed in the attack Tuesday at the airport's international terminal and as many as four attackers may have been involved. Associated Press (Yahoo! News); Al Jazeera; BBC News; Reuters (CBC News); Canadian Press (Huffington Post); Washington Post; Telegraph UK

'Long Summer of Discontent': Officials Worry Turkish Attack Could Be Start of Terror Campaign
The deadly bombings at a Turkish airport could be the start of a new wave of terror attacks, worried U.S officials told NBC News. "Our long summer of discontent has just begun," a senior intelligence official told NBC News Tuesday evening. The use of multiple suicide bombers fits the M.O. of ISIS — not the Kurdistan Workers' Party, or PKK — and so does the target, in this case Ataturk International Airport in Istanbul, they said. "There are only two groups capable of carrying out such a large scale attack," a senior U.S. counter-terrorism official said. "This does not fit the PKK profile, they go after Turkish targets, not international targets." Also, ISIS is far more bloodthirsty than the Kurdish rebel group, which has been battling Ankara for years and tends to go after military targets. NBC News

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

Gerry Pingitore
Honoured to take part in TriServices @Safety_Canada Comp-Benefits Roundtable 4 Public Safety Officers with Minister @RalphGoodale. Mandate

Randy Mellow
Pleased to rep @ParamedicChiefs in Ottawa at Rnd Table on Compensation Benefits for PS Officers with @RalphGoodale

IAFF Canada
Min Goodale addresses tri-services Roundtable. Reaffirming his commitment to PSOC. @RalphGoodale @Safety_Canada

Paramédic Québec
Déclaration cet après-midi du ministre de la Sécurité publique et Protection civile, @RalphGoodale. #paramédic #PTSD http://nouvelles.gc.ca/web/article-fr.do?mthd=index&crtr.page=1&nid=1091669&_ga=1.130425551.132429070.1467142624 …

CAPG
CAPG Director Ron Skye meeting w/@Safety_Canada Minister @RalphGoodale at Tri-Services Roundtable on Comp. Benefits

HuffPost Québec
BLOGUE Comment le vrai changement prend forme - Ralph Goodale #polcan http://huff.to/291Ff0l

Ralph Goodale
Excellente table ronde avec services pompiers, police+paramédicaux sur prestations d'indemnisations pour blessures graves/décès en devoir.

Ralph Goodale
An excellent Roundtable today w/ Fire, Police + Paramedic services about Compensation Awards for line-of-duty deaths/disabilities.

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Stewart Bell
2/ISIS "kill lists" are just random names, an attempt to swamp counter-terrorism authorities.

Stewart Bell
"Kill them immediately." Pro-ISIS group releases ridiculously overambitious Canadian "kill list" with 12,000 entries, says @MEMRIReports

Stewart Bell
Quebec CVE programs don't address the core problem: the false "war on Islam" narrative, argues @borealissaves.

Phil Gurski
My views on Quebec's CVE efforts

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CPAC
Sec. @DHSgov Jeh Johnson joins @luizachsavage to discuss borders and security issues ahead of #NALS2016 (link: https://youtu.be/d3Pv7iF3wf4) youtu.be/d3Pv7iF3wf4 #cdnpoli

Jason Kenney
1/ Here's some context on the 2009 Mexican visa imposition that is not being reported: Canada was receiving ~1000 asylum claims from Mexico

Jason Kenney
2/ per month, more than from any country at any time in the history of our asylum system, totalling 26% of all asylum claims made in Canada.

Jason Kenney
3/ 92% of those Mexican asylum claims were deemed unfounded, i.e. false claims, by the Immigration & Refugee Board, and Canadian courts.

LAW ENFORCEMENT / APPLICATION DE LA LOI

CBC Toronto
LIVE NOW: Peel police tell us the latest in the Mississauga explosion investigation http://bit.ly/2918e8k

Global News
Aftermath of Mississauga home obliterated after explosion

CBCCanada
Project E-PANA: RCMP to meet with daughter of woman found dead 40 years ago http://ift.tt/2986UzG

globalnews
'It's going to be nice for me to have some place to go': Memorial in St. Albert will honour RCMP Const. David Wynn

CTV Vancouver
#Update: RCMP say a 21-year-old Surrey man was shot near 128 Street and 60th Avenue Thursday, then showed up at local hospital.

INTERNATIONAL

AFP News Agency
#BREAKING At least 32 dead, 88 wounded in Istanbul attack: media report

Amarnath Amarasingam
As @rcallimachi rightly notes, ISIS has never claimed an attack in Turkey. And they're not shy about it, even when there is tangential link.

Washington Post
What we know now: - At least 28 killed; 60 injured - There were 3 assailants with suicide vests

Associated Press
BREAKING: Report: Turkish justice minister says 10 people killed in blasts at Istanbul airport.

Sky News
Turkish minister says Istanbul airport attacker opened fire with Kalashnikov rifle; two suspects blew themselves up

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

Sent to: !INTERNAL; CBSA Today's News; CSC & PBC Today's News; PS Today's News; RCMP Today's News; RCMP Today's News 2

Today's News / Actualités
July 14, 2016 / le 14 juillet 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Immigration detainees on hunger strike demand meeting public safety minister
A blog post states "Sixty-eight immigration detainees in two maximum security prisons in Ontario -- Toronto East Detention Centre in Scarborough and Central East Correctional Centre in Lindsay -- began a hunger strike on Monday to demand an end to indefinite detentions in maximum security prisons. The immigration detainees, all racialized and undocumented men, will not end their hunger strike until they are able to meet with **Public Safety Minister Ralph Goodale**. **Goodale's** receptionist has refused to schedule a meeting between **Goodale** and the detainees, and maintains that **Goodale** cannot speak to members of the public. When detainees phoned their local MP, Conservative MP Jamie Schmale, he refused to facilitate a meeting with **Goodale**. "We are in this together, we gotta make this happen 'cause we're really really tired of being in here. We can't take this no more," said Patrick, one of the hunger striking detainees in Lindsay, in an End Immigration Detention Network media release (…)Immigration

detainees began a hunger strike in April, following the death of Francisco Javier Romero Astorga, a 39-year-old Chilean father of four. The hunger strikers demanded an end to indefinite detention in maximum security, an overhaul of the judicial review process, and improvement in prison conditions. The hunger strike came to an end when CBSA officials agreed to meet with the detainees, but the CBSA did not follow through on the promises they made. This time around, the hunger strike takes aim at elected officials. "They [have] no way to have their voices heard, so they are on a hunger strike with one clear demand -- to meet with **Minister Ralph Goodale**," Chak explained." Rabble.ca

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Disaster assistance officials in Estevan today
Flood-affected residents of Estevan will be getting some help from provincial disaster assistance officials today. The southeastern Saskatchewan city is no longer under a state of emergency, but that was the case Sunday night, after heavy rainfall flooded streets and basements. The area got more than 13 centimetres of rain. Now, residents of the town are in cleanup mode. On Thursday, staff with the Provincial Disaster Assistance Program will be in the city to help people submit claims. They'll be bringing all the forms people will need for their applications. PDAP program advisors will be available at the Estevan Leisure Centre board room from noon to 8 p.m. CST. They'll also be available Friday (9 a.m. to 8 p.m.) and Saturday (9 a.m to 1 p.m.). There will also be a building inspector from the province's building standards branch to help with onsite inspections. The inspector will be available Thursday from noon to 8 p.m. CBC News

Road to Caddy Lake reopens after weeks-long flood closure
A road to a popular cottage destination near the Manitoba-Ontario border that closed for almost three weeks due to flooding has finally reopened. Highway 312 between Highway 44 and the Ontario border, which leads to Caddy Lake, opened back up Thursday. It was closed at the end of June after a section of the road washed out following a heavy two-day downpour. Several other roads in the Whiteshell were damaged by erosion during the same storms. Some roads and hiking trails remain closed or are under construction, while others have been opened. CBC News; Winnipeg Free Press

Fort McMurray homeowners frustrated about rebuilding process
The enthusiasm to rebuild homes after the Fort McMurray wildfire has given way to frustration for some residents. "You really don't know who you can trust, that is the biggest thing in Fort McMurray right now," said MacKenzie Cadieux, who lost her home in Abasand. The enthusiasm to rebuild homes after the Fort McMurray wildfire has given way to frustration for some residents. "You really don't know who you can trust, that is the biggest thing in Fort McMurray right now," said MacKenzie Cadieux, who lost her home in Abasand. Cadieux and other residents from fire-ravaged communities attended a forum at Shell Place on Wednesday evening, where a lawyer and a contractor answered questions. CBC News

NATIONAL SECURITY / SÉCURITÉ NATIONALE

What's Next For Canada's Surveillance Landscape?
Edward Snowden's 2013 revelations of massive state surveillance shocked the world and made it more aware of electronic privacy issues, but north of the border, Canada continues to struggle with its own. Just over a year ago, the former Conservative Canadian government, led by Stephen Harper, enacted a piece of legislation that enraged privacy advocates. Bill C-51 extended the powers of Canada's intelligence services, prompting an open letter from over 100 Canadian academics imploring the government to rethink it. Even the federal Privacy Commissioner complained about it. A year later, we have a new government that has promised to overhaul things. What has been done, and where does Canada's complex debate over privacy and national security sit now? C-51 angered privacy advocates by increasing information-sharing powers between 17 government agencies. The Canadian Security Intelligence Service (CSIS), which is Canada's domestic intelligence agency, can now obtain the tax records of anyone perceived to be a national security threat, for example. The bill also permitted the disclosure of information shared between government agencies to others. Dark Reading

Broadcast Media / Médias télédiffusés:

The Canadian Security Intelligence Service has officially joined social media. Canada's spy agency sending out its first tweet. Officials say the service recognizes that a modern organization needs to communicate using modern means. (CTV News, 10:00ET)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Border services' gun smuggling busts 'showcasing': criminologist
Smuggling charges, hidden handguns more of a warning to gun-toting U.S. tourists, not crime-related says SFU prof. If you feel safer from gun violence thanks to news that border agents have been catching U.S. handguns at the border recently, you're likely mistaken. The Canada Border Services Agency announced on Tuesday that two travellers busted with guns at the Abbotsford border crossing were convicted of smuggling, and on Monday the agency announced it had caught a woman in Prince Rupert who had hidden parts of a handgun throughout her car while driving from Alaska. "Canadian firearms laws are clear," CBSA said in a press release. "Anyone importing firearms and weapons into Canada must declare them and meet all licensing and registration requirements under the Firearms Act. (…) Although gun violence in the Lower Mainland has led to furor amongst residents after several fatal shootings this year — and mounting concern about rampant mass shootings south of the border — one Simon Fraser University criminology professor said the two issues are entirely unrelated and should not be confused.. Metro News

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Clever Tool Shields Your Car From Hacks By Watching Its Internal Clocks
Car hacking demonstrations tend to get all the glory in the security research community—remotely paralyzing a Jeep on the highway or cutting a Corvette's brakes through its Internet-connected insurance dongle. But as the nascent automotive security field evolves, defensive tricks are getting cleverer, too. Now there's a new prototype gadget that stops those vehicular attacks with an ingenious hack of its own. In a paper they plan to present at the Usenix security conference next month, University of Michigan researchers Kyong-Tak Cho and Kang Shin describe an easy-to-assemble tool they call the Clock-based Intrusion Detection System, or CIDS. It's designed to spot the malicious messages car hackers use to take control of vehicle components like brakes and transmission. Wired Magazine

LAW ENFORCEMENT / APPLICATION DE LA LOI

Bob Paulson apologizes for 'egregious behaviour,' nudity at RCMP bomb school
RCMP Commissioner Bob Paulson is apologizing to victims and witnesses of "egregious behaviour" at one of the Mounties' top training facilities. CBC News has learned the force has also removed Chief Supt. Marty Chesser, commanding officer of the force's national headquarters, from his post. The apology comes in a long-awaited internal report into allegations of harassment and sexual misconduct at the explosives training unit at the RCMP's Canadian Police College in Ottawa. The RCMP accepts all of the findings and has already drafted a plan on how it intends to implement all 28 recommendations. The force has committed to making more than two dozen reforms, including significant changes to how it investigates and disciplines employees, as well as a national initiative to eradicate sexual misconduct in the police agency's workplace. The review of what happened at the college followed CBC News reports about rampant nudity, allegations of sexual harassment, bullying and other disgraceful conduct at the school for bomb technicians. At the end of February, Paulson asked assistant commissioner Steve White to lead the review. The results, shared with CBC News, detail a historically dysfunctional workplace where employees felt they couldn't complain about mistreatment without risking retaliation and being labelled "rats." The review team found a long string of "unacceptable" failures in the leadership of RCMP

management, the disciplinary system and human resources practices. "Specifically, the investigations and processes related to these events were fraught with missed opportunities to effectively deal with misconduct, protect the victims and witnesses and heal the workplace. It is for these reasons that the RCMP commissioner and the RCMP as an organization sincerely apologize to all who were negatively impacted," the report says. Despite two previous investigations into disturbing behaviour at the school, this new inquiry has turned up new allegations, including "bullying, intimidation, harassment and new allegations of unwanted sexual touching." CBC News

Broadcast Media / Médias télédiffusés:

CBC News reports that RCMP Commissioner Bob Paulson apologizes for sexual harassment and misconduct allegations at the Canadian Police College. Rough Transcript

RCMP collide with pick-up during chase
An Okotoks RCMP member and a Volker Stevin employee are in hospital after a police car collided with a pick-up truck during a chase this morning. At about 7:45 a.m. an RCMP SUV was in pursuit of a vehicle travelling north in the southbound lane on Northridge Drive near the intersection at Elizabeth Street. The RCMP vehicle collided with a Volker Stevin pick-up truck in the intersection and the suspect vehicle then fled north in the southbound lane. The officer had to be removed from the SUV on stretcher and the Volker Stevin employee was able to walk from the truck. Both were transported to South Health Campus with minor injuries. Western Wheel; 660 News; CTV News; CBC News

Man threatenes to kill police while brandishing rifle in Nova Scotia: RCMP
Police in Nova Scotia say a young man is facing charges after he allegedly threatened to kill police while holding a rifle. The RCMP say they were called to a dispute on East Side Harbour Road in the community of Boylston, Guysborough County around 9 p.m. Wednesday after a man had broken the windows of a home, and several vehicles. When officers arrived, they were told by people inside the home that a man had threatened to kill them, and that he had fired his rifle several times. At that point, police allege the man threatened to kill officers on site. “RCMP officers moved the individuals inside the residence to a safe location and called in additional RCMP officers from neighbouring detachments and the Nova Scotia RCMP Emergency Response Team,” a police release states. “The situation was resolved when the man surrendered to the RCMP just after 5 a.m., without incident.” No one was injured. Police say the accused and the people inside the home were known to one another. A 20-year-old man from Boylston is now facing 12 charges, including eight counts of uttering threats, and single counts of assault, careless use of a firearm, unauthorized possession of a firearm and mischief. Metro News

Millington loses appeal in Dziekanski tasering
The Mountie who tasered Robert Dziekanski at YVR airport almost 9 years ago has lost an appeal of his perjury conviction in the BC Court of Appeal. Last February, Kwesi Millington was found guilty of one count of perjury for lying under oath at the Braidwood Inquiry into the death of Polish Immigrant Robert Dziekanski at YVR airport. Millington tasered Dziekanski twice before he died. He was sentenced to 30 months in prison, but appealed. That appeal has now been dismissed. Millington’s lawyers argued the evidence that Millington colluded with other officers before the inquiry was weak. The BC Court of Appeal says “it was not an abuse of process for the Crown to pursue the collusion allegation, nor was the Crown estopped from relitigating the collusion issue because of the outcome of the earlier trial.” Another Mountie convicted of perjury, Cpl. Monty Robinson, also appealed. It has yet to be heard. Two other officers were acquitted. One of them, Constable Gerry Rundel, was in court today to support Millington. He says he’s back on the force, working in Nanaimo. AM 730 (CJOB); Canadian Press (CFRA News, Castanet, Vancouver Sun, Chronicle Herald)

Nunavut RCMP least reflective of region's population of all Canadian police forces
Nunavut's top cop says it will likely take 'many generations' to build a police force that reflects Nunavut's diversity. A new CBC investigation surveyed police forces across the country to compare how diverse they are compared with the populations they serve. In Nunavut, 12 per cent of the police force is racially diverse, compared 88 per cent of the territory's total population. That makes the territory the least reflective jurisdiction in the country. Mike Jeffrey, commanding officer for Nunavut's RCMP, says the low

graduation rate of Nunavut high school students is a challenge to recruitment and those who do graduate are actively sought by other government departments looking to hire more Inuit. He said there is also a "security issue." "If you want to be a police officer, or in law enforcement, you have to have demonstrated that you were living a lifestyle that would promote the law enforcement mentality of desire," he said. "We don't want people who are taking drugs, or who would have committed a crime in the recent past." Right now, all 11 Inuit RCMP members are based in Iqaluit. About 150 people work for Nunavut RCMP, although that includes both sworn officers and civilian staff. CBC News

Rate of complaints against Codiac RCMP increase in 2016

The Codiac RCMP has received a higher rate of complaints so far this year than it did in 2015. There have been 18 complaints within six months this year, compared to a total of 24 for all of last year. At the Codiac Regional Policing Authority meeting Wednesday night in Moncton, board member Courtney Pringle Carver asked Inspector Jamie George about the types of complaints the RCMP receive. "People are not happy with the way they were spoken to, perhaps; it could be somebody who said that the police used excessive force; It could be something where there was an irregularity in procedure, in some cases it's about people feeling that the RCMP did not conduct an adequate investigation into their complaint," George listed as examples. George said he was not alarmed by the increase. He said until April, the trend suggested the RCMP were making progress addressing complaints and the numbers were down. But George said a new process now allows people to file complaints online. "We were going along very, very well in the beginning of the year and we only had three or four," George said. "But there were a number that came in through the online system that went directly to Ottawa, that didn't get processed in Ottawa and pushed down to us so we could follow them up. And then we got seven or eight in a row." CBC News

Codiac RCMP costs expected to rise in greater Moncton

Taxpayers are going to need to dig deeper to pay for the Codiac RCMP in the future as the force looks to cover several big ticket items and plan for an increase in staffing, the Codiac Regional Policing Authority heard on Wednesday night. Paul Van Iderstine, the Codiac Regional Policing Authority's treasurer, said there are several inevitable costs in front of the force that must be paid for in the next few years. "We have the new communication system, we have the new police building and we've got a collective bargaining unit that we are going to have to deal with," he said. "So the total increase in costs for the policing services in the Codiac region are really, we can't say at this point in time, but we know there's some big, big ticket items coming down that we're going to have to look at." Moncton, Riverview and Dieppe have already budgeted about $2 million to get the Codiac RCMP up and running on the New Brunswick Trunk Mobile Radio system, a communications system that will allow the police across the province to encrypt communications. Van Iderstine said a special committee has already been formed with the three municipalities to start investigating a new Codiac RCMP headquarters. That group is looking at the potential costs with the new headquarters. RCMP Insp. Jamie George was asked about a possible financial outcome of the Supreme Court of Canada decision that allows RCMP officers a right to collective bargain. George said there are still many unanswered questions about how the top court's decision will roll out and what financial demands it will create. Terry McKee, a retired RCMP officer and current spokesperson for the Mounted Police Professional Association of Canada, told the police authority that the board should expect staffing costs to rise. "Members are looking for a substantial raise in their salary," he said. CBC News

Ottawa police officer Marie Josee Seguin acquitted on drunk driving charge

An Ontario judge has acquitted an Ottawa police officer charged with impaired driving, and chastised the RCMP officers who pulled her over for their "atrocious" and "disturbing" note taking. In May 2014 RCMP Const. Gary Lee pulled Marie Josee Seguin over for erratic driving on the Highway 417 eastbound off-ramp at St. Laurent Boulevard. Seguin, who was off duty at the time, was later charged with impaired driving and failing to provide a breath sample. Sequin argued that the stop and her detention were unlawful. She argued the RCMP does not have the authority to stop drivers on Highway 417, nor is there a bilateral agreement between the RCMP and Ottawa police for that stretch of road. In his ruling Justice Allan Letourneau said he believed Lee pulled Sequin over because he feared for the public's safety. But Letourneau went on to characterize Lee as "a very poor witness," and scolded all four responding RCMP officers for their "atrocious" note taking. In court even Lee admitted he would grade his own notes that day with an "F." The judge chastised Lee for filing his general report more than 15 hours after the

incident. When pressed about why he omitted certain details in his notes, Lee said he didn't remember them until he testified. For example, he wrote that Sequin fumbled to find her ID, but failed to mention that the licence was behind other documents in her wallet. The extent of the failure of all four officers to comply with their own force's note taking requirements is astounding and disturbing," wrote Letourneau. "Contemporaneous and comprehensive notes are especially important in drinking and driving cases where often there is no independent evidence available to corroborate the testimony of police officers." The judge questioned if Sequin was in fact inebriated when "no other witness testified that she was very drunk." CBC News

Unmasked: The face of Anonymous activist shot dead by RCMP
One year after a masked man linked to Anonymous was shot dead by RCMP in northeastern B.C., a relative wants to reveal the true face of James McIntyre. McIntyre, 48, was killed on a sidewalk by officers responding to a call about a disturbance at an open house for BC Hydro's controversial Site C dam project in Dawson Creek on July 16, 2015. "Jim didn't deserve to die in a brutal manner," said McIntyre's cousin, Keith LaRiviere, Sr. "The man lying on the ground was not a criminal. He was a victim of police violence." LaRiviere described the cousin he grew up with as a gentle, innocent, intelligent man who stuttered, rarely conversed with people and loved model trains. (...) After Anonymous claimed McIntyre as a comrade and threatened to avenge his death, the Dawson Creek man made international headlines.(...) Initial reports to BC's police watchdog alleged McIntyre was shot after a man with a knife "approached officers in an aggressive manner" outside a Site C open house in Dawson Creek on July 16, 2015. Witness Mike Irmen said the man who was shot was wearing a mask, similar to the Guy Fawkes mask often used by Anonymous and refused to throw away his knife, even as he lay bleeding. LaRiviere believes his cousin was at the Site C meeting to make a statement, not to hurt anyone. "Making a statement with that mask makes all the sense in the world to me for Jim, because he was alone in his life," said LaRiviere. RCMP declined to comment, as the fatal incident is still being investigated by B.C.'s police watchdog."The bulk of the investigative work is complete," said Marten Youssef, the Independent Investigation Office's manager of strategic communications. Youssef said an internal review of the investigation still needs to be completed. Until then, there's no official information about what happened or whether RCMP officers acted appropriately. Youssef says he's aware of reports of Anonymous' interest in the case. But he says that's had no bearing on the IIO investigation. CBC News

2017 RCMP Musical Ride tour application deadline is now here
The deadline to book a 2017 appearance of the RCMP Musical Ride is Friday. "We are excited to have cities and towns across the country help us celebrate Canada's 150th birthday by hosting the 2017 Musical Ride and raising money for their communities," says Superintendent Leslie Cook, Officer in Charge of the Musical Ride Branch. To celebrate Canada's 150th birthday next year, the RCMP Musical Ride is organizing a coast-to-coast Canadian tour with stops near capital city regions, along with stops in between major centres to ensure the horses' welfare. The RCMP Musical Ride is performed by a full troop of 32 riders and their horses. Their performance consists of intricate figures and drills choreographed to music. These movements demand the utmost control, timing and coordination. The RCMP is seeking non-profit organizations to submit online applications to host the Musical Ride during this 2017 tour. Due to the large scope of this tour, applications must be received by July 15, 2016. The 2017 tour will commence in May. The Musical Ride will return to Ottawa in late June to participate in Canada Day celebrations in Ottawa. The tour will resume in early July and will continue until September. Dawson Creek Mirror

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

NIL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Increase in firearm arrests 'staggering:' Prince Albert police
As drug use and trafficking rises in Prince Albert, so does the number of firearms in the city. According to Prince Albert police Chief Troy Cooper, 52 firearms have been seized so far in 2016, compared to 19 in 2015. He said the "staggering" increase in numbers is closely tied to crystal meth and gang activity. "If one gang is using a firearm, the other gang has to use firearms as far as protection or intimidation. We saw it 15 years ago with the increase of concealed weapons like knives and now it's a real trend. It's scary for sure," he said. Police said weapons seized were primarily rifles and shotguns, many of which had been sawed-off for better concealment. Handguns contributed to six per cent of weapons arrests. CKOM

Toronto police constable quits, says tension with community contributes to decision
Former constable Marc Rainford says he recently quit the Toronto Police Service because of the difficulties in policing a society with increasingly polarized attitudes towards cops. With The Current, Rainford offers insight into the importance of police maintaining positive relationships with the communities they serve, and explains the devastating impacts of associating Canadian law enforcement with the behaviour of police officers in the United States. CBC Radio - The Current

Racism on the agenda as Mayor, Premier meet with Black Lives Matter this evening
Mayor John Tory and Premier Kathleen Wynne will hear about racism directly from the community in Toronto this evening. The province's new anti-racism directorate will meet with members of Black Lives Matter and community representatives during its first consultation. They say the meeting will focus on systemic racism, including anti-Black racism, Islamophobia, anti-Indigenous racism and racism experienced by other communities. The Premier agreed to the meeting after several BLMTO protests, including one at Queen's Park in early April and later, during this month's Pride parade. Sandy Hudson, a representative from Black Lives Matter Toronto, asked for the meeting. "We wanted to facilitate a space where the public would be able to communicate directly with decision makers and policy makers what their experiences have been at the hands of the police and how the system falls short", she told Metro Morning's Matt Galloway Thursday. She says the meeting will bring together different voices from racialized communities. (…)Lawyer and advocate Anthony Morgan will also be at the meeting. "That we have representatives from various heads of government is really important. I don't think there has been this much interest in having this honest a conversation about race, racism and its impact on impeding the lives and well-being of racialized people." Morgan says black people are over represented in the prison system, and carding has still not been fully eliminated. These are some of the issues he'd like to see addressed this evening. CBC News

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Too-stringent cannabis rules a bad idea
An editorial states, "It was always clear that many hurdles will have to be jumped before legal marijuana can become a reality in Canada. Pot advocates won't be too pleased with the latest one. Ottawa, which recently struck a marijuana task force led by former deputy prime minister Anne McLellan, is sending strong signals legalized pot will be so strictly controlled that homegrown weed (even for medical purposes) may remain an illegal substance. For advocates, this will come as surprising and unwelcome news. Federal Health Minister Jane Philpott says the government wants to treat pot like tobacco. She

may or may not be aware, however, that it is actually legal to grow your own personal-use tobacco in small amounts in Ontario. Liberal MPP Bill Blair, justifying a heavy-handed approach, told the Toronto Star last week: "Unlike (growing) tomatoes, (marijuana) is a substance that poses … significant … social and health harms and risks to Canadians … the science is overwhelmingly clear that marijuana is not a benign substance." On that basis, it doesn't exactly sound like something that should be legal, does it? Except that doctors are prescribing it for glaucoma, anxiety, pain relief, muscle spasms caused by MS, nausea, arthritis discomfort, Crohn's disease and more. And we all know recreational use is widespread. A 2015 survey showed 20 per cent of Canadians indulge and another 10 per cent will light up once it appears in stores. A Conservative attempt to prevent medical users from growing their own pot has already been tossed out by the courts. It stands to reason then that preventing non-medical users of a legal substance from growing their own plants could amount to discrimination. Perhaps that is the wrench in the gears." Simcoe

PUBLIC SERVICE / FONCTION PUBLIQUE

Student workers hit hard by federal government's Phoenix pay system glitch
One student worker went five months without a pay cheque. Another had to call the government help centre 177 times before getting an explanation about why she was being underpaid. These are just two extreme examples of how the federal government's new computerized pay system is causing significant problems for public service workers across the country. (…) Yardon, 23, has not been given a proper paycheque since January. He maxed out his credit card, exhausted his savings, and fears he will be forced to drop out of university this fall, because he can't afford his tuition. Making things worse for Yardon, he's stuck in an uncomfortable catch-22. He's employed through the federal student work experience program. To qualify for his job he must be able to prove that he is enrolled in school. CBC News

Broadcast Media / Médias télédiffusés:

The federal government has publicly acknowledged that the situation around the new pay system is unacceptable and they've opened up a temporary work centre to help deal with some of these cases, but workers say that they're still having a difficulty reaching out for help. (CBC News Network, 10:25ET)

OTHER / AUTRES

NIL

INTERNATIONAL

NIL

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

Rabble.ca
Immigration detainees on hunger strike demand meeting public safety minister | @sophia_reuss
http://buff.ly/29SGQLf

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Naomi Yamamoto
Get the Hazard app from the Canadian Red Cross! http://3cu.be/sharecanh @RedCrossBC @redcrosscanada

IBC West
Do you have an #emergency kit? It's never too late - shop or build your own! Easy as ABC123. http://goo.gl/jZFUVl

RMWB
Municipality reminds residents of options for residential debris removal http://ow.ly/auRL302dZro #YMM #RMWB #YMMStrong

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Gary Dimmock
Ottawa terror informant paid $250,000 to testify at hearing that never happened
HuffPost Canada
OMG, we were on TV, gushes Canadian spy service officer http://huff.to/29AY4qK
David Pugliese
Canadian electronic spy service was 'very excited' to be referenced on The Good Wife http://natpo.st/29FqV3h via @nationalpost

BORDER SECURITY / SÉCURITÉ FRONATLIÈRE

No One Is Illegal
Inspired and honored by the support from Colonialism No More - Solidarity Camp Regina for #MigrantStrike.... http://fb.me/4RG1lKo83

No One Is Illegal
#MigrantStrike Day 4 Update - Detainees on endless lockdown. Action in Regina today. Please share and act. http://fb.me/7fxu0OwOw

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Ray Boisvert
Surveying critical infrastructure for attack: UK rail network hit by multiple cyber attacks last year

SC Magazine
52 Flash Player bugs fixed with Adobe's July Patch Tuesday update

SC Magazine
Phishing: What makes people click?

The CyberWire
Russian security officials voice concerns similar to those heard in the West https://goo.gl/Kq7KlW #infosec

Dark Reading
1 In 3 Consumers Worldwide Hit By Payment Card Fraud

Dark Reading
Sandia Labs Researchers Build DNA-Based Encrypted Storage

LAW ENFORCEMENT / APPLICATION DE LA LOI

Global BC
Potential new #Okanagan gang dealt big blow after RCMP raid
Patrick Brazeau
Having seen the RCMP's "proof" against me, what a waste of time and taxpayer's money. Perhaps that is the real

scandal. #cdnpoli

Patrick Brazeau
For 859 days, the RCMP and Crown made me out to be a "fraudster." Perhaps this all ends today. #cdnpoli

Diana Mehta
Police forces across Canada warn of Pokemon Go risks http://fw.to/Y0iwUNQ #PokemonGo #DontCatchAndDrive

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

CBC – The Current
"The mistrust is deep. It's generational... And it's completely well-founded." - @SamTecle http://cbc.ca/1.3678574

KelownaNow.com
19 overdose deaths in #Kelowna so far this year, most #fentanyl related #Okanagan

VICE Canada
When cops can legally shoot people: http://bit.ly/29zj4E1

CBC Politics
WATCH LIVE: Day 3 of the Assembly of First Nations annual general assembly in Niagara Falls http://www.cbc.ca/1.2866916 #AFNAGA #cdnpoli #hw

PUBLIC SERVICE / FONCTION PUBLIQUE
Katie Simpson
Here's the write on our story about the federal government's pay problem:

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

Today's News / Actualités
July 14, 2016 / le 14 juillet 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Protesters unite to call on federal government to take action on issues
In a show of support for immigrant detainees, members of the Colonialism No More Solidarity Camp, gathered in front of **Ralph Goodale's** Regina office for a peaceful demonstration. Over the noon hour on Thursday, about two dozen people - including children - carried signs, waved flags and called on **Goodale** to take action in Ontario. On Monday, immigrants at two Ontario federal detention centres began refusing food because they want to meet with **Goodale**, **the federal minister of public safety.** Sue Deranger, a member of the camp, says the immigrant detainees are not asking for much. "All they are asking with this hunger strike is to meet **Goodale** and he will not meet that demand," she said... Deranger said members also invited **Goodale** to come to the solidarity camp and he has not. "We asked **him** in person and he said, ***'Send an email.'*** We did, and still **no response**," she said. "What's the harm in sitting with people?" Robyn Pitawanakwat greets **Ralph Goodale's staff**. Robyn Pitawanakwat, a

member of the camp, doesn't think it's right the Canadian government gets to decide who stays in Canada and who cannot... **Goodale** was not in Regina and could not meet with the protesters, but **his Regina staff did**. **They asked** if the group had any written requests they wanted to pass on to **Goodale**. The group did not have a letter, but asked **the staff** to tell **Goodale** to reply to his emails. **The staff said** they received all **Goodales's** email and received nothing from the solidarity camp. After some discussion, it was discovered that the protesters had the incorrect email address. The correct address was provided and the group was **encouraged** to resend their messages. Leader-Post

60 Migrants Detainted Indefinitely Launch Hunger Strike
Canada is the only western nation with a policy of indefinite immigrant detention, and over a third of detainees are held in maximum security prisons. Nearly 60 immigrant men at two Ontario maximum security prisons Thursday entered the fourth day of a hunger strike to protest the Canadian policy of indefinite immigration detention that denies immigrants access to any judicial process. The immediate aim of the strikers is to pressure Ontario's **Public Safety Minister Ralph Goodale** to meet with the detainees to discuss concerns about indefinite detention, and the use maximum security prisons for immigrants who have not been charged with crimes... According to the End Immigration Detention Network, the strikers have been organizing around these issues since 2013 but elected officials — including **Goodale** — have been unwilling to meet with them. The watchdog organization has been calling on supporters to petition the minister's office to meet strikers' demands. But so far **Goodale's** sole response to the hunger strike has been a statement this week claiming that immigration detention is a ***"last resort"*** policy, even while the immigrant justice organization No One is Illegal has long described it as a "first resort." teleSUR

RCMP apologizes over harassment episode, promises national effort
The RCMP will launch a new national effort to eliminate sexual misconduct in the workplace after an internal review criticized the police force's response to an "egregious" case involving nudity and harassment. The review concluded the RCMP's initial investigations into behaviour at the Canadian Police College were "fraught with missed opportunities" to effectively deal with the misconduct, protect the victims and witnesses and heal the workplace. RCMP Commissioner Bob Paulson accepted a special steering committee's 28 recommendations based on the findings, and he apologized to those who experienced distress over the episode. Paulson has been wrestling for years with problems of bullying and harassment within the national police force by introducing a "respectful workplace" course, setting up employee advisory committees, encouraging settlement of complaints at the earliest opportunity and promoting more women to senior posts. Earlier this year, **Public Safety Minister Ralph Goodale** expressed outrage to Paulson when allegations surfaced about unwanted sexual touching, bullying and rampant nudity in the explosives training unit of the RCMP-administered police college in Ottawa... Paulson has committed to providing **Goodale** with a "comprehensive action plan" within 30 days on implementing the recommendations. Canadian Press (Maclean's, Winnipeg Free Press); Toronto Star

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Cleanup underway from Saskatchewan flooding as evacuation order fully lifted
Flood response has shifted to recovery mode in Saskatchewan communities hit hard by heavy rainfall earlier this week. Emergency management commissioner Duane McKay said it's too soon to know how much damage was caused... The town of Arborfield lifted an emergency evacuation notice Thursday. Canadian Press (StarPhoenix)

Summer storm causes damage and power outages in Quebec
A powerful summer storm swept through Quebec on Thursday afternoon, causing power outages and damage around the province. "The worst was anywhere between the American border and south of Drummondville, and even south of Quebec City," said Robert Michaud of Environment Canada. CBC News

Unapproved drainage to be outlawed at the Quill Lakes
The Water Security Agency (WSA) is to begin clamping down on unapproved drainage systems that contribute to flooding at the Quill Lakes, using new powers under the Agricultural Water Management Strategy regulations that were passed last fall. Leader-Post

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Whistleblower Edward Snowden to keynote Toronto conference
The man that says he lives on the Internet will be the showcase speaker at SecTor, a Toronto-based security conference this year. Edward Snowden, the former CIA employee and government contractor that leaked classified documents about a mass surveillance operation run by the National Security Administration (NSA), will be appearing at the conference via a video link from Russia, where he's been living under asylum since 2013. SecTor will be Snowden's first and only commercial conference appearance in North America this year, conference organizers say. "Edward Snowden is not only one of the biggest names in cybersecurity, but his unique situation and cybersecurity experiences also make him one of the most important and influential," said SecTor co-founder Brian Bourne in an email announcement…Beyond NSA's clandestine mass surveillance operations that were leaked by Snowden, Canada's Communications Security Establishment (CSE) has also been the subject of some of his classified leaks. He's also said that Canada's intelligence gathering operations have the "weakest oversight" among western nations. IT World Canada

Mother of an ISIS Recruit Tells of Loss and Hope
Christianne Boudreau was standing in her garage, braving the cold Calgary night to finish her cigarette, when the phone rang. She didn't recognize the number on the caller I.D. Thinking it could be her 22-year-old son Damian Clairmont calling from Syria, she quickly answered. But the voice on the other end of the line was not Damian's – it was a reporter. "He asked me for a current picture of Damian," Boudreau says. "I told him he should just use the one Damian has as his profile picture on Facebook. But the reporter sighed and said, 'Never mind, that's the same picture ISIS has just used in your son's eulogy.'" Then he hung up. That was how Boudreau learned her son was dead. It had been just over a year since two agents from the Canadian Security Intelligence Service (CSIS) had arrived on Boudreau's doorstep and shattered her world by telling her that Damian – her kind-hearted, curious, goofy boy – was fighting with the so-called Islamic State (ISIS)…Like so many mothers who lose their children to radicalization, Boudreau had no support; no one to help her cope with her new, tragic reality. The CSIS banned her from telling anyone that Damian had joined ISIS, and so she spent her days pretending everything was fine. News Deeply

Twitter spies
An opinion piece states, "While the intelligence services of their southern neighbour are well-known, Canada's own surveillance network has remained more low-key, in keeping with the country's own easy-going image. But on Wednesday, the agency broke cover with its first ever tweet: "Yes, we're on Twitter. Now it's your turn to follow us." Canada's spies don't get much publicity – the closest to Hollywood glamour came in a bit part for a Canadian intelligence officer in the James Bond film Quantum of Solace – but the country ought to have very good spies, drawn from a multilingual, multicultural society used to people abroad thinking they're someone else ("No, I'm not American"). Plus, of course, being low-key means they don't see you coming. Bad guys used to avoiding CIA drones or charming MI5 operatives are likely to be less adept at avoiding flying ice hockey pucks." The National UAE

BORDER SECURITY / SÉCURITÉ FRONATLIÈRE

NIL

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

RCMP say problems with phone lines continuing in N.W.T.
N.W.T. RCMP say they are still getting reports of problems with telephone service two days after Northwestel repaired a damaged fibre line that disrupted service across the North. Service problems were reported over the weekend and Northwestel said Monday the problems were due to a fibre line in northern B.C. damaged by a landslide, and congestion on the line to which all services were rerouted. Some customers had trouble using long distance and wireless services, as well as 1-800 calling. At the time, officials advised people in N.W.T. and Yukon to go to their local RCMP detachments if local emergency phone lines were unavailable. CBC News

RCMP: iTunes tax scam
RCMP in the North Okanagan have issued yet another warning about a scam in which a caller claims to be from the Canada Revenue Agency (CRA) and demands payment. The scam has a new twist, with the caller demanding payment in iTunes cards. "Several local people have been contacted by scammers pretending to work for the CRA," said Const. Jocelyn Noseworthy, RCMP spokesperson. Castanet.net; CFJC Today

RCMP investigating reports of counterfeit currency, searching for two suspects
Police in central Alberta are on the lookout for two suspects as they investigate reports of counterfeit Canadian currency being used. Red Deer RCMP said they first received reports of counterfeit currency on July 8, after a staff member at Wild Bill's Sports Bar noticed a problem with a number of $100 bills that had been used in the establishment. CTV News

Surrey RCMP searching for SUV involved in targeted shooting
Surrey RCMP are looking for help in finding additional suspects involved in a targeted shooting that sent one man to hospital in early April. Mounties were called to the area of 86A Avenue and 140th Street at about 1:55 p.m. on April 4 after receiving reports of several shots being fired. When officers arrived they found an man suffering from a gunshot wound. He was taken to hospital and later released. Global News

Priest charged with stealing $500K meant to bring refugees to Canada
London police have charged a priest with defrauding more than $500,000 intended to sponsor Syrian refugees coming to Hamilton. Amer Saka of London, a 51-year-old Chaldean priest, is charged with fraud exceeding $5,000 and possessing proceeds of crime. CBC News

SIU investigating after senior Tasered, breaks rib during interaction with Peel cops
The province's Special Investigations Unit was on the scene of a central Mississauga home today after a 65-year-old man was seriously injured while Peel Regional Police were executing a search warrant. Mississauga.com

Annapolis Valley woman who defrauded military resource centre faces 17 tax evasion, criminal charges
The Coldbrook woman who defrauding the Greenwood Military Family Resource Centre of over $409,000 is now facing tax evasion charges. Karen Lorraine Byers, 57, was charged July 13 with 11 charges under the Income Tax Act and six under the Criminal Code. Cape Breton Post

Calgary police say suspect in new arrest video went for officer's Taser
Calgary police say a video of an arrest at the Stampede Wednesday involved a suspect who was "heavily intoxicated" and attempted to grab an officer's gun, police said in a release Thursday. Police responded to the Nashville North tent just before 10 p.m. after reports of a man stealing other people's drinks and refusing to leave. CBC News

Justice minister apologizes to departed police-board members
Manitoba Justice Minister Heather Stefanson says she has apologized to two former members of the Winnipeg Police Board for the manner in which they learned their services were no longer required. In an order of council dated July 6, Brian Pallister's Progressive Conservative government revoked the police-board membership of Leslie Spillett and Angeline Ramkissoon, who were appointed by Greg Selinger's NDP government. CBC News

Police forces across Canada warn of risks involved with playing Pokémon GO
Police forces across Canada are warning of the risks involved in playing augmented reality games such as Pokémon GO as reports mount of people getting injured or landing in trouble as they play the wildly popular game. The cellphone-based game sends players into the real world to search for digital monsters known as Pokémon, who appear on screen when users hold up their iPhones or Android devices in various locations at various times. Canadian Press (National Post)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Inquest needed, again
An editorial states, "How did it happen again? How did yet another woman with mental health issues choke herself to death while in a solitary confinement cell at Kitchener's Grand Valley Institution for Women? How and why did Terry Baker die in this terrible way last week? We thought Correctional Services Canada and the federal government had learned important lessons after all the lengthy investigations and earnest recommendations for change that followed the 2007 death of Ashley Smith, in the same prison, in what appear to be remarkably similar circumstances…" theIFP.ca

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Calgary police warning public of release of high-risk offender
Calgarians are being warned of the release of a high-risk offender who has a history of sex offences involving children. Dustin Roy Williamson, 23, was released into the Calgary community Thursday after serving a three-year sentence for sexual interference and child pornography, according to the Calgary Police Service. Calgary Herald

High Risk Sex Offender Released Into London
Police are warning Londoners that a high-risk sex offender has been released into the community. The London Police Service announced Thursday afternoon that 40-year old Jason William Cornish was released from a federal prison after completing his sentence. iNews 880 AM

Cocaine courier launches appeal
A cocaine courier is hoping for a detour, launching an appeal of his conviction. Ronald Charles Learning was sentenced last month in a Regina courtroom to nine years in prison for possession of drugs for the purpose of trafficking. With credit for time already served, eight years and 204 days remained plus an additional 30 days was added to the sentence for breaching conditions of release. Leader-Post

Pemberton festival: Want to know how much fentanyl is in your ecstasy? Drug tests won't help
Party people are heading in droves to Pemberton Music Festival this weekend, and it's a truth acknowledged that some will be on a chemically fuelled trip, Hunter S. Thompson style. But given B.C.'s fentanyl crisis, provincial health officer Dr. Perry Kendall is warning festival enthusiasts that mixing drugs could be fatal. He said health officials still don't know how much fentanyl — or worse, W-18 — is added to some recreational party drugs like ecstasy, cocaine and speed. Vancouver Sun

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

First Nations chiefs urge holdout provinces, Ottawa to stop 'dragging feet' on MMIW inquiry
First Nations chiefs expressed growing frustration with a delay in the federal government's launch of a national inquiry into missing and murdered Indigenous women, calling on both the provinces and Ottawa to stop dragging their feet, during a third and final day of an annual general assembly meeting in Niagara Falls, Ont. The delay comes as two provinces, including Manitoba, continue to negotiate with the federal government over the terms of reference that would help determine the focus and scope of a national inquiry. It's unclear which other province is still negotiating. CBC News

Broadcast Media / Médias télédiffusés :

CBC News' Power & Politics interviewed Manitoba Justice Minister Heather Stefanson regarding that province's stance into the inquiry of missing and murdered indigenous women. Rough Transcript

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Pot dispensary shuttered
The operator of a medical marijuana dispensary in Penticton has closed his doors for now, after the city issued a notice of non-occupancy Wednesday. Mayor Andrew Jakubeit said Herbal Greens Apothecary was given the notice to cease operation as the city is currently suspending the business licence and have scheduled a hearing for operator Jukka Laurio. Castanet.net

PUBLIC SERVICE / FONCTION PUBLIQUE

Les employeurs ne peuvent congédier sans motif, statue la Cour suprême
La Cour suprême du Canada statue qu'une compagnie sous réglementation fédérale ne peut congédier sans motif valable un employé qui n'est pas protégé par un syndicat. Dans son arrêt rendu jeudi, le plus haut tribunal du pays indique que cette pratique est injuste et, par conséquent, viole le Code canadien du travail. Presse Canadienne (La Presse) ; Canadian Press (Times Colonist)

OTHER / AUTRES

NIL

INTERNATIONAL

Attentat à Nice: la préfecture demande aux habitants de rester cloîtrés
Un camion a foncé jeudi soir dans la foule sur la Promenade des Anglais à Nice pendant le feu d'artifice du 14 juillet, faisant plusieurs victimes selon la mairie et des témoins sur place. La préfecture des Alpes-Maritimes évoque un attentat et demande aux habitants de rester cloîtrés. Le président de la métropole Nice Côte d'Azur, Christian Estrosi, a évoqué sur Twitter des dizaines de victimes. Vers 23H20, un important périmètre de sécurité était délimité à proximité, autour de la place Masséna. "Les gens courent, c'est la panique. Il est monté sur la Prom et il a foncé sur tout le monde" explique notre collègue. "Il y a du monde en sang, sans doute plein de blessés", explique un journaliste de Nice Matin présent sur place. Le Figaro

Au moins 73 morts dans un attentat à Nice
La scène s'est produite sur la promenade des Anglais, sur une distance de deux kilomètres, près notamment de l'hôtel Negresco, en fin de soirée après le feu d'artifice. Un témoin a affirmé avoir vu un chauffeur de camion foncer dans une foule de fêtards avec son véhicule et puis sortir en tirant avec une arme à feu, tuant plusieurs personnes. Un autre a dit: « Il y avait des mouvements de foule de partout. Moi je me trouvais devant un lieu d'animation. Des centaines de personnes se sont mises à courir dans tous les sens. On pensait à une alerte à la bombe. (...) Beaucoup de gens tapaient aux portes pour se réfugier dans les maisons. Des scènes de terreur. » Radio-Canada

Kenya police officer 'goes berserk,' kills 7 colleagues
A Kenyan police officer went on a shooting spree Thursday, killing seven colleagues including a hostage response team member before the standoff ended in a shootout, a police report said. The suspect, Abdihakim Maslah, was shot, said the report provided to The Associated Press. Associated Press (Hamilton Spectator, ABC News)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

CreesonCTV
@RalphGoodale's staff met with the rally. They said they will send their messages to Mr. Goodale.

JessieAntonCTV
Goodale's office claims they were unaware of CNM's detained immigrant protest & did not receive any CNM emails. #yqr

JessieAntonCTV
Colonialism No More advocates protest Canada's detained immigrants outside @RalphGoodale headquarters. #yqr

CreesonCTV
CNM is gathering in front of @RalphGoodale's office. They want him to meet with the people that are detained by CBSA

CAMWL
Art by hunger striking detainee. @RalphGoodale, when will you meet w them? End indefinite detention #migrantstrike

nooneisillegal
Please share powerful self-portrait & poem from R.R. in immigration detention on day 4 #migrantstrike @RalphGoodale

LINCSocietyBC
Emma's Acres: An Agricultural Social Enterprise that funds Victims.. @RalphGoodale @JustinTrudeau @Don_Head_CSC thx

LINCSocietyBC
Emma's Acres: Inmates and victims growing food in Mission BC - Vancity vancity.com/AboutVancity/I... @RalphGoodale @JustinTrudeau thx Don_Head_CSC

LINCSocietyBC
My Vision of Restorative Justice by Glen Flett @lincsociety lincsociety.bc.ca/community-gard... @RalphGoodale thx for the support @Don_Head_CSC

LINCSocietyBC
@Don_Head_CSC @RalphGoodale @JustinTrudeau We appreciate the support of the CSC for the work we do at Emma's Acres.

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

CBCMontreal
Summer storm causes damage and power outages in Quebec ift.tt/29yNrcx pic.twitter.com/6rElQ4ZubE

NATIONAL SECURITY / SÉCURITÉ NATIONALE

itworldca
Whistleblower Edward Snowden to keynote Toronto conference bit.ly/29VVa25

BORDER SECURITY / SÉCURITÉ FRONATLIÈRE

triadonaldson
Happening now in Regina: solidarity picket with migrant detainees. #ygr #skpoli #migrantstrike #cdenpoli

LAW ENFORCEMENT / APPLICATION DE LA LOI

CBC_Aboriginal
Nunavut RCMP chief says boosting Inuit recruitment will take 'many generations' http://ift.tt/29KRlyR

CBC_Aboriginal
Police diversity fails to keep pace with Canadian populations http://ift.tt/29Umu0S

NEWS957
RCMP apologizes over harassment episode, promises national effort news957.com/2016/07/14/rcm…

CBCNorth
RCMP say problems with phone lines continuing in N.W.T. cbc.ca/news/canada/no…

CastanetNews
RCMP: iTunes tax scam #VernonBC bit.ly/29MCwe6

ctvedmonton
RCMP investigating reports surrounding use of counterfeit bills, searching for two suspects: edmonton.ctvnews.ca/rcmp-investiga… pic.twitter.com/w19RJgAqdH

GlobalBC
Surrey RCMP searching for SUV involved in targeted shooting glbn.ca/l50lvJ

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

CBC_Aboriginal
Ex-priest Eric Dejaeger denied Nunavut legal aid in appeal of child sex convictions ift.tt/29zTUjJ pic.twitter.com/3l9ylTkCxp

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

AM980News
A high risk sex offender has been released into #LdnOnt, police warn bit.ly/29LddKr

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

CBC_Aboriginal
First Nations chiefs urge holdout provinces, Ottawa to stop 'dragging feet' on MMIW inquiry http://ift.tt/29Ggnkh

INTERNATIONAL

p_pradal
Il s'agit du pire drame de l'histoire de Nice car plus de 70 victimes sont déjà à déplorer.

p_pradal
Nous sommes terrifiés et nous voulons présenter à toutes les familles concernées nos sincères condoléances. #Nice06

Nice_Matin
Le conducteur du camion aurait été abattu selon le sous-préfet #AttentatNice

CanadaPE
Nous suivons les événements à #Nice, en #France. Nos pensées sont avec les morts et les blessés lors des célébrations de la Fête nationale.

CanadaFP
We are monitoring events unfolding in #Nice #France. Our thoughts are with those killed and injured while celebrating #BastilleDay/hashtag/BastilleDay?src=hash/hashtag/BastilleDay?src=hash.

Reuters
Many dead after truck plows into Bastille Day crowd in Nice, gunshots heard: media

CTVVancouver
#Breaking: At least 30 dead after truck rams crowd in France: Reuters. Being treated as an attack.

business
DEVELOPING: Fatalities have been reported after a truck rams into crowd in Nice, France

globeandmail
#Breaking: Dozens reported killed after truck plows into crowd in Nice, France

FoxNews
French TV: At least 30 people dead, more than 100 injured. #Nice, #France. #BastilleDay

CNN
Just in: Several people killed when a truck ran into a crowd in Nice, France, the mayor says http://cnn.it/29MAT02

cestrosi
Cher niçois, le chauffeur d'un camion semble avoir fait des dizaines de morts. Restez pour le moment à votre domicile. Plus d'infos à venir

Nice_Matin
Les taxis niçois prennent tout le monde en charge gratuitement pour les évacuer de la Promenade des Anglais #AttaquesNice
18:00 - 14 Juil 2016

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

Today's News / Actualités
July 15, 2016 / le 15 juillet 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

PM Trudeau says Canada will work to fight terrorism
Prime Minister Justin Trudeau says Canada is thinking of "our friends in France" and will work to fight terrorism. "We had a terrible attack last night and our hearts go out to the victims and their families," Trudeau said Friday while in Calgary to attend the Stampede. "Canada stands with France as a steadfast ally and we will work with the international community to fight terror to ensure that we live in a peaceful world. "At least 84 people were killed when a truck full of weapons plowed into a crowd of Bastille Day revellers in the French resort city of Nice late Thursday. There were no reports of Canadian casualties. **Public Safety Minister Ralph Goodale** said the federal government has no information that would necessitate a change in Canada's terror threat level, which is currently at medium. Still, **Goodale** urged Canadians to stay vigilant and alert. ***"Canadians can rest assured that when the security and intelligence sector receives credible warnings on a specific threat, they work with the appropriate***

government partners to ensure the safety of Canadians," **Goodale** said in a statement. **Goodale** noted that while in Paris in January, he signed a declaration with his French counterpart, Bernard Cazeneuve, to work together on terrorism, organized crime and irregular migration. The Canadian Press (CTV News); iPolitics

Broadcast Media / Médias télédiffusés:

At the Lindsay Detention Centre and the Toronto East Detention Centre 60 immigration detainees in two max security jails on hunger strike since Monday to protest prison conditions and the use of solitary confinement. Immigration detainees are asking for a meeting with **Public Safety Minister Ralph Goodale** to discuss their concerns. A Goodale spokesperson says the minister hopes to put forward proposals later this year. (Vancouver Co-op Radio, 7:27)

For months, protesters have been plugging away peacefully but today, Colonialism No More moved their message from their tents to the offices of **Ralph Goodale**. The group wants **Goodale** to meet with more than sixty immigrants who are being detained in maximum security prisons. (CTV Regina, 8:02)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

200 from Red Earth Cree Nation evacuated to Saskatoon due to flooding
About 200 people from Red Earth First Nation in northeast Saskatchewan are in a Saskatoon evacuation centre and hotel after getting forced out by rising water levels along the Carrot River. The evacuees, who are considered "health priority" individuals, are at the Henk Ruys Soccer Centre, and a hotel. Some people arrived last night around midnight. This is not the first time the community has been evacuated to Saskatoon. Last year, smoke from forest fires drove families south. Hendrick Head arrived last night along with his wife and daughters. He said that he has learned a few tricks about packing over the years. Of course, the family packs medications, clothes and identification. Sleeping on cots in an evacuation centre presents its own challenges. "We got a little bit of wisdom now," Head said. "We kept a bag of extra pillows, extra blankets and some mattresses." CBC News

Minister Jim Reiter to tour flooded Sask. communities of Arborfield and Carrot River
Saskatchewan's Emergency Management Minister Jim Reiter will tour Arborfield and Carrot River on Thursday to meet with local officials after heavy flooding devastated homes. Reiter and Carrot River MLA Fred Bradshaw will attend meetings with the mayor and deputy reeve of Arborfield, before travelling to Carrot River to do the same. The minister also announced on Thursday that a flood recovery centre would be set up in Arborfield from July 17-19. The centre will offer advice for residents of the Rural Municipality of Moose Range, the Town and RM of Arborfield and the Town of Carrot River. Workers from the Provincial Disaster Assistance Program will be stationed at the centre to help affected resident make claims, and a building official will be available to answer questions about structural safety and building concerns. CBC News

Relief centre helps flood victims
Estevan residents who suffered losses during the severe thunderstorm and the subsequent flood on July 10 have been able to turn to the Canadian Red Cross for support. The Red Cross set up a flood relief centre at the Civic Auditorium on July 11. Flood victims have been able to discuss their damaged homes, ask questions to volunteers and pick up a disaster relief kit. "Each household is able to have a cleanup kit," said Kathy Undseth, a volunteer with the Canadian Red Cross who came from Regina to help local residents. Most of the volunteers' time has been dedicated to helping people who have questions about damage to their homes, but they also had to handle a couple families who had to flee their homes due to the damage, and had to find hotel rooms. Estevan Mercury

Canada's new $14.1M fixed-wing drones are runway free
The Department of National Defence (DND) has purchased five new unmanned aircraft designed to take off, surveil an airspace and land without needing a runway. It's an easy task for a helicopter, but tougher

for a fixed-wing plane. For overhead surveillance, fixed-wing planes can usually fly higher, farther and remain airborne longer than their helicopter cousins. But most planes need long, straight, flat spaces for both takeoff and landing, and runways are not always located where military officials need them. The Canadian government has purchased one system, which includes five of the aircraft, from the United States Navy for $14.1 million, according to documents posted online earlier this week (…) The Blackjack drone is designed for surveillance purposes only, with its promotional material stating it offers "imagers, communication and signals intelligence capabilities and other tools to help give the warfighter a look ahead in all operational environments." CBC News

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Toronto man arrested on suspicion he'd travel and engage in terrorism agrees to peace bond
A Toronto man arrested over police concerns he would travel abroad to engage in terrorism agreed Friday to the terms of a one-year peace bond that requires him not to communicate or associate with ISIL. At a court appearance in Brampton, Kadir Abdul, 27, signed a peace bond that the RCMP had sought against him after he was arrested at Pearson airport on April 15 upon returning from Turkey, where he had allegedly been detained. The peace bond restricts him from leaving Ontario. He cannot possess a passport or weapons. He must also stay off the Internet, except under supervision. It further says he cannot "associate or communicate" with ISIL, Jabhat Al-Nusra or Samuel Aviles. Federal and defence lawyers worked out the terms in meetings Friday morning, and Abdul agreed to abide by them at a subsequent appearance before the Ontario Court of Justice. "I don't want to say anything," Abdul said following the proceedings. National Post

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Police make arrest after four sex assaults in Toronto and Vaughan
A 30-year-old Toronto man has been arrested and charged in connection with a brazen daylight sexual assault in Vaughan and three similar random attacks in Toronto. (…) A suspect identified as Le Roi Wisdom Saul was detained by Canadian Border Services agents on July 7, as he re-entered Canada at the Ambassador Bridge in Windsor, Ont. He has since been charged with a total of four counts of sexual assault and one count of criminal harassment. CP24; York Region

Pedestrian Ferry 'Extremely Unlikely' In September
A passenger ferry between Windsor and Detroit appears to be in rough waters as U.S. customs officials say it's "extremely unlikely" to happen in September. Earlier this month BlackburnNews.com first told you about a pedestrian ferry pilot project that's in the works, spearheaded by a group in Detroit. Organizers of the Open Streets Festivals in both Windsor and Detroit this September were hoping to have the service operational. (…). customs says there is no current agreement that would allow Canadian border officers to process passengers in the U.S. Some have suggested the Detroit Port Authority building be used as the designated spot for visitors to be cleared. But the CBP remains firm that "there is not a completed building on the U.S. side." The Canada Border Services Agency also says it has not received any formal application for a new ferry service. An appropriate facility to question, detain and process the public is something the CBSA requires before it can proceed. It's also the operator's responsibility to front the fees where a CBSA service didn't previously exist. Black Burn News

Nannies in Canada warned against working 'under-the-table' jobs
Canada's border services authorities are warning caregivers that they would face consequences for violating immigration laws, notwithstanding the abusive situations they may find themselves in. The Canada Border Services Agency (CBSA) urges caregivers to lodge complaints against their employers before Canada's immigration ministry if they feel abused, instead of accepting "under-the-table" jobs as "Band-Aid" solutions to their employment problems. Caregivers face being sent home the like the 19 caregivers who recently suffered the consequence following tips and complaints and subsequent investigations by the border services agency. Inquirer .net

Windsor-Essex ranked fifth among most affordable communities to do business
The Windsor and Essex County region has ranked as the fifth most affordable municipality to do business in Canada in the second annual ranking of municipalities in Canada's Best Places to do Business by Canadian Business and PROFIT magazines. The region came in 25(th) in the overall survey of municipalities. "It's an honour to be recognized nationally as one of Canada's best places to do business," said Rakesh Naidu, interim CEO of the WindsorEssex Economic Development Corporation. (…) The survey said the following about the region's economic initiatives: "Windsor is connected directly to the U.S. border and already handles one-third of all Canada-U.S. trade. The Gordie Howe International Bridge, when it opens in 2020, will increase that capacity further. Fiat Chrysler has invested $2 billion in retooling its Windsor auto assembly plant." Windsor Star

Does Mobile Passport Eliminate the Need for Global Entry?
Nothing ruins the memory of a great international vacation or a successful business trip than landing in the U.S. and having to wait in a long Customs and Border Protection (CBP) queue. There's a solution — no, not Global Entry— and it's also free. Meet Mobile Passport. Mobile Passport is a smartphone app that makes Customs clearance quick and painless. And the best thing about it is that it's completely free, unlike Global Entry. (…) Almost everyone has a smartphone these days, so it's surprising that so few people know about this. You are still required to possess and travel with your valid U.S. or Canadian Passport to use the app. Travel Pulse

The Incredible Complications of Living Atop the U.S.-Canada Border
An opinion piece states " Estcourt Station is a smudge of a village that straddles the Maine-Quebec border at the northernmost tip of the state. Although it's technically in Maine, you can't get there by way of American roads. At least not easily. (…)When visiting Estcourt Station recently, I spied a bank of mailboxes with the familiar insignia of the U.S. Postal Service and drove toward it. But then a Canadian customs agent on foot seemed to materialize from nowhere, and approached my slow-moving car. (…)The Canadian-U.S. border runs right across his back deck. If he's going to grill, his burgers would be flame-broiled in the U.S." Atlas

Broadcast Media / Médias télédiffusés:

Families of children with epilepsy are demanding help from the federal government after CBSA seized "Charlotte's Web" hemp oil shipments at the border. (CTV Saskatoon, 6:22, 8:10)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Almost Any Messaging App Will Do—If You're ISIS
On July 1, five Islamic State fighters stormed the Holey Artisan Bakery in Bangladesh's capital, Dhaka, ultimately claiming 28 lives in a 12-hour siege. Before IS (ISIS, or Daesh) officially released the claim, the group's 'Amaq News Agency released ongoing updates from inside the restaurant through its Telegram channel. The first message stated that IS "commandos" attacked the restaurant, which was "frequented by foreigners," and an update minutes later reported that over "20 people of different nationalities [were] killed." 'Amaq then increased the number of casualties to 24 with 40 wounded, and followed up with photos of the bloody scene inside the restaurant. It was clear that this direct, uninterrupted communication the attackers had with 'Amaq was facilitated by a smartphone app. Five days later, The Times of India reported that the app was Threema, an end-to-end encrypted messaging service. This reported confirmation of yet another messaging app used in a terror attack echoed other reports from this past year. The Paris attackers are known to have communicated with WhatsApp and Telegram apps prior to their operations on November 13, 2015. Najim Laachraoui, the bomb maker and co-attacker in the March 22, 2016 Brussels attacks, reportedly used Telegram, while fugitives connected to the aforementioned Paris attacks used WhatsApp, the mobile app Viber, and even Skype to talk to IS leaders in Syria before authorities located them. Motherboard

US Cyber Mission Force Nearly Ready for Action
The US military's Cyber Mission Force will finally be ready for action by the end of September, according

to US Cyber Command and NSA boss, Admiral Michael Rogers. The new elite cyber force will eventually contain over 6000 operatives split into 133 groups, which will be tasked with both offensive and defensive missions. Unusually for a military endeavor, troops will be deployed before the unit has been completely staffed, Rogers told a National Press Club gathering attended by NPR. "We find ourselves in a situation a little unusual in the military arena. As soon as we get a basic framework, we are deploying the teams and putting them against challenges," he's reported as saying (…) The force, which apparently features military personnel alongside civilians, is estimated to finally be ready on 30 September 2018. Last month Air Force Brig. Gen. Charles L. Moore Jr. told the House Armed Services Committee that the Cyber Mission Force has already encountered a few challenges relating to equipment, training, recruitment and "finalizing the command-and-control structure." Infosecurity Magazine

Here's What We Know About the NSA's Elite Hacking Squad
Some of the best hackers in the world work for the NSA. They are the ones who are tasked with hacking into the most—supposedly—impenetrable targets, be it the computers of an Iranian nuclear power facility, or the cellphones of a fugitive terrorist. As far as anyone knows, they don't have a cool sounding name, but they are collectively known as "The Office of Tailored Access Operations," or TAO. They have been called "a squad of plumbers that can be called in when normal access to a target is blocked." And while that name, and that description, might sound underwhelming, they're the NSA's elite-hacking unit, its black bag operations team. Very little is known about TAO, but most of what we know today comes from documents leaked by the former NSA contractor Edward Snowden. To learn more about them, and as part of CYBERWAR, VICELAND's ongoing series on hacking, we travelled to Berlin and London to talk to the journalists who have investigated these sophisticated government hackers in the last few years. Motherboard

LAW ENFORCEMENT / APPLICATION DE LA LOI

Man Charged in Killings of Mother, Abducted 5-Year-Old Girl After Authorities Find Child's Body
A desperate search for a little girl abducted after her mother's murdered in their Canada home has come to a devastating end as law enforcement officials announced they found a body believed to be the missing 5-year-old child. Calgary Police say they found a body they believe is Taliyah Leigh Marsman on a rural property east of Chestermere on Thursday, bringing the three-day search for the little girl to a tragic end. Inside Edition

'I was just reading a book': Canadian cops called on black man reading C.S. Lewis in his car
After the blue and red police lights flashed behind his car, Louizandre Dauphin figured he may have added another "prohibited" item to the list of things you can't do while black: Reading. Dauphin, 33, a former high school English teacher, had decided to relax last week with a few books at Stonehaven Wharf, a parking lot for fishing boats that's frequented by tourists to the Canadian province of New Brunswick. He sat inside his Volkswagen Golf hatchback watching the waves and poring over "Mere Christianity" by C.S. Lewis and another book by theologian Timothy Keller. As he drove home afterward, Dauphin recounted on Instagram, an officer with the Royal Canadian Mounted Police pulled him over, saying someone nearby had called authorities "because . . . a suspicious black man in a white car was parked at the Wharf for a couple hours. My response, Really? I was just reading a book." Cortez Journal

Canada's criminal courts get an F, cops a C+ in public confidence: poll
Technically, a 50.5 per cent test score is a passing grade. But would you consider that a good enough average mark for your country's justice system? That's the average level of Canadians' confidence in our courts, according to new Angus Reid Institute opinion poll. Provincial criminal courts in particular lagged with a mere 44 per cent of public confidence. "When you have numbers close to half or below 50 to 60 per cent, that would give rise to raised eyebrows," said the institute's executive director, Shachi Kurl, in a phone interview. "It also speaks to a sense of, 'Do we feel safe in our communities, well-protected, and have access to fairness in this country?'" However, Kurl said there are two more positive findings of this year's survey that outshine the negatives. For one, the results have actually improved dramatically over time for both police and courts — particularly compared to 2012, in some cases nearly doubling in confidence since the institute's first justice survey. "Prior to 2012 … our institutions related to justice were

not necessarily inspiring a lot of confidence in Canadians," she explained, citing the botched investigation of serial killer Robert Pickton and the tasering death of Polish immigrant Robert Dziekanski in Vancouver airport. "There's been a notable and significant improvement since." Secondly, police fared better than the courts: our national force, the RCMP, earned the equivalent of a C+ grade, with 66 per cent public confidence. Provincial police were most supported with 70 per cent, or a B-. Municipal police and local detachments, 65 per cent. Metro News

Quebec police forces have best representation of women in Canada
Quebec's major police forces have among the highest proportions of female officers in the country, a CBC News analysis has found. Leading the country is the Montreal Police Service, where nearly 32 per cent of its sworn officers are women. At the tail end for major cities is the Winnipeg Police Service, where the proportion is less than half of Montreal`s at just under 15 per cent. Of the 332 RCMP officers in Nunavut and the Northwest Territories, less than 11 per cent are women. CBC News

Federal prosecutors get 7 requests to verify evidence in Halifax drug cases
Federal prosecutors in Halifax have received requests to verify evidence in seven separate drug cases, after an internal audit by Halifax Regional Police found widespread disarray in its secure drug and money vaults. The chief federal prosecutor in Atlantic Canada says the Public Prosecution Service of Canada has forwarded the defence requests to police. "We have one answer back, indicating there's no issue with respect to the exhibits on that particular file," said Anne Marie Simmons. "We await an answer with respect to the remaining six files." Simmons says the request come from three defence lawyers. Halifax lawyer Stan MacDonald says he's one of them, but he won't give further details to protect his clients' confidentiality. CBC News

Broadcast Media / Médias télédiffusés:

CTV News presented the live press conference of independent senator Patrick Brazeau, who is returning to the Senate after all charges against him have been withdrawn. Rough Transcript (2016-07-14)

Racism exists within his police force Bob Paulson signed a protocol agreement with the Assembly of First Nations this week he says that involves increasing the number of aboriginal police officers and tackling racism. (CKTG-FM, 12:03)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

ROPE Squad searching for missing offender
The Repeat Offender Parole Enforcement (ROPE) Squad is searching for a federal offender after they say he failed to returned to his community residence in Kingston on Monday. Thomas Campbell is currently serving a six-year, two-month sentence for break and enter, theft over $5,000 and theft under $5,000 said a news release. Campbell is known to frequent Kingston and the Greater Toronto Area. Campbell, 55, is described as a five-foot-eight-inches tall,150 lb Aboriginal man. He has scars on his left hand and right wrist with a tattoo of a wizard on his right upper arm, an eagle on his right forearm, and a skull on his left forearm. Kingston Whig-Standard; Quinte News; Kingston Region

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Black Lives Matter & Police: What's real for a young, black man from Hamilton
Black lives matter. Three simple words. But rarely has there been such a divisive statement splashed over what feels like the entirety of the Internet. It has been adopted as an impassioned rallying cry for some, while met with eye rolls and vitriol from others. In the wake of multiple police shootings of black men in the U.S., five police officers gunned down in Dallas, and Toronto's Pride parade halted in protest, there's no way to ignore the conversation. Professional dancer Rodney Diverlus, 26, is the co-founder of

Black Lives Matter Toronto. He went to high school in Hamilton, and his family still lives in the city. CBC News reached him in New York City to talk about his experiences as a black man, the violence he's seeing in the world, and why Black Lives Matter interrupted the Toronto Pride Parade to protest. CBC News

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Pot shop owner says he will sell marijuana without prescriptions
Dana Larsen says his dispensaries' two locations will sell marijuana to anyone, even if they don't have a medical prescription. The well-known marijuana campaigner, and director of the Vancouver Dispensary Society, says with legalization on the way, it's time to move forward. "I think it's the right time," said Larsen. "I see us selling medical marijuana as a non-prescription drug, similar to aspirin and things like that." (...)The federal government has announced it will introduce legislation for legalization next spring. But that hasn't stopped the City of Vancouver from attempting its own measures to control the sale of marijuana. It's created a set of bylaws for marijuana-related businesses. So far, only two businesses have received a license. CBC News

PUBLIC SERVICE / FONCTION PUBLIQUE

Broadcast Media / Médias télédiffusés:

A single mother who works for the federal government shares her story about not getting paid under the new payroll system. (CBC R1 Ottawa, 7:15)

OTHER / AUTRES

Nanaimo students in Nice safe but some 'stressed' after witnessing attack, says school official
Nanaimo school officials say its students and chaperones are safe in Nice, France but they are now watching for signs of trauma after some from the group witnessed the deadly attack.
Dale Burgos, director of communications at the Nanaimo-Ladysmith School District, said he's been told some students were less than 30 metres away from the scene of the incident. (...) About 85 students and 12 adult chaperones from the Nanaimo area were on a school-related trip to Nice, where a terrorist attack during Bastille Day celebrations killed at least 84 people and injured many more. CBC News

"The French will remain resilient"
Raffelina Sirianni-Smith had been in Nice, France since Monday and had watched revellers from her balcony daily, flocking to the Promenade des Anglais for nightly celebrations. She was unsure about the crowds, which is why she decided to visit a relative in Monte Carlo Thursday evening to enjoy the Bastille Day fireworks. "We were a little uneasy about it - which sounds ridiculous but you have to consider that when you travel now - so we went to see my cousin in Monte Carlo," the former Kamloops journalist told Postmedia News. After spending the evening in Monte Carlo, Sirianni-Smith and her travelling companion were driven back to their AirBnB apartment, located on the Promenade, but were unable to get through due to road closures. The pair walked back to their apartment and once they were able to access a wifi connection, the news started pouring in. Just 10 minutes earlier, a truck had driven onto the sidewalk and through a crowd of Bastille Day revellers, including a number of families and children, who had gathered

to enjoy the fireworks. As of Friday morning, at least 84 people were dead and 50 were still critical. Sirianni-Smith and her companion are located about a kilometer from the attack site and in the hours since the attack, Sirianni-Smith said all she could see was "a long line of emergency vehicles flashing" and helicopters overhead. Postmedia Network (Vancouver Sun)

INTERNATIONAL

'There was carnage on the road'
A large truck plowed through revellers gathered for Bastille Day fireworks in Nice, killing at least 84 people and sending others fleeing into the sea as it bore down for more than a mile along the Riviera city's famed waterfront promenade. The driver was killed by police and no one immediately claimed responsibility for the Thursday night attack on France's national holiday, which rocked a nation still dealing with the aftermath of two attacks in Paris last year that killed a total of 147 people. "Terrorism is a threat that weighs heavily upon France and will continue to weigh for a long time," Prime Minister Manuel Valls said after an emergency government meeting Friday. "We are facing a war that terrorism has brought to us. The goal of terrorists is to instill fear and panic. And France is a great country, and a great democracy that will not allow itself to be destabilized." The truck plowed into the crowd over a distance of two kilometres (about 1.2 miles), a lawmaker said, and broadcast footage showed a scene of horror up and down the promenade, with broken bodies splayed on the asphalt, some piled near one another, others bleeding onto the roadway or twisted into unnatural shapes. Some tried to escape into the water, Eric Ciotti, a lawmaker for the region that includes Nice said Friday, giving new details of the horrifying last minutes of the attack. Associated Press (Kingston Whig-Standard, Toronto Sun, Ottawa Sun, Winnipeg Sun, London Free Press, National Post, Calgary Sun

Les pays arabes, l'Iran et Israël condamnent l'attentat «terroriste» de Nice
Les pays arabes, l'Iran et Israël ont vivement condamné vendredi l'attentat qui a fait plus de 80 morts la veille à Nice et appelé à intensifier les efforts pour faire face au fléau du «terrorisme». Alors que l'auteur de l'attaque a été identifié comme un franco-tunisien, la Tunisie, victime ces dernières années d'attentats meurtriers, a dénoncé un acte «terroriste lâche» et «exprimé ses profondes condoléances à la France». Son président Béji Caïd Essebsi a appelé à la «solidarité» dans la lutte antiterroriste. (...)En Egypte, la plus haute institution de l'islam sunnite, Al-Azhar, a estimé que ces «attaques terroristes abominables contredisent les enseignements de l'islam» et souligné «la nécessité d'unir les efforts pour vaincre le terrorisme et débarrasser le monde de ce mal». Les six monarchies arabes du Golfe ont condamné l'attaque «terroriste». En Arabie saoudite, le roi Salmane a, dans un message de condoléances au président François Hollande, «affirmé la solidarité du royaume avec la France» et réitéré sa position «rejetant le terrorisme sous toutes ses formes» et la nécessité des efforts internationaux en vue de l'éradiquer». AFP (Journal de Montreal)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

Ralph Goodale
Have sent message to my French counterpart, Interior Minister Cazeneuve, expressing Canada's profound grief and absolute solidarity.

Ralph Goodale
J'ai écrit à mon collègue français, le ministre Cazeneuve, pour lui faire part de notre profond chagrin et solidarité.

Félix M.Beaulieu
#nice:Député de Regina-Wascana et min. de Séc. publique @RalphGoodale a communiqué avec son homologue français #rcsk

Rabble.ca
60+ immigration detainees are on hunger strike. Ralph Goodale refuses to meet with them. http://buff.ly/29Bzyaa #migrantstrike #cdnimm

620 CKRM
Protestors converge on MP Ralph Goodale's Regina office #yqr #SK http://bit.ly/29lJldO

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

CF Operations
#OpNUNAKPUT : Canadian Rangers and #RCNavy members did search and rescue drills near Yellowknife

Saskatoon Buzz
Cleanup underway from Saskatchewan flooding: Flood response has shifted to recovery mode in Saskatchewan…

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Stewart Bell
Toronto man arrested on terrorism peace bond agrees to have no contact with ISIL. http://natpo.st/29YSCQQ

Public Safety Canada
#FF to @CSISCanada &@CSE_CST, from an appropriate distance ;)

CSE_CST
@Safety_Canada @csiscanada We expect anything Public Safety does to be from a safe distance. #FF

BORDER SECURITY / SÉCURITÉ FRONATLIÈRE

No One Is Illegal
No answers as SIU washes hands off immigration detainee's death. ACT NOW: https://www.change.org/p/no-more-deaths-no-more-detentions … #MigrantStrike

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Kaspersky Lab
Encryption, Lockscreen, and MBR, oh my! Learn about different types of #ransomware https://kas.pr/ojj3

SC Magazine
New banking malware stops customers from cancelling payment cards

Infosecurity
CyberSecurity: How Artificial Intelligence Is Your New Best Friend

LAW ENFORCEMENT / APPLICATION DE LA LOI

Stewart Bell
A troubled Canadian, whom RCMP has been monitoring, reacts after Nice.

RCMP, Ontario
Peace Tower flag (Ottawa) at half-mast until sunset July 18 to mark the tragic events in Nice, France ^JT

Surrey RCMP
Our thoughts are with the people of Nice and all first responders. @PMdeNice

GRC de Surrey

Nos pensées accompagnent la population de Nice et les premiers intervenants @PMdeNice

RCMP
Need to register a firearm? Try our online tool. #CFPonline #RCMP http://rcmp.ca/-2qw

Bob Paulson
Bob Paulson is apologizing for "egregious behaviour" at the RCMP's explosives training unit
http://www.cbc.ca/1.3680145

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Correctional Service
Our Institutions are private property - playing PokémonGo there is trespassing. #PokémonGo

Servicecorrectionnel
Nos établissements sont des zones restreintes - jouer à #PokémonGo à ces endroit est une intrusion.

OTHER / AUTRES

David Akin
"Clarification: Two Canadians not among dead in Nice"

Lawrence Cannon
#NiceAttacks: no Canadians reported among casualties to date. Thanks to the French authorities for their cooperation

Lawrence Cannon
#NiceAttentat: aucun Canadien ne figure parmi les victimes pr l'instant. Merci aux autorités françaises de leur précieuse coopération

INTERNATIONAL

The National
Former CSIS Assistant Director Ray Boisvert examines the Bastille Day attack in Nice. http://www.cbc.ca/1.3680154

Mubin Shaikh
Well then. France attacker a drug-head, ate pork, did not observe Ramadan & never prayed. "Shariah" right?

Doug Saunders
Nice terrorist fits the consistent profile: Non-religious, wife-beating petty criminal; French citizen

NSPS (CBoC)
The Global Reach of #Terrorism: Reflections on the Attacks in #Paris, Beirut, and Baghdad
http://www.conferenceboard.ca/topics/security-safety/commentaries/15-11-18/the_global_reach_of_terrorism_reflections_on_the_attacks_in_paris_beirut_and_baghdad.aspx?utm_source=twitter&utm_medium=social&utm_campaign=kbtweet … #lesm #natsec

Amarnath Amarasingam
If you're wondering how AQ and ISIS differ in target selection & tactics, read series of tweets by @thomasjoscelyn.

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

Today's News / Actualités
July 15, 2016 / le 15 juillet 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

NATIONAL AFFAIRS: Reports could hide true police activity
An opinion piece states, "Clear gaps" in how the federal government reports invasive surveillance practices may hide the true scope of police activities, according to documents prepared for Canada's privacy watchdog. Although the number of authorized wiretaps has "plummeted" since 2002, a January briefing for Privacy Commissioner Daniel Therrien suggests those numbers may mask police surveillance practices. "It would be erroneous to infer from the drop in overall warrants issued that surveillance is affecting fewer individuals," reads the document, obtained under access to information law. "While federal authorities issued just over a hundred surveillance warrants last year (2014), they issued 792 notifications of surveillance to individuals previously targeted. From this, one can conclude more and more individuals are being named as targets in a warrant application... **Public Safety** is required to issue a report each year about the number of warrants sought to put individuals under surveillance - "wiretap" warrants that

allow police extraordinary powers to keep tabs on individuals... The Star requested an interview with both Therrien and **Public Safety Minister Ralph Goodale** for this article. Neither was available Wednesday or Thursday. But in an emailed response to the Star, **a spokesman for Goodale said the minister** is open to changing the system. ***"Reporting is an important component of Canada's system accountability for security agencies," Scott Bardsley wrote. "We're open to consideration in this review (of national security oversight) of how to improve these elements to better achieve our two objectives (of) ensuring that our police and security agencies are being effective ... and safeguarding the values, rights and freedoms of Canadians in a plural, open, democratic society."*** Lisa Austin, a law professor at the University of Toronto specializing in privacy issues, said calls globally for transparency about police surveillance have increased, not just for wiretap warrants, but for any extraordinary powers for law enforcement snooping..." Chronicle Herald

(UPDATE) First Nations call on feds, Ontario to hash out deal as police strike looms

First Nations leaders and a northern Ontario MP say police officers' lives are on the line and they want the federal government and the province to negotiate a new policing agreement with Nishnawbe-Aski Police Service. The force services 35 First Nations communities in northern Ontario and currently faces a strike deadline as a result of a vote earlier this week. Two of the central issues include the call for increased staffing and wage parity. Alvin Fiddler, the grand chief of Nishnawbe-Aski Nation, said First Nations have raised concerns about dangerous conditions for officers for two decades. "We cannot keep going the way that we have been operating," Fiddler said... Officers are rolling the dice when they go out in the field with a lack of resources such as a lack of backup, says New Democrat MP Charlie Angus... The complaint suggests disparity in services between aboriginal and non-aboriginal community stems from flaws in the federal government's First Nations Policing Program and funding regime. Resource struggles also impact the mental health of officers, said Sgt. Jason Storkson, a local union president with the Public Service Alliance of Canada. In a **statement** Friday, a **spokesman for Public Safety Minister Ralph Goodale** said the government is committed to making progress on community safety and policing for indigenous communities. At this stage of the engagement process, no decisions have been made on funding, expansion or other details of how the renewed approach to indigenous policing would be implemented, **said press secretary Scott Bardsley**. ***"In the event of a strike, the OPP would have to take over policing duties in the Nishnawbe-Aski community as it would fall under provincial jurisdiction," he said.*** Canadian Press (Brandon Sun)

Coroner's inquest called into immigration detainee Abdurahman Hassan's death at Peterborough Regional Health Centre

A coroner's inquest has been ordered into the June 11, 2015 death of a mentally ill diabetic Somali refugee at the Peterborough Regional Health Centre while he was in immigration detention at the Central East Correctional Centre in Lindsay. Abdurahman Hassan, 39, died at the hospital after a police escorted transfer from the provincial jail for medical treatment. The inquest is mandatory under the Coroners Act, according to a release issued Friday afternoon by Dr. Paul Dungey, the regional supervising coroner for the Ministry of Community Safety and Correctional Services' East Region office in Kingston... Hassan had been in Canadian Border Services Agency custody for more than three years... The End Immigration Detention Network watchdog group called on Immigration Minister **Ralph Goodale** this week to end indefinite immigration detentions. The group has posted an online petition at https://www.change.org/p/no-more-deaths-no-more-detentions. The group had also urged a coroner's inquest into Hassan's death last year. The End Immigration Detention Peterborough group is planning a rally on Monday from noon to 1 p.m. outside the constituency office of Democratic Institutions Minister and Peterborough-Kawartha MP Maryam Monsef at 417 Bethune St. in support of the hunger strike and to back up the call to end indefinite immigration detention. The protesters will be urging Monsef to take action to urge **Goodale** and the federal government to respond to the claims of the detainees on the hunger strike, according to a release. Peterborough Examiner

Edmonton student missing as Trudeau pledges solidarity with France following truck attack

Prime Minister Justin Trudeau made a pledge Friday that Canada will work with the global community to fight terrorism following a deadly truck attack in the French resort city of Nice — as an Edmonton university raised the grim spectre of a Canadian victim among the 84 dead. Edmonton's MacEwan University said Friday that five students and one faculty member were in the Mediterranean hotspot

participating in a program at the European Innovation Academy, but one of those students is missing... **Public Safety Minister Ralph Goodale said** the federal government has no information stemming from the attack that would necessitate a change in Canada's terror threat level, which is currently at medium. Still, **Goodale** urged Canadians to stay vigilant and alert. ***"Canadians can rest assured that when the security and intelligence sector receives credible warnings on a specific threat, they work with the appropriate government partners to ensure the safety of Canadians,"* he said** in a statement. A spokesman with a Vancouver Island school district said several students from the Nanaimo area were just metres from the site of the terrorist attack, but that all 85 teens are safe. Canadian Press (iPolitics)

Canadian politicians express solidarity with France after Nice attack; Goodale says threat level unchanged

Canadian politicians are joining the outpouring of international outrage and sympathy after a truck plowed through a Bastille Day crowd on the iconic seaside Promenade des Anglais in Nice, France Thursday night. At the Calgary Stampede Friday, Prime Minister Justin Trudeau said Canada is thinking of "our friends in France" and will work to fight terrorism. "We had a terrible attack last night and our hearts go out to the victims and their families," Trudeau said of the massacre of 84 people during the annual celebrations of the French Revolution. "Canada stands with France as a steadfast ally and we will work with the international community to fight terror to ensure that we live in a peaceful world." **Public Safety Minister Ralph Goodale** said Friday that the federal government has no information that would require a change in Canada's terror threat level, which is currently at medium. Still, **Goodale** urged Canadians to stay vigilant and alert. ***"Canadians can rest assured that when the security and intelligence sector receives credible warnings on a specific threat, they work with the appropriate government partners to ensure the safety of Canadians," Goodale*** said in a statement. French officials say that, in addition to those killed, at least 50 more people were injured in what is widely assumed to have been a terrorist attack, though no group has yet claimed responsibility for the carnage and the motive of the driver, who was killed by police, remains unknown. iPolitics; CBC News

Five ways Canada is trying to prevent the kind of attack that happened in France

Investigators are still trying to determine why a man drove into crowds celebrating Bastille Day in Nice, France, killing scores of people. But authorities have called it an undeniable act of terror. Here are five ways that Canada is trying to prevent this kind of attack on Canadian soil: Threat assessments: Federal agencies are constantly gauging possible threats to dignitaries, public events and symbolic sites. The Integrated Terrorism Assessment Centre draws on expertise from across the federal government to evaluate the intent and capability of terrorists to carry out attacks. The assessments go to members of the Canadian security community, provincial emergency authorities, first responders and the private sector. Individual agencies also produce specialized assessments. For instance, Transport Canada has looked at the threat to various modes of transportation including airliners, passenger trains and buses. A November 2014 assessment mentioned the possibility of a bus being used as a weapon in a large crowd setting. Counter-radicalization: **Public Safety Canada**, the RCMP and some municipal police forces actively work with communities to try to prevent young people from becoming radicalized and embracing violence. The Mounties also train first responders, investigate national security cases and help intervene in high-risk cases. The Liberals have promised to appoint a co-ordinator of community outreach and counter-radicalization to serve as a needed focal point for multi-agency efforts. An announcement is expected soon. Interventions: Once a suspect comes to their attention, authorities can use a range of tools. The Canadian Security Intelligence Service has power to disrupt a plot — for example by disabling the ignition of a suspect's truck or cancelling their airplane reservation. Police can ask a judge to have someone with information relevant to the investigation of a future terrorist act appear before a court and answer questions. They can also seek an order for the court appearance of someone who may carry out a terrorist attack. A judge then considers whether to impose restrictions. It is a crime to go abroad to receive terrorist training, take part in extremism or facilitate terrorism. Federal officials collaborate to deny issuance of a passport or revoke an existing one, preventing overseas travel. Terrorist listing: Any person or group on Canada's terrorist list may have their assets seized, and there are criminal penalties for assisting listed entities with the aim of helping them carry out extremist activities. In addition, foreign nationals or permanent residents found to be members become ineligible to enter Canada. National security review: **Public Safety Minister Ralph Goodale** plans to publish a discussion paper as early as

next month to begin an in-depth review of Canada's national-security system. **Goodale** says the goal is to examine policies, laws and procedures with the aim of ensuring both public safety and fundamental freedoms. A parliamentary committee is expected to hold hearings before the government tables any new legislation to rescind existing measures or introduce new ones. Canadian Press (Metro News, Winnipeg Free Press, Hamilton Spectator, News 1130)

Broadcast Media / Médias télédiffusés :

CTV News interviewed **Public Safety Minister Ralph Goodale** regarding the attack in Nice, France. Rough Transcript

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

200 from Red Earth Cree Nation evacuated to Saskatoon
About 200 people are being evacuated from Red Earth Cree Nation in northeast Saskatchewan in response to rising water levels along the Carrot River. The evacuees, who are considered "health priority" individuals, are being taken to the Henk Ruys Soccer Centre in Saskatoon. Some people arrived last night around midnight. Some of the evacuees will also be sheltered in local hotels, the provincial government said. Also struggling this week are people at Shoal Lake Cree Nation, which is just east of Red Earth. Rising water has covered some of the roads leading into the First Nation. Some people from the reserve who have medical conditions, or who are considered at high risk of health problems, have been evacuated to Prince Albert. CBC News

Severe weather watches and warnings blanket southern Alberta
Environment Canada is warning people in the Calgary area and around southern Alberta about a severe thunderstorm that could hammer the region early Friday afternoon. The watch for Calgary was issued at 11:43 a.m. just as dark clouds started to move east towards the city... Just before 1 p.m. Environment Canada also issued a tornado watch for Lethbridge, Taber, Milk River, Crowsnest Pass, Pincher Creek and Waterton Lakes National Park. Cardston, Fort Macleod and Magrath were added to the list about half an hour later. Global News

St. John's shipyard wins multi-million-dollar coast guard contract
A lucrative federal contract granted to a St. John's shipyard is expected to add dozens of jobs to the firm. Newdock has won a $3.6-million contract for repair and maintain the Samuel Risley, a Canadian Coast Guard Ship, the federal government said Friday. CBC News

Mississauga mosquitoes test positive for West Nile virus
Mississauga residents might want to load up on the bug spray this summer. Peel Region public health officials say that mosquitoes captured in a Mississauga trap this week tested positive for West Nile virus. CBC News

Storm's consequences could have been serious
An opinion piece states, "When I was driving up Two Mile Hill on Tuesday evening, I could see the storm coming, and it looked like a bad one (Star, July 13). We all have seen them before... The city fire department was on it very fast, and that shows great work by them. Then, when I went on Facebook, there were pictures of flooding in different places. Does the city have in place a rapid response team for this kind of flooding and other types of situations?... Fort Mac was a major mess from the May wildfire, and they were not prepared for what was to come. They will pay the price of $4 billion (so far), and 2,400 structures are gone. I will ask city council to order a complete evaluation of the fire and other potential dangers to the city of Whitehorse..." Daily Star

NATIONAL SECURITY / SÉCURITÉ NATIONALE

NIL

BORDER SECURITY / SÉCURITÉ FRONATLIÈRE

Gun smuggler caught at Aldergrove
A Florida man who tried to bring a loaded pistol through the Aldergrove border crossing has been convicted of smuggling. Joseph Buice, 66, pulled up to the border crossing on April 11 of this year, according to a Canada Border Services Agency announcement. Joseph Buice, 66, pulled up to the border crossing on April 11 of this year, according to a Canada Border Services Agency announcement. Langley Advance

Two men convicted of gun smuggling at Abbotsford border in separate incidents
Two men have been convicted of smuggling firearms at the Abbotsford-Huntingdon border crossing in separate incidents, in May of this year. Rodrick Hines, 32, of Sacramento, California was trying to enter Canada on May 4 when border agents decided to do a secondary examination of his vehicle, according to a statement from the Canadian Border Services Agency. Abby News

Special Investigation Unit clears Peterborough Police officer, OPP officer in immigration detainee's death at Peterborough Regional Health Centre
No charges are warranted against a Peterborough Police officer and an Ontario Provincial Police officer in the June 11, 2015 death of an immigration detainee at Peterborough Regional Health Centre, the Special Investigations Unit has concluded after a 13-month investigation. Abdurahman Hassan, 39, died at the hospital after a police escorted transfer for medical treatment from the Central East Correctional Centre in Lindsay. He had been in custody for more than three years awaiting deportation... The SIU investigation determined the following: •On June 10, 2015, subject officer 1 (with the Peterborough Police) and subject officer 2 (with the Ontario Provincial Police) accepted a paid duty assignment at the Peterborough Regional Health Centre. The duty entailed guarding a refugee claimant who was in the custody of the Canadian Border Services Agency and awaiting deportation. The 39-year-old man suffered from significant mental health issues, including schizophrenia and bipolar disorder. Peterborough Examiner

Arctic science cooperation agreement 'good for Canada': POLAR
An agreement on enhancing scientific cooperation among circumpolar countries and others interested in polar research signed in Ottawa last week by the representatives of all eight Arctic nations will benefit Canada's northern communities, says the president of Polar Knowledge Canada (POLAR). "I think this is good for Canada, it will assist us in creating more knowledge about Canada and it will be globally relevant knowledge about Canada," said David J. Scott. "And from the perspective of the organization that I have the privilege to lead, Polar Knowledge Canada, we really trying to ramp up the creation of new knowledge that is primarily intended to benefit the lives of northern Canadians."..."At the conclusion of the Ottawa round of discussions last week, we were very pleased that were able to come up with a text that addressed all of the important issues basically to the satisfaction of each of the negotiating teams," Scott said. "And it's now the responsibility of each of the countries to bring that back, check in with each country's respective authorities and approval system." In case of Canada that means checking with other federal agencies whose mandates are impacted by this agreement, including the Canadian Border Services Agency, because part of the agreement deals with facilitating the entry of foreign scientists who are coming to Canada to collaborate on science research, Scott said. RCI

Double booked: The library that's in two countries at the same time
Meet the library which is in two countries at the same time: Haskell Free Library and Opera House was deliberately built on the border between the USA and Canada. A black line is marked on the floor of the building to show where Derby Line, Vermont ends and Stanstead, Quebec begins – and vice versa. BT.com

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Almost Any Messaging App Will Do—If You're ISIS
On July 1, five Islamic State fighters stormed the Holey Artisan Bakery in Bangladesh's capital, Dhaka,

ultimately claiming 28 lives in a 12-hour siege. Before IS (ISIS, or Daesh) officially released the claim, the group's 'Amaq News Agency released ongoing updates from inside the restaurant through its Telegram channel. The first message stated that IS "commandos" attacked the restaurant, which was "frequented by foreigners," and an update minutes later reported that over "20 people of different nationalities [were] killed." 'Amaq then increased the number of casualties to 24 with 40 wounded, and followed up with photos of the bloody scene inside the restaurant. It was clear that this direct, uninterrupted communication the attackers had with 'Amaq was facilitated by a smartphone app. Five days later, The Times of India reported that the app was Threema, an end-to-end encrypted messaging service. This reported confirmation of yet another messaging app used in a terror attack echoed other reports from this past year. The Paris attackers are known to have communicated with WhatsApp and Telegram apps prior to their operations on November 13, 2015. Najim Laachraoui, the bomb maker and co-attacker in the March 22, 2016 Brussels attacks, reportedly used Telegram, while fugitives connected to the aforementioned Paris attacks used WhatsApp, the mobile app Viber, and even Skype to talk to IS leaders in Syria before authorities located them. Motherboard

US Cyber Mission Force Nearly Ready for Action

The US military's Cyber Mission Force will finally be ready for action by the end of September, according to US Cyber Command and NSA boss, Admiral Michael Rogers. The new elite cyber force will eventually contain over 6000 operatives split into 133 groups, which will be tasked with both offensive and defensive missions. Unusually for a military endeavor, troops will be deployed before the unit has been completely staffed, Rogers told a National Press Club gathering attended by NPR. "We find ourselves in a situation a little unusual in the military arena. As soon as we get a basic framework, we are deploying the teams and putting them against challenges," he's reported as saying (…) The force, which apparently features military personnel alongside civilians, is estimated to finally be ready on 30 September 2018. Last month Air Force Brig. Gen. Charles L. Moore Jr. told the House Armed Services Committee that the Cyber Mission Force has already encountered a few challenges relating to equipment, training, recruitment and "finalizing the command-and-control structure." Infosecurity Magazine

Here's What We Know About the NSA's Elite Hacking Squad

Some of the best hackers in the world work for the NSA. They are the ones who are tasked with hacking into the most—supposedly—impenetrable targets, be it the computers of an Iranian nuclear power facility, or the cellphones of a fugitive terrorist. As far as anyone knows, they don't have a cool sounding name, but they are collectively known as "The Office of Tailored Access Operations," or TAO. They have been called "a squad of plumbers that can be called in when normal access to a target is blocked." And while that name, and that description, might sound underwhelming, they're the NSA's elite-hacking unit, its black bag operations team. Very little is known about TAO, but most of what we know today comes from documents leaked by the former NSA contractor Edward Snowden. To learn more about them, and as part of CYBERWAR, VICELAND's ongoing series on hacking, we travelled to Berlin and London to talk to the journalists who have investigated these sophisticated government hackers in the last few years. Motherboard

LAW ENFORCEMENT / APPLICATION DE LA LOI

(UPDATE) RCMP didn't 'purge' public documents, the Mounties actually just had no idea where they were

The RCMP now says it didn't destroy access-to-information files, after all. It only thought it did. That's why it announced a "purge" of documents that never really happened. And the series of snafus built on itself until it appeared that the Mounties had even erased details of scores of access-to-information records — everything it had processed since the start of 2016. You may recall the details, described Friday morning by the Citizen. Someone had asked the RCMP for documents related to former prime minister Stephen Harper's 2012 trip to India. The 219 pages released by the RCMP gave details on the cost of flying three armoured limousines to and from India — more than $1 million. Once one person receives documents under the access laws, anyone can receive the same set of papers. The Citizen asked for this one — and got a letter from the RCMP access office saying the documents could not be found and "it is likely that any RCMP record that may have existed has been purged." The letter blamed rules from Library and

Archives Canada, though a check with Library and Archives showed that no such rules exist. Dirty dealings? Dark secrets? Political interference? Nope. Friday afternoon, an RCMP spokesman phoned, offering an apology, and the story of a tough week at the office that processes access-to-information requests. Snafu No. 1: "This was wrong from our part," he said. "What happened was that the (person) that checked for that file number checked our system and she could not find it in the system." Out went the letter saying the documents were probably destroyed. In fact, they do exist, and they will be sent out next week. But that isn't all. At the same time as the documents were reported as purged, the list of all RCMP access-to-information records from 2016 had disappeared off the federal Open Government website, which means the public can't see, or ask for, whatever is available. Ottawa Citizen

RCMP did nothing wrong in Peguis First Nation shooting death, review finds
RCMP who were on the scene when a Peguis First Nation man died during a shooting last fall did everything by the book, the Independent Investigation Unit (IIU) of Manitoba finds. RCMP from Fisher Branch and Peguis were both called Sept. 4, 2015, after reports of gunshots, two people injured and a vehicle in the ditch. Four officers arrived to find a third person, who was in the vehicle by himself at the time. He was heard talking and officers tried to communicate with him, RCMP said. Not long after, a gun went off inside the vehicle, RCMP said. CBC News; Winnipeg Sun

Nunavut RCMP struggle to get Inuit cadet program off the ground
Prospective Inuit police officers will have to wait a bit longer for a new year-long police foundations course aimed at improving Indigenous representation within Nunavut RCMP. The Inuit Cadet Development Program has been in the works for more than a year and has gotten support from senior management within the RCMP and territorial government. CBC News

Beaverbrook man facing charges after allegedly hitting RCMP car with vehicle
A 48-year-old man from Beaverbrook, N.S., is in custody after he allegedly struck an RCMP vehicle with his own Thursday afternoon. Nova Scotia RCMP say the incident happened around 1 p.m. on Princeport Road. The officer suffered minor injuries and was able to arrest the driver without incident. CTV News

400 marijuana plants seized at property near Gibbons
Two Sturgeon County residents are facing child endangerment and drug charges after an RCMP raid on a rural property northeast of Gibbons, Alta. A search of a rural property netted more than 400 marijuana plants and more than two kilograms of marijuana packaged for sale, plus cultivation equipment and some foreign currency, St. Albert RCMP said in a news release Friday. CBC News

Burnaby realtor has grow-op charges drop over court delays
A realtor who was charged after police raided a suspected grow-op at a home he owned in Burnaby has had his charges stayed due to an unreasonable delay in getting the case to trial. In February 2011, RCMP received a tip about a possible marijuana grow operation in a house at 7206 Braeside Dr. in Burnaby and began surveillance of the premises. Vancouver Sun

Halifax man arrested after police seize cocaine
Police arrested a 49-year-old man in Halifax Thursday after seizing contraband including 2.2 kg of cocaine. Officers executing a search warrant at the Ivanhoe St. residence found drug paraphernalia, 14.5 cases of contraband cigarettes and approximately $75,000. Khalid R. Mansour was arrested and charged with Trafficking in Cocaine, Possession of Cocaine for the Purpose of Trafficking and Possession of Proceeds of Crime... The RCMP were assisted by both Halifax Regional Police and Service Nova Scotia's audit and enforcement unit during this investigation. Chronicle Herald

Cocaine, cash & contraband tobacco seized by N.S. RCMP
Police say charges have been laid against a Halifax man following a six month investigation by RMCP and the Serious Organized Crime Unit. This week, RCMP executed a search warrant at a home on Ivanhoe Street where they seized 2.2 kilograms of cocaine, drug paraphernalia and 14 cases of contraband cigarettes. $75,000 in cash was also seized from the residence. Global News

RCMP Musical Ride comming to Virden
The Virden Community Chamber of Commerce (VCCC) presents the RCMP Musical Ride, Thursday, July 14 at the Agricultural Society Fairgrounds. This will be their first time in Virden since 1978. This event will bring in people from all across We s t m a n and parts of Eastern Saskatchewan. Virden Empire-Advance

Bonavista RCMP officer awarded Sovereign's Medal for Volunteers
Bonavista RCMP officer, Const. Justin Lyall says he was shocked when he found out last fall he was going to be recognized with a national award for his volunteer work. The Packet

Four arrested in Gatineau drug raids; 300 meth pills, 53 grams of pot seized
Gatineau police have seized nearly 300 methamphetamine pills, four marijuana plants and a 2011 Ford Edge after a two-month drug operation. On Wednesday, police raided a location on Daniel Johnson Street. The next day, police raided another location on Normand Street. Ottawa Citizen

Toronto council asks police to consider 911 texting
Toronto city council is asking the police services board to review options that would enable residents to text 911 instead of making phone calls. The motion was put forward Thursday by Coun. Norm Kelly, who came up with the the idea following a mass shooting at Orlando nightclub Pulse last month. During that incident police received frightened calls from the club's bathroom from trapped people worried the shooter might hear them talking. CBC News

Data Hub proposed for former Waterloo police station
If big data is the new oil, the former police station on Erb Street could be Waterloo's new economy gusher. The Communitech Data Hub is slated to move into 19,000-square-feet of space in the former police station at Erb and Albert streets late this fall. The Record

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Le PQ veut s'attaquer à une situation devenue intenable dans les prisons
Le Parti québécois (PQ) estime que la situation est devenue à ce point intenable dans les prisons québécoises qu'il est urgent de dresser un état des lieux afin d'agir le plus rapidement possible pour apporter des correctifs. Le chef de l'opposition officielle, Sylvain Gaudreault, a réclamé vendredi, à Montréal, la création d'une commission parlementaire itinérante non partisane pour faire une tournée des établissements de détention et dégager des pistes de solution en vue de la rentrée parlementaire. Presse Canadienne (L'actualité)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Windsor Islamic Council urges members to expose extreme ideologies
The Windsor Islamic Council, in condemning Thursday's deadly attack in Nice, Frances calling on members of the local Muslim community to expose extreme ideologies. "The perpetrators who commit such attacks in the name of Islam are criminals who follow a sickening perverted ideology that is the farthest from the noble teaching of Islam and the basic norms of humanity," the Windsor Islamic Council said in a statement released Friday. Windsor Star

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Coming soon to store near you: pot
A federal task force has rolled up its sleeves to put together a report due in November on how Canada might legalize marijuana. It would then take until next spring for the governing Liberals (perhaps April 20?) to bring a legislation up for debate in the House. Notwithstanding the gateway argument, which suggests the slippery slope into drug addiction begins with weed, there are many other questions to be answered: In the meantime, entrepreneurs are still trying to find loopholes in laws around the use and distribution of medical marijuana in Canada. A British Columbia company thinks it's found a way to offer mail-order marijuana. Well not quite, but close. Weed Glass and Gifts Ltd. has already opened locations in B.C., Ontario, Quebec and, just last week, in Winnipeg. The business in the Exchange District is there basically to take your "medically prescribed" order and arrange shipment to you. They'll also sell you some usage tools, while you wait... Meanwhile, the highly reported decision to legalize marijuana in Colorado is two years old and statistics are now coming in. They are now tops in the nation when it comes to weed use among kids 12 to 17. Less than 10 years ago, they were number 14. And a 2015 Washington State report found DUIs involving marijuana had almost doubled since legalization. Couple that with the contention from the medical case that "today's" marijuana is a super potent and potentially lethal version of the highly romanticized product of the '60s and '70s. Winnipeg Free Press

PUBLIC SERVICE / FONCTION PUBLIQUE

Public service unions taking Ottawa to court over pay system problems
Thousands of Canadian public servants have missed paycheques, been over- or underpaid, or have been denied health benefits since the roll-out of the government's new pay system, Phoenix, which went live in February. Thirteen public service unions are now taking the government to Federal Court over the matter, seeking a ruling that will force the government to pay public servants properly and punctually. Globe and Mail

Minister blames payroll problems on inadequate training
While federal government employees continue to struggle to make ends meet without a regular income, the minister in charge of the beleaguered new payroll system blames the problems partly on inadequate training, and admits those issues should have been worked out sooner. "It would appear that there wasn't sufficient training done of those who had to implement the system to ensure that it was rolled out as it was intended to be," said Judy Foote from St. John's, Nfld., in an interview with CBC News. Foote explained that although the Phoenix system was tested thousands of time before the switchover from the previous payroll system, staff had not been properly trained in data entry, resulting in a backlog of files. CBC News

OTHER / AUTRES

Broadcast Media / Médias télédiffusés :

CTV News interviewed the French ambassador to Canada, Nicolas Chapuis, regarding the attack in Nice, France. Rough Transcript

CBC News' Power & Politics interviewed the French ambassador to Canada, Nicolas Chapuis, regarding the attack in Nice, France. Rough Transcript

INTERNATIONAL

Turkish President Erdogan urges supporters to take to streets, protest coup
Chaos and confusion gripped Turkey on Friday after an attempted coup by elements of the military plunged the country into a state of unrest, with reports of gunshots fired in the area near Istanbul's Bosporus Bridge. A Turkey military faction has claimed armed forces have "fully seized control" of the country, but Deputy Prime Minister Numan Kurtulmus said on local television that Turkey's AK Party is still in charge. Turkey's state-run Anadolu Agency reported 17 police officers had been killed in a helicopter attack on police special forces headquarters on the outskirts of Ankara. The agency said Turkish Air Force planes shot down the helicopters. CBC News has not been able to independently confirm the reports. Reuters (CBC News); Associated Press (CTV News); Global News

Estranged wife of man who slammed truck into crowd in Nice, France arrested
French leaders extended the country's 8-month-old state of emergency Friday and vowed to deploy thousands of police reservists on the streets after a Tunisian man drove a truck through crowds celebrating Bastille Day in Nice, killing 84 people and wounding 202 others. Thursday night's massacre of pedestrians leaving a fireworks display along the southern city's famed boulevard ended only after police killed the armed attacker in a hail of bullets. Associated Press (Whig-Standard, Edmonton Sun)

President Obama Calls Attack on Nice 'Appalling' and 'Sickening'
President Obama today called the killing of more than 80 people in Nice an "appalling attack on the freedom and the peace that we cherish," adding that the hearts of Americans are with the people of France. The president made the remarks at what was originally planned as a private reception for the Diplomatic Corps in the East Room of the White House. Obama said he had spoken to French President Francois Hollande and that he "reminded him that France is America's oldest ally and one of our strongest." ABC News; Reuters; Fox News

France attacks bolster growing global fears, but long-term impact uncertain
The deadly truck attack in Nice, France, had an enormous human cost, but it may also weigh on the economy of a country - and a world - that has now seen several horrific terrorist incidents over a relatively short period of time. It is very hard to determine what impact a single tragedy can have on a huge economy such as France, said Craig Wright, chief economist at Royal Bank of Canada, but the fact that there have been a series of attacks could put a damper on growth. Globe and Mail

The terrible new tools of terrorism
The use of a 19-tonne truck to cut down scores of seaside revelers in Nice, France - if connected to jihadist-inspired terrorism - would represent a dramatic escalation in what experts describe as an emerging trend in attacks: simple, even crude instruments employed to kill ever-larger numbers of people. Thursday's rampage appears to have set a grisly new standard as one of the deadliest attacks in years in which most victims were killed by nonexplosive means. Instead of guns or bombs, the driver mainly used his vehicle to crush men, women and children who had gathered to watch a fireworks display. Hamilton Spectator

Horrifying details of the Bataclan Theatre massacre revealed
The Islamic State terrorists who attacked the Bataclan Theatre in Paris last November may have committed heinous acts of torture, including gouging the eyes and genitals of some hostages, according to a shocking new French report. Some victims' bodies from the second floor of the theater appeared to have been beheaded, eviscerated and otherwise mutilated, according to the report, which details testimony before a parliamentary committee by French police who rushed to the scene. New York Post

Post Pulse, hearing into why Orlando didn't get funds
A month after the Pulse nightclub massacre, law enforcement leaders told a congressional committee in Washington on Friday that the Orlando area's tens of millions of tourists should be given a greater say in determining which metro areas get federal money for preventing and responding to terrorist threats. Associated Press (660 News, ABC News)

Secret chapter of 9-11 inquiry released after 13-year wait
The U.S. on Friday released once-top secret pages from a congressional report into 9-11 that questioned whether Saudis who were in contact with the hijackers after they arrived in the U.S. knew what they were planning. The newly declassified document , with light redactions, names people the hijackers associated with before they carried out the attacks, killing nearly 3,000 people in New York, Washington and on a plane that crashed in Pennsylvania. It identifies individuals who helped the hijackers get apartments, open bank accounts, attend local mosques and get flight lessons. Fifteen of the 19 hijackers were Saudi nationals and several were not fluent in English and had little experience living in the West. Associated Press (London Free Press, Toronto Sun, Ottawa Sun, Whig-Standard)

There is no clash of civilizations
An opinion piece states, "Mohamed Bouhlel, who turned a truck into a deadly weapon and murdered dozens of people in Nice, was not unknown to police. He'd had run-ins with the law for small offences, and earlier this year had been convicted in an incident of road rage. He apparently beat his wife; she was divorcing him. Neighbours described him as a weird and creepy loner who made them nervous. Originally from Tunisia, he doesn't seem to have been religiously observant or deeply interested in Islam. He wasn't on a terror watch list..." Globe and Mail

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

Ralph Goodale
Have sent message to my French counterpart, Interior Minister Cazeneuve, expressing Canada's profound grief and absolute solidarity.

Ralph Goodale
J'ai écrit à mon collègue français, le ministre Cazeneuve, pour lui faire part de notre profond chagrin et solidarité.

Félix M.Beaulieu
#nice:Député de Regina-Wascana et min. de Séc. publique @RalphGoodale a communiqué avec son homologue français #rcsk

DesmondCole
Immigration detainees on hunger strike against prison conditions, endless detention. Where is Minister @RalphGoodale?thestar.com/news/canada/20...

620 CKRM
Protestors converge on MP Ralph Goodale's Regina office #yqr #SK http://bit.ly/29lJldO

CharlieAngusNDP
Letter 2 @RalphGoodale on systemic underfunding of @NAP_Police Cops roll dice with their lives. charlieangus.ndp.ca/sites/default/...

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NewsTalk770
Tornado warning ENDED for Lethbridge. Tornado watch still in effect. #yql #abstorm

CF Operations
#OpNUNAKPUT : Canadian Rangers and #RCNavy members did search and rescue drills near Yellowknife

Saskatoon Buzz
Cleanup underway from Saskatchewan flooding: Flood response has shifted to recovery mode in Saskatchewan...

CBCSaskatoon
ICYMI: 200 from Red Earth Cree Nation evacuated to Saskatoon cbc.ca/1.3680454 #skstorm #skflood

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Stewart Bell
A troubled Canadian, whom RCMP has been monitoring, reacts after Nice.

natnewswatch
Five ways Canada is trying to prevent the kind of attack that happened in France | National Newswatch
nationalnewswatch.com/2016/07/15/fiv…

Public Safety Canada
#FF to @CSISCanada &@CSE_CST, from an appropriate distance ;)

CSE_CST
@Safety_Canada @csiscanada We expect anything Public Safety does to be from a safe distance. #FF

BORDER SECURITY / SÉCURITÉ FRONATLIÈRE

No One Is Illegal
No answers as SIU washes hands off immigration detainee's death. ACT NOW: https://www.change.org/
#MigrantStrike

BlackPressMedia
Gun, ammo cause trouble for American at #Aldergrove border crossing bit.ly/29KH0Sh pic.twitter.com/4DXIpMWnlM

PtboExaminer
RT @Northofsevn: Special Investigation Unit clears Peterborough Police officer, OPP officer in immigration detainee's fb.me/9yeAWHplV

PtboExaminer
Coroner's inquest called into Central East Correctional Centre immigration detainee's death at #ptbo hospital @PRHC1
thepeterboroughexaminer.com/2016/07/15/cor…

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Kaspersky Lab
Encryption, Lockscreen, and MBR, oh my! Learn about different types of #ransomware https://kas.pr/ojj3

SC Magazine
New banking malware stops customers from cancelling payment cards

Infosecurity
CyberSecurity: How Artificial Intelligence Is Your New Best Friend

LAW ENFORCEMENT / APPLICATION DE LA LOI

OCHeadlines
RCMP didn't 'purge' public documents, the Mounties actually just had no idea where they were ow.ly/Ffjf502s0de

CBC_Aboriginal
RCMP did nothing wrong in Peguis First Nation shooting death, review finds ift.tt/2a4DdkT
pic.twitter.com/SKn0iRpeJN

chronicleherald
First Nations leaders call on feds, Ontario to hash out new policing agreement herald.ca/nt8

CharlieAngusNDP
Here's an article I wrote in 2012 on the PTSD crisis hitting @NAPS_Police from underfunding and lack of resources.

CharlieAngusNDP
crisis facing @NAPS_Police is unacceptable. Officers/communities at risk in @NANComms territory from underfunding http://www.chroniclejournal.com/

CBC_Aboriginal
Nunavut RCMP struggle to get Inuit cadet program off the ground ift.tt/29VfRwU pic.twitter.com/9Ftkci1XrW

UBCIC
.@CBC_Aboriginal Nunavut RCMP struggle to get Inuit cadet program off the ground ow.ly/SKFW502sgjZ

CTVAtlantic
Beaverbrook man facing charges after allegedly hitting RCMP car with vehicle: A 48-year-old man from Beaverbr... bit.ly/29ZdXcS

VancouverSun
Burnaby realtor has grow-op charges drop over court delays - A realtor who was charged after police raided a su... ow.ly/sAm1502s8L4

RCMP, Ontario
Peace Tower flag (Ottawa) at half-mast until sunset July 18 to mark the tragic events in Nice, France ^JT

Surrey RCMP
Our thoughts are with the people of Nice and all first responders. @PMdeNice

GRC de Surrey
Nos pensées accompagnent la population de Nice et les premiers intervenants @PMdeNice

RCMP
Need to register a firearm? Try our online tool. #CFPonline #RCMP http://rcmp.ca/-2qw

Bob Paulson
Bob Paulson is apologizing for "egregious behaviour" at the RCMP's explosives training unit http://www.cbc.ca/1.3680145

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Correctional Service
Our Institutions are private property - playing PokémonGo there is trespassing. #PokémonGo

Servicecorrectionnel
Nos établissements sont des zones restreintes - jouer à #PokémonGo à ces endroit est une intrusion.

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

TheWindsorStar
#Windsor Islamic Council urges members to expose extreme ideologies ow.ly/9Pup302hQBB pic.twitter.com/AhEladE8vi

PUBLIC SERVICE / FONCTION PUBLIQUE

globepolitics
Public service unions taking Ottawa to court over pay system problems trib.al/1HhBkSk #cdnpoli

CBCPolitics
Minister blames payroll problems on inadequate training cbc.ca/news/canada/ot... #cdnpoli #hw

OTHER / AUTRES

TravelGoC
Canadians in #Turkey: Remain indoors and monitor local media. http://ow.ly/yqCa302ivQI

MinCanadaFA
Very concerned about reports from #Turkey: Urging calm, order, safety of all people in Turkey

TravelGoC
Canadians in or around Istanbul can also call 90 (212) 385-9700. All consular contact info: https://travel.gc.ca/assistance/embassies-consulates/turkey …

David Akin
"Clarification: Two Canadians not among dead in Nice"

Lawrence Cannon
#NiceAttacks: no Canadians reported among casualties to date. Thanks to the French authorities for their cooperation

Lawrence Cannon
#NiceAttentat: aucun Canadien ne figure parmi les victimes pr l'instant. Merci aux autorités françaises de leur précieuse coopération

natnewswatch
Edmonton student missing as Trudeau pledges solidarity with France following truck attack | National Newswatch nationalnewswatch.com/2016/07/15/que…

ipoliticsca
Edmonton student missing as Trudeau pledges solidarity with France following truck attack ipolitics.ca/2016/07/15/edm… via @ipoliticsca

INTERNATIONAL

The National
Former CSIS Assistant Director Ray Boisvert examines the Bastille Day attack in Nice. http://www.cbc.ca/1.3680154

Mubin Shaikh
Well then. France attacker a drug-head, ate pork, did not observe Ramadan & never prayed. "Shariah" right?

Doug Saunders
Nice terrorist fits the consistent profile: Non-religious, wife-beating petty criminal; French citizen

NSPS (CBoC)
The Global Reach of #Terrorism: Reflections on the Attacks in #Paris, Beirut, and Baghdad http://www.conferenceboard.ca/ #lesm #natsec

Doug Saunders
Nice terrorist fits the consistent profile: Non-religious, wife-beating petty criminal; French citizen

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

Today's News / Actualités
July 19, 2016 / le 19 juillet 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Hunger strike continues at Central East Correctional Centre; activists press Monsef to end indefinite immigration detentions
A rally outside Peterborough-Kawartha MP Maryam Monsef's constituency office Monday offered solidarity to immigrant detainees on hunger strikes at jails in Lindsay and Toronto. About 40 people gathered at the Bethune St. office over noon hour to show their support for detainees who've been on hunger strike for several days. More than 50 detainees between the two jails haven't eaten since July 11. They're demanding to speak with **Public Safety and Emergency Preparedness Minister Ralph Goodale**. They want to express their concerns about state of current jail conditions and are seeking an end to indefinite immigration detention in Canada. Peterborough Examiner

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

The one per cent are coming to Canada's Arctic
Residents of Ulukhaktok, N.W.T., population 402, may feel as though New York's tony Upper East Side has come to visit when Crystal Serenity steams into town later this summer. The towering cruise ship, the biggest to traverse the fabled Northwest Passage, will be carrying 1,070 passengers who paid between $25,000 and $155,000—and 655 crew members—for a 32-day trip that promises "intrepid adventure, the great outdoors and immersive cultural experiences (…)" With the Arctic's defences melting, Los Angeles-based Crystal Cruises is understandably excited about a huge opportunity to wow well-heeled cruise junkies who've grown bored of sand and sun. The company's inaugural Northwest Passage cruise, from Anchorage, Alaska, to New York, sold out quickly, and tickets for next year's trip are already on sale. Less thrilled are those asked to make sure such voyages go smoothly and safely (…) Indeed, the straits and sounds of Canada's Arctic archipelago are mostly uncharted and, depending on the day, can either be totally clear or choked with hull-cracking sea ice. Add to that the unpredictable weather and a general lack of Arctic infrastructure—like deepwater ports or search-and-rescue bases—and it's easy to see why the Guardian asked whether Crystal Serenity might be "a new Titanic (…)"One thing Crystal Serenity doesn't offer, however, is much tolerance for sea ice. So its owners set out to hire a support ship as an insurance policy. But finding a suitable vessel in Canada wasn't easy. "There's been a long-term rundown of the fleet," explains Dermot Loughnane, the CEO of Tactical Marine Solutions in Victoria, who was hired to give Crystal a helping hand. Crystal eventually found what it needed on the opposite side of the planet: the British Antarctic survey vessel RRS Ernest Shackleton. The sturdy, red-hulled ship will carry two helicopters and containers full of extra water and emergency rations for Crystal Serenity—enough for three days. There's also emergency oil-spill and damage-control gear on-board. "By having the Shackleton there, we can make up for quite a few things," says Loughnane, who spent 11 years of his 35-year career working in the Arctic. "It's above and beyond anything that's required." The planning didn't stop with equipment. Crystal Cruises did an extensive analysis of Arctic sea ice in past years, including the most likely choke points. One of those areas is the Victoria Strait, to the west of King William Island. "I describe it as the toilet," says Loughnane. Maclean's

Huge military aircraft visits St. John's International Airport
The St. John's Airport played host to a rather noticeable guest on Monday — a gigantic Canadian Forces Aircraft. The CC-177 Globemaster III, with a length of 53 metres and a wingspan of almost 52, landed at the St. John's Airport Monday afternoon for training, just after a stop in Stephenville (…) The Globemaster is a transport plane, used to fly troops and machines all throughout the world. Church says his plane has launched Canada's Disaster Assistance Response Teams in the Philippines and in Nepal. It's also been used to fly into Afghanistan and Iraq for the military's middle-eastern missions. CBC News

Ranger Patrol
They are the eyes and ears of remote Canada and a vital part of the Canadian Armed Forces' (CAF) domestic operations, but most people still don't know they exist. With that in mind, the newly appointed commanding officer of the 4th Canadian Ranger Patrol Group (4 CRPG), Lt.-Col Russ Meades, says one of his key focuses will be educating both military personnel and the public about the approximately 5,000 part-time Canadian Rangers across our country who provide patrols for national-security and public-safety missions in difficult to access, sparsely settled regions as members of the Canadian Army Reserve (…) With the transformation complete, the 4 CRPG ranks have swelled from 600 in 2007 to its present-day level of approximately 1,000 Rangers, plus over 800 Junior Canadian Rangers, all overseen by 65 full-time staff. He notes how 4 CRPG, a unit of the 3rd Canadian Division which is headquartered in Edmonton, has become a go-to organization for both Joint Task Force West and Joint Task Force Pacific. "The Canadian Rangers have gone from being a pre-2007 military backwater, a program with very limited funding and resources, to a robust organization that is a very capable and a reliable resource for Division and Joint Task Force commanders," said Lt.-Col Meades. Esquimalt Lookout

Glimpsing the future: Researchers predict how fires will change N.W.T. forests
A group of forest fire scientists are studying areas of forest in the Northwest Territories that have re-burned in the past 15 years to try and understand what the future boreal forest might look like. "We're seeing more and more big fire years in the past decade or so," said Daniel Thompson, a forest fire

scientist with the federal government. "That means we're expecting to have more fires in younger forest stands," he said, which could result in a very different kind of forest in the N.W.T. "Trees have evolved to be burning every 70 to 120 years," explained Thompson. "But if they're now burning at 16 to 18 years, we're wondering whether the seeds are going to propagate in the same way, are the plant communities going to react in the same way?" CBC News

Tree Canada commits to urban replanting in Fort McMurray in wake of wildfire
After visiting the scorched areas of the Wood Buffalo region, Tree Canada is now committed to helping Fort McMurray rejuvenate its urban foliage. Following a helicopter tour of the area July 14, Tree Canada president Michael Rosen met with city officials, including Wood Buffalo Mayor Melissa Blake and urban forestry planner Stephen Fudge, to discuss how best to go about replanting the 10,000 urban trees that the city lost during the wildfire that began in May. "Fire is a natural part of the boreal forest, so it regenerates naturally quite well," said Rosen, explaining why they won't be replanting trees in rural areas. "So we're looking more at people's residences, like the 2,000-plus homes that actually burnt. We're trying to give them that sense of normalcy when they finally come back and build their new homes." Edmonton Journal

Thunderstorms knock out power to thousands in Quebec
More than 33,000 Hydro-Québec customers lost their power during thunderstorms on Monday that saw torrential rain, strong winds and hail tear through parts of the province. Though the outages affected parts of Montérégie and the Eastern Townships, more than half of the customers who lost power were in the Montreal area. As of 6 a.m. Tuesday power was returning to most customers, with Hydro-Quebec saying 1,431 customers were still without power, including 12 in the Montreal region. Montreal Gazette; Radio-Canada

Calgary under severe thunderstorm warning, tornado watch issued for swath of southern Alberta
After Calgary was under a severe thunderstorm warning for most of Monday, Environment Canada has now downgraded the advisory to a severe thunderstorm watch. Large portions of Southern Alberta, including Strathmore, Fort Macleod and Lethbridge remain under severe thunderstorm warnings. As of late evening, several areas were also under a tornado watch, including Okotoks, Strathmore, and Fort Macleod. Lethbridge and Cypress Hills Provincial Park are under tornado warnings as of late Monday evening. Calgary Herald

Rafters run into trouble on Gander Lake
Three rafters on Gander Lake were safely located in the early morning hours of July 11 thanks to the efforts of Bonavista Bay Ground Search and Rescue members. According to Staff Sargent Roger Flynn, with the Gander RCMP, two men and a woman – all in their early 20s from Gander – decided to head out for a day of rafting in a rubber dingy and inner tube. The group was headed for Little Harbour but had some trouble reaching the location. “The wind probably came up and they didn’t quite make it as far as they had wanted to,” said Flynn. ”Darkness had set in and they didn’t quite know where they were.” So the group headed for shore and started a fire, as the weather had turned misty and cold. Luckily they were within cellphone range and were able to call for help. Flynn said the RCMP received the call at 10:15 p.m. and followed up with the area Ground Search and Rescue members, who travelled in from Glovertown and launched at Little Harbour. The two-person crew located the group by 3 a.m. and returned to shore less than an hour later, cold but uninjured. Rogers had nothing but praise for the work of the ground search and rescue crew, saying the response was timely and the men involved carried themselves in a very professional manner. “It’s nice to have ground search and rescue on hand to assist, call them up and in an hour or so they are on scene with a boat in the water,” he said. Gander Beacon

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Why France—again?
An opinion piece by Canadian security expert Phil Gurski states “The horror of what happened in Nice compounds the horror of what happened in Paris in January and November 2015. These large-scale attacks got a lot of attention, but there were also some smaller ones like the killing of a police officer and

his wife and an attempt to blow up a gas plant that have to be added to the list of terrorist attacks in France. It seems that France is making the headlines for all the wrong reasons (…) Nevertheless, there are a number of issues in France that are complicating matters. I provide a partial list with the caveat that none of these gives us a complete answer whether we tackle them individually or as a whole, nor are they necessarily tied to an increase in terrorism. France has done a terrible job of integrating Muslims. Yes, integration is a two-way street and it is not all the state's fault, but there is a huge gap between different types of citizens. France could learn a lot about how we do things here in Canada. French prisons are breeding grounds for radicalization; this is a tough problem to solve, but something needs to be done about it. French Muslims are estimated to represent between 60-80 per cent of the prison population, widely disproportionate to their almost 8 per cent of the general population (…) We are never going to "beat" terrorism anymore than we are going to "beat" crime. It is a part of the human condition and while we have to do everything we can to minimize the incidents and effects of terrorism, we must accept that it will occur on rare occasions. Our security agencies will continue to do the best job they can and we will be safer because of them." Hill Times

Time for Canada to export inclusivity: Gwyn
An opinion piece states "Among the official explanations given for the slaughter in the French city of Nice were, from the jihad organization Daesh, that the murderer was one of their "soldiers," and from France's president, François Hollande, that the act had "a terrorist character (…)" Certainty is impossible but what may have triggered the horror that Bouhlel unleashed was not the tempting explanation that he did it because he hated non-Muslims but that, as a deeply depressed man whose life had become an utter failure, he hated himself. Legitimately, many would say, so what? The difference does matter, though. In contemporary Europe the single most important political issue is an ever-increasing fear and rage by Europeans about Muslims. In a recent survey by the Pew Research Center, a majority in eight of ten European nations declared that the presence of refugees increased the likelihood of acts of terrorism (…) Just about the only country where Muslims are now treated as individuals no different in almost all respects than are all other individuals is — this one. Canadians owe that singularity to the values they possess and which they consistently refuse to give up. They owe it also to the fact that Justin Trudeau won the last election and then, as prime minister, set about "bringing Canada back (…) Many years back we made a major contribution to international affairs by developing the idea and the institute of peacekeeping. Somehow we need to develop a contemporary equivalent, this one based on the presumption that all are equal. Easy to say; excruciatingly difficult to accomplish. But it's what the world needs." Toronto Star

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CBSA asking Americans to leave weapons at home; hundreds of guns seized locally in recent years
If you're coming to visit us, please leave your guns at home. That's the message the Canada Border Services Agency plans to deliver to our American friends following hundreds of gun seizures in our region in recent years. A total of 466 guns have been seized by the CBSA over the last five years in the Pacific region. An additional 72 have been confiscated in the first half of this year. "It's a huge concern," says Erin Steeksma with the CBSA. "Illegal firearms are very high risk, and they're an enforcement priority for us across Canada. It's something that we're very aware of." Given this, Steeksma says in the coming months, the CBSA is planning an information campaign to let Americans know what they can and can't bring up here. News 1130

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

'Prominent' Admin of Top ISIS Forum Hacked
An administrator of a top-tier ISIS web forum, who one expert describes as a "prominent" member of the online jihadi community, has been hacked. On Sunday, an independent researcher known as "Switched," who first reported the news, tweeted two Pastebin posts containing alleged correspondence of Abu Alaaina Khorasani, who is an administrator of the "Shumukh al Islam" website. Shumukh al Islam, or

"Glory of Islam," regularly hosts official ISIS propaganda (…) According to Alkhouri, the messages, which are mostly in Arabic and stretch back over two years, deal with the conflict between ISIS and Al Qaeda supporters, the procedures around obtaining new members for the forum, and other correspondence with current members. A small number of messages also appear to have been encrypted with Asrar al-Mujahideen, a custom jihadi encryption program similar to PGP. Motherboard

Governments Ramp Up User Data Requests to Google
Google handed over data on users to the authorities in nearly two-thirds of cases in the second half of 2015, according to its latest Transparency Report. The report shows that the web giant received requests for data 40,677 times during the period 1 July and 31 December 2015, and user account information 81,311 times - up from 69,000 during the previous six months. It claimed that 64% of the time it produced "some data," although it's impossible to know how much. Infosecurity Magazine

Pre-Snowden Whistleblower Explains How NSA Got 'Unleashed' To Spy On Everyone
Thomas Drake was a 48-year-old decorated Air Force and Navy veteran, and a senior executive at the National Security Agency, the NSA, when he decided he had to speak up against what he considered the spy agency's abuses. That's when he anonymously contacted a reporter at The Baltimore Sun, helping her expose wrongdoing at the agency in a series of articles. Two years later, the FBI raided his home, and the US government launched an investigation into Drake for leaking classified information and espionage (…) "History was at stake," he said in a recent interview with VICE's reporter Ben Makuch filmed for VICELAND's series on hacking and surveillance, CYBERWAR. In a deleted scene, Drake explains how the NSA got "unleashed" after 9/11 and expanded its spying powers, pushing it beyond the limits of what he believed was acceptable. "The mantra was, just get the data," Drake said. "Collect it all, so we can know it all." Motherboard

LAW ENFORCEMENT / APPLICATION DE LA LOI

Mystery of Hudson Brooks shooting death sparks emotional rally
A candlelight vigil for Hudson Brooks yesterday outside the South Surrey RCMP detachment turned into a raucous protest for the 20-year-old who was shot in a police encounter a year ago. A 100-strong crowd gathered near the detachment chanting and waving "Honk for Hudson" signs. At one point the vigil took a turn for the worst when a man driving by sparked a fight and police officers had to break up an obscenity-peppered shoving match.The circumstances surrounding Brooks's shooting on July 18, 2015, remain a mystery to people who loved him, mired in investigation and shrouded in suspicion. "You ruin our lives. You make us sit there and ruin our lives. It's the worse. How did my son die? I want to know," said Brooks's mother Jennifer. All the Independent Investigations Office (IIO) has told family is that Brooks was shot at 2:30 a.m. PT by the RCMP. Another officer ended up with a gunshot wound in her leg during the incident, but the only weapons found at the scene were police weapons. Neither the IIO, nor the RCMP has revealed what happened in the moments leading up to the shooting, and why, or how a weapon was drawn on the young man described as "quirky" and "happy" by those who knew him. It remains unclear whether Brooks was armed or not, but a IIO statement released earlier this year said: "Other than police issued equipment, nothing of significance was recovered from the scene." CBC News; Global News

Who pays? New guide sets out rules for Trudeau travels
Justin Trudeau's frequent trips abroad — often with an entourage of family, officials and guests — raise tricky questions about who travels on the public dime and who does not. So the government recently "formalized" the rules, setting out who digs into their own pockets for travel expenses and who gets their bills picked up by taxpayers. One unexpected disclosure in the four-page guideline document, obtained by CBC News under the Access to Information Act, is the extent to which public money can underwrite the prime minister's personal travels, such as vacations or trips for the Liberal party. (…) In addition, one aide from the Prime Minister's Office is allowed to travel to "support" Trudeau on personal trips, again on the government dime. The principle is that the prime minister must have access to secure communications at all times, even during vacations, to respond effectively to crises, such as the recent attempted coup in Turkey. Privy Council Office spokeswoman Regine Beauplan says staff provide

support during all travel by the prime minister, including "the creation of a temporary satellite equipped office that provides access to the secure equipment he needs to carry out his duties." The RCMP is responsible for all ground transportation if the Trudeau family travels for personal reasons, the guidelines say, and the government pays the entire bill without seeking reimbursement. CBC News

Man accused of ramming into RCMP cruiser released on bail
A provincial court judge agreed to unlock the door and throw away the key for a Colchester County man Tuesday. Kevin Dean Underwood, 48, was released on $1,000 bail until his return to Truro provincial court on Sept. 21 to face four charges related to ramming into an RCMP cruiser on Thursday. The conditions of his release preclude Underwood from possessing the key to or sitting in the driver's seat of any vehicle. The release conditions, read in court by defence lawyer David Mahoney and agreed to by Crown lawyer Alison Brown, also stipulate that the accused keep the peace and be of good behaviour. Underwood, whose 34 address listings have jumped from British Columbia to Kennetcook, Maitland, Truro, South Maitland, Upper Kennetcook, Five Mile Creek and Beaver Brook, is accused of twice smashing into the RCMP vehicle early Thursday afternoon on Princeport Road in southwestern Colcester County. An RCMP spokeswoman said that police were heading toward the Princeport Road area, about halfway between Truro and South Maitland and just off Highway 236, to set up a checkpoint when an officer noticed a small pickup truck with no licence plate and no box. The officer turned the cruiser around and deployed the emergency lights in an effort to pull the truck over. The pickup driver did not stop and instead turned back toward the police cruiser and rammed into it, police said. The driver then backed up and smashed into the police vehicle again. The driver tried to drive off in the pickup truck but was apprehended and arrested. The officer sustained minor injuries. Local Xpress

Whitehorse police investigate car fires
A second car fire in as many days has police in Whitehorse investigating a potential serial arsonist. Shortly after 6 am Monday, fire crews and RCMP responded to a car fire along Taylor Street. On Sunday, fire crews were called to 6th Avenue and Steele Street for a report of a car fire causing damage to three vehicles. There were no reported injuries in either case. Mounties are calling both incidents suspicious, and say they are not ruling out the possibility that the two are connected. CKRW; CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Il avait tué sa femme le jour de la fête des Mères: Timothy Rapley meurt en prison
Emprisonné depuis 2011 pour avoir tué sa femme le jour de la fête des Mères, dans la résidence familiale de Dollard-des-Ormeaux, Timothy Rapley est mort en prison, ont annoncé les autorités carcérales. Rapley, 61 ans, était incarcéré au Centre régional de santé mentale, à Sainte-Anne-des-Plaines. Le Service correctionnel du Canada (SCC) n'a pas fourni davantage d'informations quant aux circonstances du décès du meurtrier, survenu samedi. «Comme c'est toujours le cas lors du décès d'un détenu, la police et le coroner ont été prévenus, et le Service correctionnel du Canada examinera les circonstances de l'incident», a indiqué le SCC dans un communiqué laconique. (…)L'homme a été condamné pour meurtre non prémédité en mai 2015 et purgeait depuis ce temps «une peine indéterminée», selon le SCC. Journal de Montréal; CJAD

Triple killer Jon Rallo's defiant claims of innocence slam the door on parole
Forty years after Jon Rallo killed his wife and two small children, his refusal to admit his guilt is still standing in the way of his freedom. The Parole Board of Canada has once again turned down the former Hamilton city manager's bid for full parole Tuesday morning during a hearing at Beaver Creek Minimal Institution in Gravenhurst. The two-member panel also refused to increase the number of days Rallo is allowed to live out in the community. Currently Rallo, 73, spends four days living in an apartment with his girlfriend in Sudbury. The other three days he must spend at a halfway house in that city. It took the panel just 10 minutes to come to its decision. Hamilton Spectator

Broadcast Media / Médias télédiffusés:

Edward Downey, who is accused of murdering Sara Baillie and Taliyah Marsman, was denied parole twice by the Parole Board of Canada. When Parole Board members denied those attempts, they cited his likelihood to violently offend if released. He was granted full parole in 2010. (CBC News, 11:15ET, 12:20ET)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

25% of Canada's human trafficking victims are minors: Statistics Canada
People under the age of 18 made up about a quarter of recorded human trafficking victims in Canada between 2009 and 2014, new data reveals. In a recent report, Statistics Canada noted that minors not only make up a significant portion of victims of forced labour or sex trafficking crimes, but that they also make up around seven per cent of the perpetrators. The 18 to 24 age cohort was even more startling, with nearly 50 per cent of victims and 41 per cent of perpetrators falling into that range. Nicole Barrett, a human-trafficking expert at the University of British Columbia's Allard School of Law, said that some of those numbers are supported by her experience with the Canadian Women's Foundation's National Task Force on the Trafficking of Women and Girls. Anecdotally, she said, 12 or 13 years old was generally the age when young women were forced into the sex trade. Barrett said that much like the overall picture of human trafficking in Canada, the data related to the ages of victims and abusers is hobbled by the fact that only a small fraction of trafficking crimes are ever uncovered or reported. Canada still isn't doing a good job monitoring labour trafficking in particular (nannies, seasonal agricultural workers, etc.), she said, and human trafficking is still "vastly under-counted" for a variety of reasons. Global News

Human trafficking convictions increasing in Toronto since last year
Toronto Police Service has been collecting statistics related to human trafficking since 2013. There has been a total of 9 human trafficking convictions to date; as of last summer police had only one. A provincial strategy was recently announced to combat human trafficking. It was noted Ontario has 65 per cent of human trafficking cases in Canada. The conviction rate across Ontario is seven per cent. Inside Toronto

ESCAPING THE TRAP: Coming up with a co-ordinated strategy to combat human trafficking
The young man stands before the judge, barely crossing the age threshold of being tried in adult court. Charges against him are lengthy and grim: a snippet includes forcible confinement, uttering threats, sexual assault, and human trafficking. Police know the human trafficking charge will be the hardest one to land a conviction on, mainly due to the victim's unwillingness to testify or memory lapses, and will often take pleas for lesser offences. The total number of human trafficking convictions in Toronto since 2014 now stands at nine; in the first week of July alone, Toronto police arrested seven men within a four-day span on human trafficking charges, one case involving a victim as young as 14. And one York Region cop has no problem dropping human trafficking charges if it means pimps will land in jail. "It doesn't mean they all walk, they all got away," said Det. Sgt. Thai Truong, adding as a police officer, as long as the accused is found guilty for what he's done and justice is served, "I'm happy with that." The provincial government unveiled the long-awaited human trafficking strategy Thursday, June 30, which calls for an investment up to $72 million aimed at increasing awareness and coordination, enhancing justice-sector initiatives and improving survivors' access to services. Currently, Ontario is grappling with roughly 65 per cent of police-reported human trafficking cases in Canada. The strategy involves nine ministries and is based on four pillars: strong leadership through an anti-human trafficking office through CommSoc, which will collect and share information; increased awareness and community supports to help survivors heal; justice sector initiatives to identify trafficking earlier and hold traffickers to account; and indigenous-led approaches. Inside Toronto

Broadcast Media / Médias télédiffusés:

150 Toronto teens were chosen to work on youth in policing initiatives. (CBC News, 10 :55ET, 11:45ET)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

NIL

PUBLIC SERVICE / FONCTION PUBLIQUE

Oops! Can someone just program this damn computer?
Everyone's apologizing, there's lots of pointing fingers, words like "unacceptable" are being thrown around, and a whole lot of people who work for the Canada's federal government are not getting their proper monetary compensation. What, you may wonder, is going on? Turns out a vaunted new pay system called Phoenix has managed to mess up more than a few peoples' lives. Federal public service employees are reporting tanking savings, maxed-out credit cards and growing mounds of unpaid bills because....well, the federal government, (and its Phoenix surrogate) is just not coming up with the money. "This is a national disgrace," says Chris Aylward, vice-president of the Public Service Alliance of Canada, which wants Phoenix taken off line until the problems are solved. The Conservative government originally introduced Phoenix last year, but Marie Lemay, deputy minister for Public Services and Procurement, says the Liberal government "grossly underestimated the time and training needed to move to the new system and clear out old cases, outstripping the capacity to respond." Radio-Canada

Unpaid Parks Canada staff are getting so desperate — they're borrowing money from their parents
A new payroll system introduced by the federal government earlier this year has been so riddled with problems, that it's forcing some Parks Canada staff to borrow money from their parents. "I can't afford to pay gas, I can't afford to pay my insurance. I can't afford rent or food," said Scott Munro, who works at the Lake Louise campground in Banff National Park. Since the end of May, Munro and at least 30 other staff at the Lake Louise campground have either been underpaid, overpaid or not paid at all. His coworker, Natasha Olsoff, said she's so short on cash right now, that she "can't really even afford to buy groceries" and often relies on leftover food donated by people leaving the campground. CBC News

Broadcast Media / Médias télédiffusés:

CTV News interviewed Chris Alward, National Executive Vice-President of the Public Service Alliance of Canada, concerning problems with the government's new pay system. (CTV News Network, 6:10ET)

It's been six months since Ottawa rolled out a new pay system plagued with problems. Thousands of public employees have been overpaid, underpaid or not paid at all. The temporary work centre was open to deal with all of these problems. The government is focusing on some of the most urgent cases, which includes people who haven't been paid. (CBC News, 7:15, 8:15ET, 9:15ET, 10:15ET, 11:15ET, 12:35ET) (CTV News, 6:10ET, 7:10ET)

Documents obtained by *CBC News* show that managers at StatCan have warned the nation's chief statistician that many of its programs and information are at risk due to the low quality of tech support it's getting from Shared Services Canada. (CBC News, 7:10, 8:10ET, 9:10ET, 10:10ET, 11:10ET)

OTHER / AUTRES

Liberals replacing Tory-appointed ambassadors
The Trudeau Liberals have replaced several high-profile political appointments made by the previous Conservative government with a major shuffle of the top ranks of Canada's foreign service. Almost all are career public servants, with three of them replacing political appointees of the Harper government in the United Kingdom, Iraq and Israel.Foreign Affairs Minister Stephane Dion announced the appointment of 26 new ambassadors, high commissioners and others — 13 men, 13 women — in a major shuffle the government says is intended to ensure diplomats represent a wide diversity of Canadians. (...) Former Prime Minister Stephen Harper had appointed the former head of his RCMP security detail, Bruno Saccomani, as the ambassador to Jordan but he is now being replaced. The Jordan mission oversaw neighbouring Iraq, where Canada has no embassy.Saccomani, who was appointed three years ago, spent much of his time in Iraq, as the diplomatic spearhead of Canada's military engagement in the U.S.-led military coalition fighting the Islamic State of Iraq and the Levant.Prior to his appointment, Saccomani faced criticism for his management style while in charge of the more than 100 Mounties that made up the prime minister's security detail, but he quickly won the respect of many of his new diplomatic employees in the Middle East. Canadian Press (Citizen 100, National Post, Chronicle Journa)

Refugee arrivals delays from Turkey likely in wake of attempted coup
Delays in the resettlement of Syrian refugees from Turkey to Canada are likely to grow even longer after a failed coup attempted there last week. Securing exit permits for Syrians in Turkey has been a difficult process already, holding up the Liberal government's plans last fall to resettle thousands of people from there as part of their landmark program to bring 25,000 Syrians to Canada in a matter of months. Now, political instability in the country in the wake of the military's failed efforts to seize power last week is expected to delay things more. "We are continuing to work with the government of Turkey to obtain exit permits as quickly as possible and are continuing to monitor the situation," said Sonia Lesage, a spokesperson for the Immigration Department. "However, given recent events, we do expect delays." Canadian Press (CTV News, CP24, Times Colonist, Winnipeg Free Press)

INTERNATIONAL

Mystery Numbers in N. Korea Broadcasts Carry Cold War Echoes
North Korea's state radio has recently broadcast strings of indecipherable numbers, Seoul officials said Tuesday, in a possible resumption of a Cold War-era method of sending coded messages to spies operating in South Korea. A female announcer at the radio station read numbers for 2 minutes on June 24 and 14 minutes on Friday, according to Seoul's Unification Ministry and National Intelligence Service. A copy of those comments provided by the ministry included phrases such as "No. 35 on Page 459" and "No. 55 on Page 913." During the Cold War, Pyongyang sent such numbers via shortwave radio to give missions to agents dispatched to South Korea, according to captured North Korean spies. It later reportedly stopped such broadcasts once it could communicate with its spies overseas via the internet, and as animosities with South Korea eased following a historic inter-Korean summit meeting in 2000. Relations have deteriorated greatly since then as North Korea has pursued the development of nuclear weapons despite international sanctions. Associated Press (New York Times)

Islamic State claims Germany train attack, but officials dispute link
The Islamic State group claimed responsibility Tuesday for an axe-and-knife attack on a German train that left at least five people wounded, but authorities said the 17-year-old Afghan asylum-seeker who was shot and killed by police as he fled the scene appears to have self-radicalized and had no direct link to the extremists. The boy shouted “Allahu akbar” (“God is great”) as he attacked people on the regional train near the Bavarian city of Wuerzburg Monday night, and a hand-painted flag of the Islamic State was found during a search of his room, according to state Interior Minister Joachim Herrmann. (...)Herrmann said people close to the attacker told investigators he had seemed like a calm person, not overtly

religious or an extremist. He said investigators were still looking into the evidence found in the teenager's room, saying it could be possible that the notes included a farewell letter to his father. Globe and Mail

Erdogan tells Turkey coup escape story, hints at death penalty
Turkish President Recep Tayyip Erdogan made a series of televised appearances overnight in which he disclosed dramatic details of his survival on the night of a failed coup and raised the spectre of reintroducing the death penalty to punish conspirators. He told U.S. broadcaster CNN he narrowly escaped death after coup plotters stormed the resort town of Marmaris where he was vacationing. "Had I stayed 10, 15 additional minutes, I would have been killed or I would have been taken," he said in the interview broadcast late Monday. Addressing hundreds of supporters outside his Istanbul residence in the early hours of Tuesday, Erdogan responded to calls for the death penalty with the simple statement: "You cannot put aside the people's demands." Toronto Star

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

nooneisillegal
BREAKING! @RalphGoodale crashed by #MigrantStrike supporters. Meet the detainees now! https://endimmigrationdetention.com/ RT!

rabbleca
60+ immigration detainees are on hunger strike. Ralph Goodale refuses to meet with them. buff.ly/29P8YZX #migrantstrike #cdnimm

CouncilofCDNs
15 people have died in detention. Tell @RalphGoodale meet the 60 hunger strikers #not1more #endimmigrationdetention

CBrentPatterson
The @CouncilofCDNs-Peterborough calls on @MaryamMonsef to urge @RalphGoodale to meet with detainees, canadians.org/blog/peterboro... #migrantstrike

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

620 CKRM
Active #weather over #Saskatchewan to bring more unstable conditions #skstorm #yqr http://bit.ly/29J0FDW

620 CKRM
#SKSTORM : Still some #wx watches in SE #SK. Humidity will be a factor today. High #humidex forecast. #SK #yqr

GlobalEdmonton
A sterilization error at an Edmonton medical clinic may have exposed hundreds of patients to Hepatitis B and C. glbn.ca/otSXJu

CBCNL
Huge military aircraft visits St. John's International Airport
cbc.ca/1.3684980
#cbcnl pic.twitter.com/s4SbXz654d

TreeCanada
RT @OpenTreeMap: @TreeCanada helping Fort McMurray replant urban10K trees after fire in May #urbanforestry bit.ly/29R8ULl https://pic.twitter.com/ofPQeEXNly

CBCNorth
Glimpsing the future: Researchers predict how fires will change N.W.T. forests cbc.ca/news/canada/no...

NATIONAL SECURITY / SÉCURITÉ NATIONALE

CSIS Canada
DYK: we've been a Top 100 Canadian employer for 8 years (and counting)? http://content.eluta.ca/top-employer-csis ...

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

VancouverSun
West Vancouver property developers caught in cross-country lawsuit ow.ly/4Q6Z502yA4s

calgaryherald
Varcoe: NAFTA is under fire, but should Canadians worry? calgaryherald.com/business/energ...

NEWS1130
CBSA asking Americans to leave weapons at home; 100s of guns seized locally in recent years bit.ly/29Wfv9u pic.twitter.com/x3GPskesKh

LAW ENFORCEMENT / APPLICATION DE LA LOI

660NEWS
RCMP warn about scammers pretending to be #STARS Lottery 660news.com/2016/07/19/rcm...

xpress_local
Man accused of ramming into Mountie cruiser released on bail: localxpress.ca/local-news/man... pic.twitter.com/Zth0UyLqjC

Canoe
RCMP get more than 850 complaints in Manitoba over Canada Revenue Agency scam cnews.canoe.com/ pic.twitter.com/6CNM4MjKuu

cbcnewsbc
Mystery of Hudson Brooks shooting death sparks emotional rally ift.tt/29KZ5NQ

OttawaCitizen
Two Ottawa men charged following July 11 grow-op raid in Beckwith Twshp. ow.ly/pME0302okQd #ottnews

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

CJAD800
West Islander serving time for murder of his wife dies in prison at Sainte Anne des Plaines. Corrections Canada investigating.

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

CBCNS
Tasty Budd's in Cole Harbour still considered illegal business: UARB bit.ly/2a4Tu8h pic.twitter.com/qIXBS5OTKz

chronicleherald
Tasty Budds marijuana dispensary illegal, says review board herald.ca/hwP pic.twitter.com/7YoadFs1yh

Althia Raj
Marijuana task force faces 'fascinating journey' in crafting legal framework writes Daniel Leblanc

PUBLIC SERVICE / FONCTION PUBLIQUE

PSACNCR
Unpaid Parks Canada staff are getting so desperate — they're borrowing money from their parents cbc.ca/news/canada/ca… #cdnpoli #canlab

OTHER / AUTRE

CBCPolitics
Ottawa's diplomatic shakeup removes high-profile Harper appointees. CBC.ca/1.3685157 #cdnpoli #hw

INTERNATIONAL

CTV News
UPDATE: Islamic State group claims teen's axe-and-knife attack on German train http://ow.ly/IRwp302oc49

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

Today's News / Actualités
July 31, 2016 / le 31 juillet 2016
9:00 - 18:00 ET

This collection contains news items that appeared online between 9:00 a.m. and 6:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 09h00 et 18h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Dorchester residents hope prison farm returns
Mel Goodland and other Dorchester residents are hoping the local penitentiary gets its prison farm program back. "I think the biggest thing that was lost was the identity because the inmates that I have spoken to over the years that worked on the farm enjoyed the fact that they got to work," said Goodland, a cranberry farmer and former mayor, who served when the prison farm system was operational."And the local people had pride in the farm because it was recognized as one of the better farms in the region. And it was a sad time when the farm closed." In 2010 the federal government decided to stop the six prison farms across the country. Federal Minister of Public Safety and Preparedness Ralph Goodale started a feasibility study to examine Ontario's previous two prison farms in the Kingston region. CBC News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Driving over ramp too fast may have damaged temporary water line in Saskatchewan
Government officials say efforts to activate a temporary water pipeline following an oil spill into the North Saskatchewan River were interrupted by what they suspect was a motorist who drove over the line too fast. Workers have been building the 30-kilometre-long pipeline for more than a week in order to supply Prince Albert with an alternate source of water after the city of about 35,000 shut its intakes to prevent oil from the spill upstream from entering its treatment plant. Duane McKay, Saskatchewan's commissioner of emergency management, says the line crosses a highway in several places. McKay says there are ramps at the crossings, but he says it appears a driver may have failed to obey the speed limit at one of the crossings on Saturday and damaged the line. The city has been relying on stored water from reservoirs and a retention pond since the Husky Energy pipeline near Maidstone leaked up to 250,000 litres of oil and other materials into the North Saskatchewan more than a week ago. McKay says he believes the damage to the water pipeline has been repaired, but doesn't know how much of a delay the incident caused. Canadian Press (iPolitics)

Heavy rains flood parts of Fort McMurray, closing roads and causing power outages
After going through hell, Fort McMurray is going through high water, as heavy morning rainfall floods parts of Gregoire, downtown and Thickwood. People who had spent weeks clearing smoke fumes out of their homes woke up to flooded basements and leaking roofs. The high waters formed pools on the road that are deep and wide enough to make regular traffic impossible. Roads throughout the city have been closed, as work crews scramble to divert flooding with barriers and use vacuum trucks to suck up the rising waters. Power outages have been reported across the city. For the first time since May's wildfires, the municipality activated the Regional Emergency Operations Centre around 11 a.m. A state of emergency has not been declared by any level of government. No evacuations, mandatory or voluntary, have been announced for any area of Wood Buffalo, although the municipality is asking people to restrict travel and respect any barricades. National Post; Canadian Press (CFJC Today)

Vernon wildfire: Evacuation order rescinded
The City of Vernon rescinded its evacuation order for residents of Adventure Bay Sunday morning after firefighters contained an aggressive wildfire east of the community. The fire started shortly after 9 p.m. Saturday and quickly grew due to high winds and difficult terrain. Firefighters worked through the night to bring the fire under control and at about 1 a.m. Sunday, 60 residents had been evacuated. "Although all the fires are not yet extinguished, they are contained and crews from Vernon Fire Rescue Services and The Ministry of Forests, Lands and Natural Resource Operations are still mopping up," the news release said. "Helicopters are being used for water drops to aid in fighting the fire in challenging terrain." As of Sunday 11 a.m., displaced residents were being allowed to return home. There was no structural damage due to the fire. The Province; Vernon Morning Star

Missing hiker located near Buntzen Lake area
Coquitlam Search and Rescue have rescued 21-year-old Alec Winter. Winter had been missing since last Friday when he went for a hike along the Dilly Dally trail on Eagle Ridge but never returned. Michael Coyle with Coquitlam Search and Rescue says Winter was found on the opposite side of the ridge where he was supposed to be hiking. Global News; 640 AM Talk Radio; News 1130

First Nations fisherman falls into Fraser River at Soda Creek
The search is on for a fisherman who fell into the Fraser River early Sunday morning at Soda Creek north of Williams Lake. RCMP Staff Sgt. Del Byron said police were called at 1:45 a.m. July 31 when it was reported that approximately 20 minutes earlier a man had fallen into the river while fishing. Byron said members of the Central Cariboo Search and Rescue team set up spotters at Sheep Creek Bridge in the night and began ground and air searches at daylight. Williams Lake Tribune

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Nuttall and Korody back in Victoria following release

During this busy B.C. Day long weekend, the grounds of the B.C. legislature will be bustling with tourists and locals. It was a similar scene three years ago on Canada Day, when a couple from Surrey were recorded by RCMP cameras, putting what police believed to be lethal pressure-cooker bombs around the legislature building. Victoria Councillor Charlayne Thornton-Joe was in the crowd that day. "We're definitely more vigilant than we've been in the past," she said. Michael Vonn, with the B.C. Civil Liberties Association, said it was clear from the beginning it had been an RCMP "plot." And Duke Islamic Studies Centre Director, Omid Safi, agrees. "They were in charge of radicalizing him. They passed on erroneous information to him, only then to turn around and arrest him," Safi said. Safi was an expert witness during the Nuttall and Korody trial. The couple have been released on a Peace Bond while the Crown appeals the case. Global News learned the pair boarded a BC Ferry after leaving the courthouse Friday night. They decided to spend their first night of freedom in three years, back in Victoria. But many in Victoria were not too happy to learn the couple was back in the city where the alleged terrorism sting had been carried out. Nuttall and Korody have several bail conditions banning them from possessing weapons or accessing Jihad extremist internet sites. They are also prohibited from visiting the B.C. legislature. Global News

BORDER SECURITY / SÉCURITÉ FRONATLIÈRE

Border mayors want feds to resolve bridge delays
Niagara's three border mayors plan to write a letter next week calling on the federal government to address the traffic backups that have been a frequent problem at bridges into Canada this summer. "We're all feeling the pain. It's very frustrating," said Niagara Falls Mayor Jim Diodati, adding counterpart mayors in the U.S. are equally frustrated. Diodati said he has heard from people that it has taken them more than an hour to come back to Canada on Niagara's bridges. He said even at the Whirlpool Bridge, which is a Nexus-only crossing, it took motorists half an hour to come into Canada Saturday. "This is having an impact on cross-border trade and tourism and it needs to be addressed right away," he said. "We have seen the pendulum swing on this side of the border – the dollar is encouraging Americans to come back and gas prices are relatively inexpensive." Diodati said Canada Border Services Agency does not have appropriate staffing levels at the bridges, and that he, along with Fort Erie Mayor Wayne Redekop and Niagara-on-the-Lake Lord Mayor Pat Darte, will send a letter to the federal minister responsible for CBSA, as well as Prime Minister Justin Trudeau, outlining their concerns. Niagara Falls Review

Passengers try to fly out of Canadian airports with tear gas, blades, Tasers, guns and drugs
It should be no surprise to anyone who has travelled through an airport that there are some common-sense restrictions on what we are allowed to bring along in our carry-on baggage. Things such as meat cleavers, shotguns, rifles, handguns, live bullets and all manner of butterfly knives, switchblades and, yes, even throwing stars are all items we should leave at home with our far more benign household items... Through access to information requests, CBC News has obtained a list of items seized or identified as potentially dangerous by the Canadian Air Transport Security Authority (CATSA) at airports across the country from Jan. 1 to Dec. 31, 2015. Here's a look at ten of the most interesting incidents: The fake grenade. CBC News

Now all the new train station needs is passengers
An editorial states, "As Niagara Falls celebrates its $42 million train station — to open later this summer — it is a time of hope for the revival of rail passenger service to this city and across the state. That is indeed one 21st century challenge for the Cataract City... Meanwhile, the Cataract City is uniquely positioned at the U.S.-Canada border to benefit from international travel between two of the most important destinations in North America, New York City and Toronto. Being a widely acclaimed magnet for tourists, Niagara deserves at least a better piece of that action..." Niagara-Gazette

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

Manitoba man charged in alleged cocaine smuggling ring in Ontario
A Manitoba man was arrested after a two-year RCMP investigation following cocaine from Mexico to Canada. The man was arrested on Friday near Rosenort, Man. and charged with conspiracy to traffick cocaine, while three other people were being arrested in Ontario in relation to the investigation. During the investigation, police seized more than two kilograms of cocaine and uncovered what it called "sophisticated concealment methods which enabled the cocaine shipments to cross international borders." Officers with the RCMP, CBSA, OPP and the Chatham-Kent police worked in tandem on the investigation, according to a media release from the RCMP. CBC News

RCMP vehicle involved in Highway 101 collision
Highway 101 is shut down between exit 19 and 20 following a collision involving an RCMP cruiser and a civilian vehicle. Traffic is being diverted along Highway 1 until around 6 p.m. Sunday evening. Traffic analysts are assisting at the scene. RCMP say the crash happened around 9:40 a.m. Sunday morning. The driver of the RCMP cruiser and the two people in the civilian vehicle had minor injuries. CBC News; Torstar (Cape Breton Post, Hamilton Spectator); CTV News; Metro News

RCMP execute search warrant in Rosenort
A two year investigation by the RCMP into the importation and trafficking of cocaine concluded this past week, resting in multiple arrests of individuals from both Manitoba and Ontario. These individuals were involved in the importation and subsequent distribution of cocaine. My Steinbach

Un policier de la SQ accusé de voies de fait
Nicolas Landry, un policier de la Sûreté du Québec, a été arrêté jeudi à l'aéroport Montréal-Trudeau. Il a été accusé ce matin de voies de fait et de non-respect des conditions au palais de justice de Saint-Hyacinthe. C'est la troisième fois qu'il est arrêté en moins d'un an. Radio-Canada

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

'We are reliving it:' Victim of serial rapist Larry Takahashi speaks as her as attacker is freed on day parole
There are no pictures of Erica Hammermeister. None in her house. None on her phone. She hasn't allowed one to be taken since March 1982, since the night she was raped by a masked man in the utility room of her downtown Edmonton apartment building. "There are none, that's the sad fact," said Hammermeister, 56. "I moved 10 times in less than eight years, just because I did not want to be found. To this day, I don't own a house, I don't own a car, I don't own credit cards. There is no way that anybody can find me." On that March night more than three decades ago, Hammermeister came home from a evening out with friends. When she pressed the button to call the freight elevator, Larry Takahashi, known as the 'Balaclava Rapist,' stepped out of the shadows and held a knife to her throat... The other charges were stayed or withdrawn as part of a plea deal, according to the Parole Board of Canada. In court, Takahashi admitted to "hands-on" attacks of 29 women. He sexually assaulted one woman in front of her children. CBC News

Broadcast Media / Médias télédiffusés:

CBC News provided a report on Larry Takahashi receiving day parole. Rough Transcript

Dénicher du boulot après un séjour à l'ombre: pas toujours évident
Les obstacles dressés devant un détenu qui sort de prison ou encore d'un pénitencier fédéral après avoir purgé une longue peine peuvent parfois s'avérer ardus à surmonter... De là la raison d'être du Centre de placement spécialisé du Portage (CPSP). Peu connu du public en général, le CPSP œuvre pourtant à

Gatineau depuis 40 ans. Financé en quasi-totalité par Emploi-Québec, l'organisme à but non lucratif «s'occupe de la clientèle judiciarisée adulte» de l'Outaouais, explique son directeur général, Michel Allard... «Soixante pour cent des gens débarquent chez nous par eux-mêmes. Quelques-uns nous sont référés par le service de probation du Québec, d'autres par Service correctionnel Canada. Parfois aussi, les gens entendent parler de nous par l'entremise d'amis, d'autre par les intervenants d'une maison de transition.» L'analyse du dossier criminel et la confection d'un plan d'action personnalisé constituent deux étapes incontournables «pour préparer le retour de la personne sur le marché du travail», indique M. Allard. Info07.com

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Fentanyl fears: Surrey woman would have chosen pain relief alternative
The fentanyl Lynette Killam was administered after her colonoscopy last week is not the same as the street pills - manufactured and pressed illegally - that have been responsible for an overdose epidemic in Metro Vancouver in recent months. The prescription version Killam took is intended for pain relief, but it's still a powerful opioid. "That first day was not so bad, but the next morning when I got up I was tense, agitated, depressed," Killam said. "I was not in a good way at all. It felt awful. I don't have a good clinical word to describe it." CTV News (2016-07-30)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Legalize pot, but bring in quality controls
Back in the day, when Canadians bought their weed from a mustachioed guy in a '72 Camaro in a back parking lot, there was no quality control. You forked over 10 bucks and hoped you didn't get a dime bag of schwag in return. Today, marijuana has gone mainstream and upscale. It's sold in dispensaries that could be mistaken for tea shops, by dudes and dudettes in Rasta tams, who can lecture earnestly about the comparative benefits of strains named Triple Diesel and Golden Goat while they weigh purchases on a digital scale. Yet despite fancy digs and botanical baristas, most dispensaries have about the same quality control as the guy in the '72 Camaro. Globe and Mail

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

NIL

INTERNATIONAL

France church attack: Two arrested over priest's killing

Two men have been placed under formal investigation over the murder of a priest in a Normandy church, including a cousin of one of the killers. Farid K, 30, a cousin of attacker Abdel Malik Petitjean, was arrested on suspicion of terrorist association. The other man, named as Jean-Philippe Steven J, 20, was put under formal investigation for attempting to travel to Syria in June with Petitjean. Petitjean and fellow attacker Adel Kermiche were shot dead by police. They had interrupted the church service in Saint-Etienne-du-Rouvray last Tuesday, taken hostages and slit the throat of Father Jacques Hamel, 86. The Paris prosecutor's office said both men arrested on Sunday were being held in custody. BBC News; AFP (Canoe); Reuters (Radio-Canada)

Al-Shabaab claims a car bomb attack that killed 10 in Mogadishu
Militants set off two car bombs outside a police base in Somalia's capital before gunmen stormed inside on Sunday, leaving at least 10 people dead, police said. Islamist group al-Shabaab claimed responsibility for the assault on the headquarters of Somalia's Criminal Investigation Department (CID) in Mogadishu. "At least 10 people including four militants, five civilians and a soldier died in today's attack," Hussein Ali, a police officer, told Reuters. Another 15 people were injured, some seriously, he added. VICE News; UPI.com

Kabul explosion: Huge blast rocks Afghan capital
Witnesses said the blast struck at about 01:25 local time (20:55 GMT Sunday) and was heard across most of the city. Reports on social media indicated that the electricity in parts of Kabul briefly cut off shortly before the explosion. The cause of the explosion is not yet clear, but reports indicate it may have happened in a gas storage facility. Afghanistan's Tolo news organisation said the explosion happened in the Pul-e-Chakri area to the west of the city. Last week, two suicide bombers linked to the so-called Islamic State (IS) killed 80 people and wounded 230 more in Kabul. BBC News

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

DavidHeap
Tell @RalphGoodale no #child should be held in #immigration #detention! Act w/@AmnestyNow bit.ly/28Jkdms #CanPoli #MigrantJustice

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

ipoliticsca
Activation of temporary water line for Prince Albert interrupted | iPolitics http://ift.tt/2aCU79Z

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Star_Politics
Snowden made Canadian spies review contractor policy on.thestar.com/2aqm8OA #cdnpoli

natnewswatch
Snowden made Canadian spies review contractor policy on.thestar.com/2aoORFJ via @TorontoStar

LAW ENFORCEMENT / APPLICATION DE LA LOI

RCMP_HC
Memorial plaque unveiled for RCMP Cst. Sarah Beckett cbc.ca/news/canada/br...

CTVAtlantic

RCMP vehicle struck by car in Annapolis County: A Nova Scotia Mountie escaped with minor injuries after his R... bit.ly/2arKuqy

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

CBCNews
'We are reliving it:' Victim of serial rapist Larry Takahashi speaks as her as attacker is… ift.tt/2a98Ide pic.twitter.com/l3z0aUJCUc

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

globeandmail
Legalize pot, but bring in quality controls trib.al/aH01Pqj @GlobeDebate pic.twitter.com/l5DdsYPOWJ

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

Today's News / Actualités
August 2, 2016 / le 2 août 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Mohamed Harkat girds himself for another fight to stay
Mohamed Harkat — an Algerian who says he was wrongly accused of being an Al Qaeda sleeper agent — hopes he can finally win his freedom and the right to stay in Canada. "What the government is doing is wrong, and it's not fair," Harkat said in an exclusive interview with the Star. "And they got the wrong guy." Harkat, who came to Canada in 1995 and claimed refugee status, has been fighting deportation since his arrest on a national security certificate in December 2002. He still dreams of one day becoming a Canadian citizen, even though his life in Canada has been very different from what he'd expected. "I thought one day I would have children, a house, a family . . . everything is destroyed. When I met Sophie, we had a plan to buy a house and have children." The 47-year-old Harkat says he's innocent and will face torture and persecution in his native Algeria if he is deported. Canada Border Services Agency did not comment on the specifics of the case, but confirmed that Harkat is under a removal order, following a

Federal Court decision upheld by the Supreme Court of Canada. Esme Bailey, a senior media spokesperson for CBSA, added that the removal order "can only be enforced once due process under the Immigration and Refugee Protection Act has taken place." A February 2016 CBSA document — marked top secret — states that, "should Mr. Harkat be allowed to remain in Canada, it can be presumed that, given the opportunity, he would work toward the ends espoused by the Bin Laden Network." It recommends his removal from Canada. His lawyer, Barbara Jackman, plans to argue, in a formal petition to the **public safety minister**, that Harkat will face torture and persecution if sent back. She also plans to argue he is not a threat to Canada and should be allowed to stay on humanitarian grounds. In early September, she will seek an exemption from deportation. (…) Organizations such as the Canadian and B.C. civil liberties associations have added their voices to those asking **Minister of Public Safety Ralph Goodale** to exempt Harkat from deportation. If Goodale decides there is no risk of torture and opts to send Harkat back, Jackman says there will be a constitutional challenge. But Harkat is hopeful the new Liberal government will decide he is not a threat to Canada and will allow him to stay. Toronto Star

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Husky oil spill: Prince Albert water situation stabilizing
After an oil spill last week, officials in Prince Albert, Sask., say the city's water situation will slowly be returning to normal. Water from the South Saskatchewan River will flow into the city's water reservoir today. Last week, city workers began building a 30-kilometre emergency waterline connecting the city's water treatment plant to the South Saskatchewan River. Now, after several days of testing, officials are convinced that the water is ready to be treated. CBC News

Emergency medical cards help rural Albertans with special needs better communicate with first responders
A non-profit organization that serves special needs Albertans living in rural areas has developed a program to help its clients better communicate with police, paramedics and firefighters. The 1st Response Emergency Details, or 1st R.E.D., is a pocket-sized card that provides first responders with important patient medical information. CBC News

Nuke the oilsands - Alberta's narrowly cancelled plan to drill for oil with atomic weapons
It's often forgotten what a technological feat it was to pump oil out of the Fort McMurray area. While it's long been known that the Athabasca region is swimming with petroleum, geologists spent decades banging their head against the problem of how to turn oily sand into something that could be refined into gasoline. National Post

OPP locate body of missing Michigan woman in Lake Erie
Ontario Provincial Police have located the body of a woman who went missing on Lake Erie Sunday afternoon. Police said the Michigan woman's body was discovered around 8:45 p.m. on Monday. Officers with Essex County OPP marine unit, emergency response team, K-9 unit, helicopter and underwater search and recovery unit had been searching for the woman since she went missing around 4:30 p.m. Sunday. Windsor Star

Two boaters OK after BC ferry sails to the rescue of grounded vessel
A BC ferry travelling between Duke Point, on Vancouver Island, and the mainland has been involved in a rescue. BC Ferries spokeswoman Deborah Marshall says the Coastal Inspiration was called to assist Tuesday morning when a 10-metre pleasure boat ran aground off Valdez Island, south of Gabriola Island, in Georgia Strait. Canadian Press (Eagle Valley News)

More flare training for SAR-Techs tonight
There will be more flare training taking place in the skies over the Quinte Region tonight. Members of CFB Trenton's 424 Transport and Rescue Squadron will be shooting off search and rescue flares over Lake Ontario, south of Brighton and west of Prince Edward County, starting at 9:00 tonight. A C-130 Hercules will be flying at about 5,500 feet and launching the yellow-white flashes, to help SAR-Techs train for night time missions. Quinte News

North Shore Rescue to talk funding with local Liberal MP
North Vancouver Liberal MP Jonathan Wilkinson says he wants to help North Shore Rescue solve its funding problems. But first, Wilkinson said he must determine if the federal government is the correct jurisdiction to provide those funds. CBC News

Resources called in to locate missing child at Cobourg beach
Children getting lost isn't an uncommon occurrence along the Cobourg beach throughout the summer months but on Saturday when an 11-year-old was last spotted in the waters of Lake Ontario a number of resources were called in to search. Cobourg Police, lifeguards, Northumberland OPP Marine Unit, YIPI students, and a Search and Rescue helicopter from CFB Trenton were called in for the search that lasted nearly an hour. Lifeguards organized volunteers who joined arm-in-arm walking through the water in a grid searching for the child. In the end, the child was located along the beach by Cobourg Police and returned back to his parents safe and sound. Northumberland Today

Search and rescue training for trouble
More than a dozen search and rescue (SAR) personnel from Drumheller, Strathmore, Calgary, Olds, Sundre and elsewhere have taken part in a six-day training course at Cipperly's Pond Campground south of Olds. Held over two weekends, the course saw participants take part in various exercises, lectures and hands-on indoor and outdoor training. Events were also held at the Olds SAR building. Mountain View Gazette

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Snowden made Canadian spies review contractor policy
When Edward Snowden began leaking secrets about mass surveillance in the United States, Canada's electronic spy agency quietly wondered if their security screening was sufficient to stop a copycat. Newly released documents show some of the behind-the-scenes actions taken by the Communications Security Establishment (CSE) three years ago, when contractor Snowden first pulled back the curtain on the West's pervasive mass surveillance capabilities. Whatever changes were contemplated have been blacked out from the heavily censored document, most watermarked "secret" or "top secret." While the documents note that CSE is generally confident in its security clearance process for contractors, officials added that contractors are only "assessed for engagement for short, defined periods of time." (…) The secretive spy agency, who had received less than 40 media calls in 2012, was suddenly thrust into the spotlight. "As CSE has not been able to provide the level of detail about activities that the media requested, academics, so-called experts and commentators have provided their opinions on the subject," the memo reads. "While some commentators have been well-versed on the issues, and have outlined accurate accounts of CSE activities, others, including [name censored] have inaccurately represented CSE's activities and authorities." "CSE has been accused of being too secretive, which has led to misunderstandings of the agency's activities and authorities. This has highlighted the need for outreach to the academic community and to the media." CSE's communications staff recommended a briefing for academics and journalists, including reporters at the Star, La Presse, the Globe and Mail, the CBC and a number of other outlets both Canadian and international. It does not appear that briefing took place. CSE did give a briefing earlier this year, when its independent oversight body revealed the agency had inadvertently broken the law by transferring Canadian metadata to international partners. It was touted at the time as the first press conference in CSE's 70 year history. Toronto Star

Risque terroriste : l'Université Laval outille ses étudiants
En raison du contexte actuel de risque terroriste, les étudiants de l'Université Laval qui comptent se rendre en échange à l'étranger devront obligatoirement suivre deux nouvelles formations sur le terrorisme. Ces deux ateliers, qui portent respectivement sur la menace terroriste et la sécurité, s'intégreront à la formation sur l'adaptation culturelle qui est déjà offerte aux étudiants. Ces formations ont été mises sur pied par un professeur expert en terrorisme de l'Université Laval et un militaire à la retraite. « Il n'y a plus d'endroit à l'abri dans le monde. Il faut vraiment être attentif », affirme la vice-rectrice aux études et activités internationales de l'Université Laval, Nicole Lacasse. « Ça fait partie du bagage qu'un

voyageur doit avoir aujourd'hui. On veut essayer de contrôler les risques. » Échanges en Turquie En raison de la tentative de coup d'État du 15 juillet en Turquie et de l'état d'urgence qui a été décrété, l'Université Laval a pris la décision de ne pas y envoyer d'étudiants pour la prochaine session. Affaires mondiales Canada a baissé la cote de sécurité de la Turquie à 3. Les universités québécoises envoient des étudiants seulement dans les pays dont la cote est de 1 ou 2. Chaque année, une moyenne de 1000 étudiants quittent l'Université Laval pour se rendre à l'étranger. Radio-Canada

Sur les traces de ces sectes qui se cachent au Canada
Un auditeur nous demande de lui faire un portrait de la présence des sectes au Canada. À ce chapitre, la meilleure référence au pays demeure celle d'Info-Secte qui débat en français et en anglais du visage contemporain des sectes en sol canadien. Cet organisme qui se fixe comme but de venir en aide aux personnes qui ont été victimes d'abus à la suite de leur adhésion affirme que la présence des sectes au pays est beaucoup plus importante qu'au moment de sa fondation en 1980. La poussée des points de vue extrémistes et terroristes contribue beaucoup à cette impression. De fait, un grand débat a lieu au Canada comme en France autour du phénomène de la radicalisation des jeunes musulmans qui adopte au contact du web bien souvent des comportements qui s'apparentent à ceux exhibés par les victimes de sectes. Mais une secte n'est pas seulement une communauté d'esprit aveuglée par une série de croyances uniques et partielles, mais aussi une communauté réelle d'hommes et de femmes qui entretient une proximité physique au point de former un clan exclusif et fermé dans un lieu géographique donné. Selon cette définition, les jeunes terroristes ou brebis égarées ne sont pas des membres d'une secte au sens conventionnel. Radio Canada International

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Passengers find knife on Air Canada flight leaving St. John's
Air Canada is dealing with a security breach after a St. John's couple found a knife on one of their assigned seats as they boarded AC1197 to Toronto on Saturday. Glenn Deir said his wife, Debbie Youden, discovered the knife when she sat on it. (...) Deir said he showed the knife to the window seat passenger, folded the potential weapon back up and put it in his pocket until everyone had boarded the 6:30 a.m. flight. Then he "discreetly" approached the flight director. (...) He said the incident speaks to the need for better screening of airport workers. CBC News (2016-08-01)

Le Canada augmentera la protection des passagers victimes des compagnies aériennes
Le ministre des Transports du Canada, Marc Garneau, vient de terminer une série de consultations pancanadiennes sur un éventail de questions touchants les transports. Il a ainsi entendu des plaintes variées allant de mesures de sécurité excessives à des cabines exiguës et des vols où plus de billets ont été vendus qu'il n'y a de sièges disponibles dans l'avion. Le porte-parole du ministre, Marc Roy, déclare que le manque de protection des passagers est un thème récurrent et que c'est une grande préoccupation des Canadiens : « c'est une question qui a été soulevée d'un océan à l'autre » précise-t-il. Les histoires abondent sur les passagers des compagnies aériennes frustrés par un mauvais service, y compris le cas cet été d'un garçon de 15 ans qui a fini par dormir une nuit sur le plancher de l'aéroport international Pearson de Toronto après avoir perdu son siège sur un vol d'Air Canada. On ne lui a fourni qu'un simple bon alimentaire de 10 $. (...) En juin, le Canada a annoncé la création d'un nouveau bureau fédéral qui traitera les plaintes des voyageurs éprouvant des problèmes aux aéroports en raison des listes de sécurité aérienne. Radio-Canada

Pregnant Canadians urged to avoid parts of Florida because of Zika virus
The Public Health Agency of Canada is urging pregnant women and women planning to get pregnant to avoid travelling to parts of South Florida with reported cases of the Zika virus. The advisory comes as the State of Florida reports additional cases of Zika virus infections transmitted by local mosquitoes in small areas of Miami-Dade and Broward Counties. (...) "Zika virus is occurring in many regions of the world, although local transmission of Zika virus was first reported in the Americas in 2015," the advisory states. "There have been travel-related cases of Zika virus reported in Canada in returned travellers from countries with ongoing Zika virus outbreaks." (...)That outbreak started in Iowa and spread to nine states, several of which were on the Canadian border. Toronto Star

Bridge takeover bad idea for Canada
A letter to the editor states, "Canada buying Ambassador Bridge - Does it make sense? Opinion column by Anne Jarvis, July 28. This deal only makes sense if, in effect, Canada pays all of Matty Moroun's legal expenses over the past 15 years, pays for all of what he has provided in infrastructure for his bridge, and endows his family corporation with the most golden of handshakes for taking over what could be the whitest of elephants. Also, it would mean Canada assuming the cost of providing necessary repairs to an almost 100-year-old structure. In military terms, this is a tactical retreat to allow the enemy to come in and occupy territory no longer deemed necessary for defense and at a greater cost to himself." Windsor Star

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

Crime spree leads to arrest
Calgary's William Riley Gossen, 20, and Michaila Mitchell, 18, are facing a list of charges after an alleged multi-jurisdictional crime spree and police chase that took place last week. Calgary Police arrested the couple without incident at around 6 p.m. on July 27 in a Calgary apartment building, located in the 2000 block of 11 Avenue S.W., after seven hours of following them as they drove around the city. The Bonnie and Clyde style crime spree allegedly began just before 10 a.m. on July 25 in Mountain View county when Didsbury RCMP responded to a report of a residential break-in involving two suspects armed with a sawed-off shotgun. A homeowner returned to his rural home to find a red Hummer—later discovered stolen from Cochrane—parked in his driveway. A man and woman exited the home and demanded his keys, brandishing the gun and loading it with shells. The duo took off towards Carstairs. Mounties say the couple also searched for fuel at a different residence. They left and headed south on Range Road 12 in the Hummer. Airdrie Echo

UPDATE: Victim identified in potentially targeted Surrey shooting
The victim of last night's shooting in Surrey has been identified by IHIT as 27-year-old Sean Christopher Kelly. Homicide investigators say they believe the shooting was targeted. Court documents show a man with the same name faced several charges including trafficking and aggravated assault. Mounties were called to the 13900 block of Antrim Road last night around 8:30 to reports of an injured man. He later died. IHIT says it is now notifying the victim's next of kin. AM 730

Investigation continues into house fire
Tensions are running high in Happy Valley-Goose Bay where residents are concerned about a suspicious house fire on July 24 that claimed the life of an 88-year-old woman. As of Aug. 1, the RCMP said they have 15 members on the case and cannot release any further details as the investigation is ongoing. Reports from around town say the RCMP are searching areas and homes, even taking some people in for questioning. RCMP media liaison Rick Mills said the searches are related to the ongoing investigation, but no further information is available. A woman who lives in the area where police appear to be searching the most told the Labradorian that residents want more information from police, just to feel safe in their homes. "There's a tension over the whole town," she said. "Even just to come out and tell us they're searching the town for evidence, if they have suspects or should we keep our eyes out, should we keep our doors locked. Give us something. The murder on the island that happened recently, at least they put out a release saying they're looking for people. Even that." Labradorian

Local RCMP looking for help
100 Mile House RCMP is looking for assistance from the public to help solve the suspicious death of a Deka Lake man. The body of Gary Edwards, 72, was found in his home on July 29. Police believe foul play may be involved in the Edwards' death. Noting that he had not been for a week, the RCMP hopes

members of the public might be able to help establish a timeline leading up to his death. 100 Mile Free Press

Leduc RCMP investigate fatal railway collision
On the morning of August 1, Leduc RCMP responded to a report of human remains found by a passerby on the railroad tracks near Highway 2A and 50 Street in Leduc, Alberta. Officers arrived on scene to find a deceased adult male with injuries consistent with a train versus pedestrian collision. The Leduc RCMP were assisted in their investigation by Leduc Fire Services and CP Police Service. Leduc RCMP believe that the collision occurred sometime after 10 p.m. on Sunday, July 31. The identity of the deceased male is not known at the time of this release.The investigation remains ongoing. Leduc Rep; CTV News; Global News

No increased calls to police during Hells Angels gathering in Musquodoboit Harbour
As the Hells Angels makes its return to Nova Scotia, police say they are continuing to monitor biker gang activity, including a meetup this past weekend. RCMP say there was a Hells Angels gathering in Musquodoboit Harbour, at the former Gate Keepers clubhouse. That clubhouse was the site of an official opening of a Nova Scotia Hells Angels chapter last month, where a party was held to mark the club's return to the province. Police said there were no calls from the public about the meeting, but they were closely watching the activity. "We didn't have any increase in calls or anything like that because of it, but there was a lot of proactive work that was done over the weekend," says RCMP Cpl. Jennifer Clarke. CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Study suggests federal prisons blacking out errors in death reports: ombudsman
A study prepared by Canada's federal prison ombudsman says Corrections Canada consistently blacked out possible errors or shortfalls documented in investigation reports into jail deaths sent to families. Howard Sapers says in a study released Tuesday that his office compared the uncensored investigatory reports it received from Corrections Canada with the highly edited versions eight families obtained through access-to-information laws. The report says the "current practice of exempting errors, shortfalls and policy non-compliance leaves little room for public scrutiny, accountability or ... legal recourse." Titled "In the Dark," the 38-page study was carried out last year after some families complained to Sapers' office about their difficulty in receiving information about how loved ones died between 2013 and 2015. "It's very hard for me to conclude that all the redactions that I reviewed for this investigation were that legitimate. There were some redactions that I think Correctional Service Canada is going to have to explain," Sapers said in an interview. There were 65 deaths in 2015-16 in federal correctional institutions. Sapers' report says his office's advisor concluded that the blacking-out of sections of the seven reports, prepared by a panel that looks into non-natural deaths, "completely change the context of the information that is provided." But the report says the greater concern was the slicing out of sensitive material that might implicate Correctional Service Canada officials for failing to follow policy. (...) Sapers said he believes the edits were a misuse of the access to information law and privacy laws, given that the commissioner of Correctional Service Canada has discretion to release information in the public interest. (...) A spokeswoman for Correctional Service Canada said a response to the report will be provided later Tuesday. Canadian Press (Times Colonist, Western Star, Brandon Sun, iPolitics, Huffington Post, Truro Daily, Mississauga News, City News, CP24, St. John's Telegram, Prince Albert Daily Herald, CTV News, Coast Mountain News, The Guardian, Montreal Gazette); Presse canadienne (La Presse)

Prisons callous and secretive with families when inmates die: watchdog
Families of inmates who die in federal penitentiaries are told very little about what happened and complain that prison staff are “callous and unprofessional” in dealing with them, a report published by Canada’s prison watchdog charged today. In one case, a dead inmate’s cremated remains arrived without warning at a family member’s home in a Purolator shipment. Sapers started investigating how prisoners’ next of kin are treated after a death when three families complained to his office “in quick succession,” the report says. In cases where inmates were near death in hospital, Sapers found that families weren’t told at first that the situation was serious, just that the inmate had been hospitalized: “The

family reported being very upset because had they been better informed of the seriousness of the situation … they could have called the hospital to get more information and would have come immediately and been able to spend more time with the offender before death," he wrote. (…) In a response published today, federal prison officials conceded that "more can be done to facilitate the disclosure process." "We recognize that the death of a family member is an extremely challenging time, often made more difficult when he or she has been incarcerated away from his or her home community," the unsigned statement says. "We want to ensure that we are communicating with the families of offenders following a death in a clear, transparent and empathetic way." Global News; CBC News; Radio-Canada

Broadcast media / Médias télédiffusés :

CBC News reported that Correctional Investigator Howard Sapers released a report on how the federal government prisons treat the families of those who passed away in prison. (11:20ET, 13:20ET) Rough Transcript

Many radio stations mentioned that Howard Sapers, the Correctional Investigator, is raising concerns that families are not getting the whole story when inmates die behind bars. In a new study, Howard Sapers makes nine recommendations including one that urges investigative reports to be shared in a timely manner with the next of kin. (CHQR-AM, 11:35ET, CFFR-AM, 9:20ET, CHQT-AM, 12:40ET, CJOB-AM, 9:00ET, CBC-R, 11:00ET)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Northern Ontario students more likely to be cyberbullied, study finds
Students in northern Ontario face more cyberbullying than their peers in the rest of the province. (…) Those are among the findings of a new report titled The Mental Health and Well-being of Ontario Students, published by the Centre for Addiction and Mental Health. The report is based on data collected in a large-scale survey of students in Grades 7 through 12 called the Ontario Student Drug Use and Health Survey, which has been taking place every two years since 1977. A total of 10,426 students took part in the 2015 survey. CBC News

Red Deer tops province in Crime Severity Index
Red Deer is top of the Alberta list when it comes to the Crime Severity Index measured by Statistics Canada and some people tell CBC News that crime has started to hit more people at home. (…) Mayor Tara Veer says that's because the city has started working more closely with regional and provincial crime task forces. "We knew full well that if we were going to be more aggressive in terms of focusing on those areas, that it would translate into higher reported crime and higher arrests and convictions made." Veer says she's pleased violent crimes are generally trending down. CBC News

Crime down compared to last spring
Crime stats compiled by the Merritt RCMP show a slight dip in a number of offences this spring compared to last year. From April through June of 2016, police responded to 40 assault cases, 13 less than the 53 from the same time period last year. Break and enters also saw a dip between quarters. Last spring there were 11 break-ins reported to police, but only nine this year. Fewer vehicles were stolen too. Last year five vehicles were stolen between April and June, but only three were reported stolen this past spring. Theft of items from vehicles numbered 13 this past spring down from the 15 theft from vehicle files police had in the spring of 2015. However, one statistic that wasn't lower was the number of domestic dispute files, which can range from a verbal argument to a physical confrontation. Merritt Herald

Un festival de musique veut se doter d'une machine pour détecter le fentanyl
Le festival de musique électronique Shambhala, qui commence mercredi en Colombie-Britannique, lance une campagne de financement participatif en ligne pour se procurer une machine coûteuse permettant de détecter certains produits présents dans les drogues comme le fentanyl. Les organisateurs du festival espèrent amasser les fonds nécessaires pour acheter la machine, un spectromètre de masse miniature,

d'ici l'année prochaine. Pour l'heure, ils ont été incapables d'obtenir le financement de la part des gouvernements pour l'appareil qui peut coûter 250 000 $ ou plus. En attendant, cette année, ils distribueront 4000 dépliants pour mettre les festivaliers en garde contre les dangers du fentanyl. L'événement, qui a lieu depuis 14 ans sur un ranch dans les montagnes de la région Kootenay Ouest, aide depuis des années ses participants à découvrir ce que contiennent les substances qu'ils consomment en mettant à leur disposition des agents chimiques qui changent de couleur selon leurs compositions. Toutefois, ces produits ne détectent pas le fentanyl. « Nous devons agir très rapidement si nous voulons empêcher d'autres morts », dit Chloe Sage qui s'occupe des activités de réduction des risques depuis six ans pour le festival. Radio-Canada; CBC News

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Bennett to meet families of MMIW ahead of inquiry announcement
Indigenous Affairs Minister Carolyn Bennett will meet families of missing and murdered indigenous women tonight on the eve of the government's formal announcement of an inquiry into the deaths and disappearances. That Wednesday announcement will mark the end of the government's role in shaping the design of the inquiry and the beginning of work for the commissioners. It is expected that five commissioners will be appointed to the body. They will have the power to summon witnesses and to compel them to give evidence. The federal government has earmarked $40 million over two years for the inquiry but Bennett has said this is a placeholder budget. Key themes raised in pre-inquiry consultations included policing practices and the justice system, the role of colonialism and residential schools and poverty. Canadian Press (iPolitics, CTV News)

Winnipeg Indigenous leader calls Bobby Hull's hall of fame induction a 'slap in the face'
The head of the Aboriginal Council of Winnipeg says it would be a "slap in the face" to see Bobby Hull, an alleged abuser of women, inducted into the new Winnipeg Jets hall of fame. Damon Johnston, who also serves on mayor Brian Bowman's Indigenous Advisory Circle, says violence against women is a central issue within the Indigenous community, pointing to the upcoming inquiry on murdered and missing women. "It's a slap in the face to all of us. It's a step backward in time," he said of True North Sports and Entertainment's decision to honour Hull. "There's zero tolerance for violence against women. Zero. Period. No ifs, ands or buts, and the same with racism." Metro News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

NIL

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Récompense de 25 000 $ pour l'arrestation d'un terroriste canadien au Bangladesh
La police du Bangladesh offre des récompenses pour toute information sur deux islamistes, dont le Canadien Tamim Chowdhury. Ils sont accusés de mener des groupes extrémistes dans le pays. Le Canadien serait l'un des auteurs de l'attaque d'un restaurant de Dacca qui avait fait 20 morts, dont 18 étrangers, le 1er juillet. L'homme âgé d'une trentaine d'années, né au Bangladesh, est suspecté d'être le cerveau de l'attaque de Dacca. Mais il a disparu des écrans radars depuis le sanglant événement. Les services antiterroristes soupçonnent Tamim Chowdhury de diriger une faction du Jamayetul Mujahideen

Bangladesh (JMB), un groupe islamiste local interdit et accusé du meurtre de dizaines d'étrangers ou de membres de minorités religieuses. La police a annoncé une récompense de deux millions de takas (25 000 $) pour toute information conduisant à son arrestation. La police offre également une récompense pour retrouver un commandant renvoyé de l'armée, Syed Mohammad Ziaul Haq. Il est accusé d'être à la tête d'un autre groupe islamiste, Ansar al Islam, suspecté de meurtres d'activistes laïques. Radio Canada International

INTERNATIONAL

Gas dropped on Syrian town where Russian helicopter downed: rescuers
A Syrian rescue service operating in rebel-held territory said on Tuesday a helicopter dropped containers of toxic gas overnight on a town close to where a Russian military helicopter had been shot down hours earlier. The opposition Syrian National Coalition (SNC) accused President Bashar al-Assad of being behind the attack. Assad has denied previous accusations of using chemical weapons. A spokesman for the Syria Civil Defence said 33 people, mostly women and children, were affected by the gas, which they suspect was chlorine, in Saraqeb, in rebel-held Idlib province. The group, which describes itself as a neutral band of search and rescue volunteers, posted a video on YouTube apparently showing a number of men struggling to breathe and being given oxygen masks by people in civil defence uniforms. "Medium-sized barrels fell containing toxic gases. The Syrian Civil Defence was not able to determine the type of the gas," said the spokesman. The Syrian government and its Russian allies were not immediately available for comment. Reuters (Globe and Mail)

Bodies found off coast of Libya as migrant toll climbs
The bodies of 120 migrants believed to have been trying to reach Italy by boat from Libya have been found off the Libyan coast over the past 10 days, the International Organization for Migration (IOM) said on Tuesday. "We are getting this information from Libyan authorities that we are collaborating with," said IOM spokesman Joel Millman. The bodies had been discovered near Sabratha and had not come from previously known shipwrecks in the Mediterranean. Mainly African migrants are taking often unseaworthy boats from Libya to Italy, gateway to Europe. Nearly 8,000 were rescued at sea between Friday to Monday on that central Mediterranean route, Millman told a briefing. It is a longer and more perilous journey than that from Turkey to Greece, largely shut down since a deal was struck between the European Union and Turkey in March, although 174 migrants did make it by sea to Greece over the weekend, IOM said. CBC News

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

EndNRA
Ralph Goodale Yet To Confirm Meeting With Immigrant Detainees On Hunger Strike endthenra.com/ralph-goodale-... #UniteBlue, #EndTheNRA, #MomsDemand

ceasefireblog
@RalphGoodale The righteous fight against excesses of Ottawa's anti-terror law goes on #KillBillC-51 #cdnpoli ow.ly/EJqE302Q3JB

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

CBCSask
Update: Husky oil spill: Prince Albert water situation stabilizing #HuskyOilSpill cbc.ca/1.3703837 pic.twitter.com/MjopUMb7Rc

911_wire
Emergency medical cards help rural Albertans with special needs better communicate with first responders binged.it/2ayw9Jv

natnewswatch
Nuke the oilsands: Alberta's narrowly cancelled plan to drill for oil with atomic weapons canada.com/news/national/...

cbcnewsbc
North Shore Rescue to talk funding with local Liberal MP ift.tt/2arKvdr pic.twitter.com/UJx9JsQszZ

NATIONAL SECURITY / SÉCURITÉ NATIONALE

AlCanadaMedia
.@AlexNeveAmnesty: #MohamedHarkat at risk of incommunicado detention, torture if deported back to #Algeria on.thestar.com/2auQlcf

OxfordAmnesty
RT @AlCanadaMedia: .@AlexNeveAmnesty: #MohamedHarkat at risk of incommunicado detention, torture if deported back to #Algeria on.thestar.com/2auQlcf

georgiastraight
B.C. Civil Liberties Association rips into #RCMP following stay of proceedings in legislature terrorism case straight.com/news/746301/bc...

TheTyee
BC Terror Trial Verdict a Scathing Indictment of RCMP Management thetyee.ca/Opinion/2016/0... #bcpoli

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CTVNews
'Our jaws dropped': N.L. couple finds knife aboard Air Canada plane ow.ly/zdv8302QPSr pic.twitter.com/lzKDqPVaif

CBCNL
Debbie Youden sat on folded knife as she boarded flight AC1197 Saturday cbc.ca/1.3703311 pic.twitter.com/zHhf3Wumw8

Clnet
Le Canada augmentera la protection des passagers victimes des compagnies aériennes bit.ly/2aMi1k0

Star_foreign
Pregnant Canadians urged to avoid parts of Florida because of Zika virus on.thestar.com/2aNLQRl

RCPWindsor
WStar Opinion - Bridge takeover bad idea for Canada dlvr.it/LxMxgh #rcp #windsor pic.twitter.com/WJ2zAkgsw6

LAW ENFORCEMENT / APPLICATION DE LA LOI

CBCNS
Monitoring of Hells Angels meetup part of 'continuous' monitoring, say police bit.ly/2apo4aR pic.twitter.com/nPq4T2sKGs

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

RadioCanadaInfo
Les familles de personnes mortes en détention seraient mal informées, selon un rapport rc.ca/LxSV3y

Global_NB

In one case, a dead prison inmate's cremated remains arrived without warning at a family member's home by Purolator. glbn.ca/Z3Bpuz

globalnews
In one case, a dead prison inmate's cremated remains arrived without warning at a family member's home by Purolator. glbn.ca/foqa4q

infonewsvernon
Study suggests federal prisons blacking out errors in death reports: ombudsman goo.gl/10K2Mu pic.twitter.com/qaoy2yC3xG

NEWS957
Study suggests federal prisons blacking out errors in death reports: ombudsman news957.com/2016/08/02/stu…

HuffPostCanada
Prison watchdog fears death reports are being censored #cdnpoli huff.to/2aZOrDW pic.twitter.com/JlAoZVMTYi

natnewswatch
Study suggests federal prisons blacking out errors in death reports: ombudsman | National Newswatch nationalnewswatch.com/2016/08/02/stu…

CityNews
Study suggests federal prisons blacking out errors in death reports ow.ly/1CT6302QypP pic.twitter.com/k8B7jBCElt

CBCCanada
Correctional service lacks compassion dealing with families of inmates who die: report ift.tt/2aKcr0M pic.twitter.com/gDzh77yT1M

CBCNS
Prison watchdog says correctional service withholds information from families of dead inmat… bit.ly/2arQDbE pic.twitter.com/rMn9kaIrQK

CBCNews
Inmate's ashes arrive at family's front door by courier after prison death: Watchdog's sca… ift.tt/2aKcr0M pic.twitter.com/POqY1XlxMU

CochraneCBC
Prison watchdog says correctional service withholds information from families of dead inmates cbc.ca/1.3700844

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

CBCTBay
Northern Ontario students more likely to be cyberbullied, study finds : cbc.ca/1.3704019 #tbay #CAMH

CBCEdmonton
Red Deer tops province in Crime Severity Index cbc.ca/news/canada/ca… #yeg

MerrittHerald
Crime down compared to last spring merrittherald.com/?p=309925 #Merritt, #NicolaValley

ici_cb
Un festival de musique veut se doter d'une machine pour détecter le fentanyl rc.ca/LxSFs2

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

YahooCanadaNews
.@Carolyn_Bennett to meet families of MMIW ahead of inquiry announcement yhoo.it/2as9fZg pic.twitter.com/DdtwUCQ5JA

ipoliticsca
Bennett to meet families of MMIW ahead of inquiry announcement | iPolitics ift.tt/2avmwxK

MetroNewsCanada
RT @metrowinnipeg: Winnipeg Indigenous leader calls Bobby Hull's hall of fame induction a 'slap in the face': ow.ly/5iPt302QcGw httpspic.twitter.com/WS9adMA92l

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

Today's News / Actualités
August 16, 2016 / le 16 août 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Trudeau says rights must be balanced with security in battling terrorism
An alleged terrorist plot in Ontario that created anxieties over police monitoring of suspects hasn't shaken Prime Minister Justin Trudeau's emphasis on balancing civil liberties with public safety. In his first reaction to an alleged plot that led to the death of Aaron Driver in Strathroy, Ont., Trudeau said Tuesday that balancing individual rights with keeping Canadians secure from bombing threats has to be handled with care. "Canada is a country that values its freedom (and) its basic charter rights," he said during a stop in Bridgetown, N.S., for an infrastructure announcement. "All Canadians expect their government to do two things: to keep Canadians safe and to defend and uphold the values and rights that all Canadians hold dear." "Getting that balance right isn't always easy in the challenging situation we now live in but it's

extremely important."...Trudeau said to applause from about 300 people gathered along the tranquil Annapolis River that he congratulates the security services and police for "having managed to prevent any serious incidents related to this particular individual." "It is something we continue to work very, very hard on to keep Canadians safe in their homes and communities right across this country." The prime minister mentioned the continuing presence of Canada's special forces in northern Iraq, where they are assisting in the war against the Islamic State of Iraq and Syria, also known as ISIS or ISIL. He said the wider response against domestic terrorism will be rolled out by **Public Security Minister Ralph Goodale** as the Liberals continue plans to reform former prime minister Stephen Harper's anti-terror law, Bill C-51. Parliamentary oversight. During the last federal election, the Liberals pledged to guarantee that all Canadian Security Intelligence Service warrants respect the charter, that the right to lawful protests and advocacy aren't violated, and they pledged to "narrow overly broad definitions (in Bill C-51), such as defining 'terrorist propaganda' more clearly." They also said a Liberal government would limit the Communications Security Establishment's powers by requiring a warrant to engage in the surveillance of Canadians and emphasize community outreach to battle radicalization of youths. Asked if the reforms are being revisited in light of cases like Driver's, Trudeau referred to the Liberals' plan to create an all-party committee of parliamentarians to oversee national security agencies. He said the committee will ensure the agencies "don't go too far and violate our fundamental rights and freedoms when they work hard to keep us safe." "But at the same time, oversight will ensure that our intelligence and security agencies do everything necessary to keep Canadians safe," said Trudeau. "This situation of last week and situations like it will be exactly the kind of thing I expect this committee of parliamentarians to weigh in on and advise how we can do an even better job of keeping Canadians safe, like we were able to do last week." Canadian Press (CBC News, Globe and Mail)

Toronto passed over for detention centre spending

The **federal public safety minister** says a $138-million plan unveiled Monday to replace two immigration detention centres in greater Vancouver and Montreal will ease pressure on an overburdened national system. However, **Ralph Goodale** offered nothing to expand or replace an immigration holding centre in the Greater Toronto Area...At the time **Goodale**, the minister responsible for Canada Border Services Agency, promised reforms were coming. On Monday at a news conference in Laval, **Goodale** pitched his announcement as the launch of a new national immigration detention strategy and a marked departure from the narrow approach of the previous Conservative government...**Goodale** stressed Monday that ***"the law says that detention should be the last resort, that the agency has to look at every other alternative. "Well, we've had — in my judgment — a list of alternatives in the past that is too limited. There aren't enough other choices to make."***...He said the new funding will reduce use of provincial jail facilities and mean ***"safer, more secure and humane detention conditions"*** in a system that will operate under consistent national standards. One of its objectives is to ***"minimize to the greatest extent possible the housing of children in detention facilities,"*** he said. ***"If we fail in our duty of care to the smallest among us then we fail the most basic test of justice and compassion."***...**Goodale** said the hunger strike that ended a couple of weeks ago underscored the ***"serious pressures within the system."*** He said he hoped his plan would ***"alleviate the root causes of those pressures,"*** and while the system wouldn't be ***"absolutely perfect and without flaw," this is "a major step in the right direction."*** He said he wrote the hunger strikers to explain ***"the broad nature of our plan"*** and to invite written submissions about why their individual detention is unfair or inappropriate, but had not yet received any written responses. Toronto Star

The Sprout: MacAulay, Freeland working on canola dispute with China

Good afternoon and welcome to the Sprout, where your host is told today is National Rum Day. In Canada: **Public Safety Minister Ralph Goodale** is headed to Kingston today for a town hall meeting over whether to reinstate some of Canada's prison farms. The meeting, which is set for 6 p.m. at Kingston City Hall, will be preceded by a rally organized by prison farm activists, who want the programs restored. Officials from Correctional Services Canada are also expected to be at the meeting. The National Farmers Union says it is opposed to Health Canada's plans to allow meat irradiation. In a press release Tuesday, the union said irradiation could instil "a false confidence in the meat's safety." Canada's food safety system, the NFU insisted in its submission, should instead be a priority for officials - including an increase in inspections and improved regulations. Irradiation is a process that exposes food to a controlled amount of energy called ionizing radiation in order to kill bacteria and prevent food poisoning

and spoilage. Canada's grain fleet is in serious need of repair, with more than 800 cars considered as "bad order" cars, a new federal report says. iPolitics

Le Canada veut prévenir la radicalisation de certains de ses citoyens
Au Canada, le gouvernement cherche des moyens pour prévenir la radicalisation de ses citoyens. Un dossier d'actualité alors que la police a dû abattre la semaine dernière un jeune homme qui avait projeté un attentat contre une ville canadienne. Le ministre canadien de l'Intérieur a visité, ce 15 août 2016, un centre spécialisé à Montréal au Québec. Dès cet automne 2016, le gouvernement canadien va mettre en place un bureau national pour lutter contre la radicalisation. **Ralph Goodale**, le ministre canadien de l'Intérieur, a annoncé la création de cet organisme alors qu'il visitait le Centre de prévention de la radicalisation à Montréal. Inauguré il y a un peu d'un an, ce regroupement de travailleurs sociaux, de chercheurs, de psychologues vient en aide à ceux et à celles qui s'inquiètent pour un proche. Jour et nuit, amis et parents peuvent joindre le Centre et leur demander conseil. Les Voix du Monde

'Traumatized' by jail, immigration detainee encouraged by government review of system
A French man detained at the Ottawa-Carleton Detention Centre while he awaited a Canadian work permit says he's encouraged the federal government is pledging to review and upgrade its system for detaining immigrants. Antoine Pacory says the experience last spring left him traumatized, and he welcomes news the minister responsible for Canada Border Services Agency will be looking at the system that landed him in jail. **Public Safety Minister Ralph Goodale** announced Monday the federal government would be adding $138 million to upgrade immigration detention centres as well as begin a review of alternatives to detention. ***"The government is anxious to address the weaknesses that exist and to do better," Goodale*** said. Pacory, along with his Ottawa lawyer Arghavan Gerami, have been fighting the decision to remove the 25-year-old from Canada and send him back to France. The deportation process began when a CBSA agent detained him in May, on the same day he was to receive his work permit from the federal government. CBC News

Public Safety Minister Goodale Outlines Intention to Combat Radicalization
Public Safety Minister Ralph Goodale says Canada must do better to be a leader in understanding and countering violent radicalization. **Goodale** says the death of Aaron Driver in Strathroy, who was suspected of planning a terrorist attack, demonstrates the need for ***"continued vigilance"*** in responding to threats posed by those who have been radicalized to the point of wanting to harm or kill innocent people. While there are no official plans in place, he says the federal government is working to create a new national office for community outreach and engagement that will help combat radicalization. There is no word on when the office will open, or if multiple locations will be established across the country. **Goodale** made his comments after visiting a centre in Montreal on Monday that works to prevent radicalization leading to violence. Last Thursday, the RCMP revealed that it was the FBI and not the Mounties who discovered a video that led them to Aaron Driver in Strathroy, who police said had threatened to detonate an explosive in an urban centre. Driver died Wednesday night after a confrontation with police that saw a bomb detonated in a taxi cab that was called to take him to Citi Plaza in London. An investigation continues to determine if Driver died from the blast or from a police bullet. AM980

Une stratégie nationale de lutte contre la radicalisation
Le gouvernement fédéral souhaite implanter une «stratégie nationale» pour la lutte contre la radicalisation menant à la violence. Hier, le **ministre fédéral de la Sécurité publique**, **Ralph Goodale**, a rappelé que les événements des dernières semaines», faisant référence à l'attaque terroriste déjouée en Ontario a démontré que nous avons besoin d'outils pour comprendre et agir en réaction au problème sérieux de radicalisation menant à la violence. L'analyse de Jocelyn Bélanger professeur de psychologie à l'Université de New York Abou Dhabi, spécialiste des processus de radicalisation. Radio-Canada

C-51 review expected to launch before Parliament resumes
The government's highly-anticipated review of its national security framework, including the Harper government's controversial anti-terrorism legislation C-51, is expected to start before parliamentarians return from summer break. "***Yes, it will be soon — so most likely before parliament resumes***," **said Scott Bardsley, press secretary for Public Safety Minister Ralph Goodale**. (…) In Bridgetown, N.S.

Tuesday, Trudeau reiterated his position on the importance of balancing security with civil liberties — a balance critics of C-51 said the previous government did not achieve. "All Canadians expect their government to do two things: to keep Canadians safe and to defend and uphold the values and rights that all Canadians hold dear," Trudeau said. "Getting that balance right isn't always easy in the challenging situation we now live in but it's extremely important." As **Goodale** recently re-iterated in a column with the Huffington Post, the problematic C-51 elements identified in the campaign platform are only the minimum of what the government will do to fix national security legislation. In particular, those elements include the need to "***ensure compliance with the Charter of Rights and Freedoms, full protection for advocacy and protest, the correction of appeal procedures in respect of 'no fly' lists, a more precise definition of 'terrorist propaganda', and a full review of all anti-terrorism laws after three years***." Input from Canadians could see those priorities expand during the course of the national security review, which is expected to wrap up this fall. A more specific timeline will be announced once the review is launched, **Bardsley says**. (…) In June, **Goodale** announced the creation of a new government office to support those travellers, with the eventual goal of allowing those travellers to apply for a unique identification number to distinguish them in aviation systems.That overhaul could take roughly a year and a half, **Goodale says**. iPolitics

Public Safety Canada launches public consultation on cybersecurity landscape
Public Safety Canada (PSC) has launched a public consultation on the "evolving cybersecurity landscape." On Tuesday, the federal government launched the Consultation on Cyber Security to help identify gaps and opportunities, bring forward new ideas to shape Canada's renewed approach to cybersecurity and capitalize on the advantages of new technology and the digital economy, PSC said in a statement. From now until Oct. 15, PSC will be leading the consultation by engaging stakeholders and Canadians on the trends and challenges of cybersecurity, as well as on new initiatives under consideration which will strive to build Canada's resilience, capability and innovation in cybersecurity, the department said. Topics of the consultation include: the evolution of the cyber threat; the increasing economic significance of cybersecurity; the expanding frontiers of cybersecurity; and Canada's way forward on cybersecurity. "***Canadians spend more time online than people in any other country***," **said Ralph Goodale, Minister of Public Safety and Emergency Preparedness, in the statement**. "***We need to get really good at cybersecurity – across our personal, business, infrastructure and government sectors – so we can take full advantage of the digital economy, while protecting the safety and security of Canadians, and selling our valuable cyber skills and products into a booming market throughout the rest of the world***." Canadian Underwriter

Canadians Have Your Say on Cyber Security
The Government of Canada has launched its public consultation to engage with Canadians on the evolving cyber security landscape. This consultation will help identify gaps and opportunities, bring forward new ideas to shape Canada's renewed approach to cyber security and capitalize on the advantages of new technology and the digital economy… ***"The government's cyber security review is an opportunity to build Canadian strength and expertise. Canadians spend more time online than people in any other country. We need to get really good at cyber security - across our personal, business, infrastructure and government sectors - so we can take full advantage of the digital economy, while protecting the safety and security of Canadians, and selling our valuable cyber skills and products into a booming market throughout the rest of the world. I hope Canadians will participate vigorously to help us shape this opportunity."*** **The Honourable Ralph Goodale, Minister of Public Safety and Emergency Preparedness**. Montreal Gazette

How much do we really know about the Canadian intelligence community?
An opinion piece states, "The Trudeau government is set to review the activities of Canada's spy agencies at a time when it appears Bill C-51 has empowered many of the more than 20 agencies and departments with surveilling powers to violate the Canadian Charter of Rights and Freedoms. Last year American whistle-blower Edward Snowden proclaimed that Canadian intelligence agencies have the "weakest oversight" in the Western world and compared the Canadian government's Bill C-51 to George W. Bush's post-9-11 U.S. Patriot Act…There should be an inquiry into the events that led to Driver's death. In essence he was "engaged and killed" for an action he had not yet carried out. Moreover, it appears the young man was under close surveillance by at least two different countries, making it difficult

to imagine that authorities could not see it coming. However, putting aside those important questions for the moment, one thing is clear: the event gave **Minister of Public Safety Ralph Goodale** justification for the continued delay of the Liberals' election promise to reform C-51... Mapping the issue is helpful. Different agencies report to different ministries. The RCMP and CSIS, for example, report to **the Minister of Public Safety**, while The Canadian Security Establishment (CSE) reports to the Minister of National Defence. Broadly speaking, the agencies are divided into civilian and military, but there is a lot of overlap... For example, the Integrated National Security Enforcement Teams (INSET), established in 2002, is made up of special inter-departmental counter-terrorism units that operate under **Public Safety Canada**. It is very unlikely that they have no contact with the Canadian military. Moreover, Canada is a small country and in the course of an individual's professional life they may work for two or more agencies (see the career trajectory of Leonard N. Giles, for example). But back to the question of numbers — or to be more precise, how difficult it is to establish the exact number. A recent article in the Toronto Star mentioned four intelligence agencies listed in a government document with the fourth name blacked out (why would the government black out the name of a security agency?). However, the six security agencies that most people may have heard of include the RCMP, and then, under the umbrella of the Department of National Defense, the CSE, and the lesser known Intelligence Branch. The latter is the main intelligence service of the Canadian Forces, which is concerned primarily with vetting personnel and is associated with The Canadian Forces School of Military Intelligence (CFSMI) in Kingston. There is also the aforementioned CSIS, and finally, the Canadian Border Services Agency (CBSA). One does not normally think of a border agency as an intelligence agency but collecting information is a by-product of their operations. Even more surprising, the list mentioned above also included Citizenship and Immigration Canada. That brings the number up to seven, which already seems like a lot for a country with only 34 million people. The U.S., for example, has 17 different intelligence agencies for a population of 322 million. In addition to the aforementioned agencies, there are at least two groups occupied with psychology which could also arguably be added. The Canadian Forces has a Psychological operations (PSYOPS) unit, and then there is the Extremism and Terrorism section of the Canadian Psychology Association... The RCMP is monitored by the Civilian Review and Complaints Commission (CRCC), while CSIS is tracked by the Security Intelligence Review Committee (SIRC). The CSE has the CSE Commissioner, who supposedly provides some kind of external assessment. Considering the importance of the internet to our lives now, the fact that there is only one man in charge of checking up on the CSE is alarming, to say the least. In contrast, SIRC reports directly to the Government of Canada rather than any one minister. Chaired by various corrupt individuals during the Harper era, it lacks funding and any real authority..." The Independent (Newfoundland & Labrador)

Broadcast media / Médias télédiffusés :

Public Safety Minister Ralph Goodale was interviewed concerning the immigration detainee overhaul and CBSA oversight changes. (CBC Radio, 8:11 ET; CBC Radio One, 8:12ET)

Prime Minister Justin Trudeau mentioned during a press conference today that the federal government will get the balance right in terms of defending our rights and freedoms and protecting Canadian security. He noted that **Public Safety Minister Ralph Goodale** has been making announcements about how the government will keep Canadians safe while defending our values and rights. He also said that the government announced a new committee of parliamentarians who will be tasked with overseeing our national security agencies. (CBC News, 10:00ET)

TOP STORIES / MANCHETTES

ISIL supporter Aaron Driver was killed by police gunfire, not explosive device he detonated, family says

An ISIL supporter who died during a confrontation with an RCMP tactical team outside his home in Strathroy, Ont. was killed by a police bullet, his family said Tuesday. Wayne Driver said an autopsy had determined that his son Aaron had been shot two times and that one of the bullets had struck his liver and traveled to his heart. The other hit his spleen, he said... Following the incident, the RCMP said it was

unsure whether Driver had died as a result of his own bomb or police bullets but the father said the autopsy had put that question to rest. "It was the police officer's bullet that killed him," the father told the National Post. "The bomb that exploded he could have walked away from with minor to severe injuries they said." National Post; CBC News; Canadian Press (London Free Press, Kingston Whig-Standard, CTV News); Radio-Canada

Crime in Canadian cities: 'Perceptions do not necessarily match the reality,' pollster says
The statistics say Saskatoon, Regina and Edmonton have the most severe crime but Canadians believe Winnipeg, Toronto and Montreal are the most dangerous cities, according to a new poll from Mainstreet Research. "The results paint an interesting portrait of how we see each other," Mainstreet president Quito Maggi said in a release. "Perceptions do not necessarily match the reality of crime and safety." Ottawa was perceived as the safest city of 15 included in the poll, followed by Charlottetown and Moncton. According to Statistics Canada, however, the cities with the least severe crime last year were Quebec City, Toronto and Ottawa, respectively. Canada's biggest city had the biggest perception-reality gap - despite having the second-lowest crime severity index, Toronto was perceived as the second most dangerous city, behind only Winnipeg. And Manitoba's capital, despite its unsafe reputation, had less severe crime than Vancouver, Edmonton, Regina and Saskatoon. CBC News

Cybersécurité: les chefs de police réclament l'accès légal aux mots de passe
Les chefs de police canadiens réclament une loi pour contraindre les gens à révéler leurs mots de passe aux forces de l'ordre avec l'approbation d'un juge. L'Association canadienne des chefs de police (ACCP) a adopté une résolution incitant le gouvernement à prendre des mesures législatives pour faciliter l'obtention de preuves électroniques. L'ACCP estime que les criminels ont de plus en plus recours au chiffrement pour dissimuler leurs activités illicites en ligne. Le commissaire adjoint de la Gendarmerie royale du Canada (GRC), Joe Oliver, a déclaré qu'aucune loi canadienne ne contraignait actuellement le détenteur d'un mot de passe à le révéler aux policiers dans le cadre d'une enquête. Lors d'une conférence de presse mardi, M. Oliver a soutenu que les criminels, qu'ils soient membres de la mafia ou pédophiles, bénéficiaient d'un anonymat quasi absolu en ligne. Cette résolution de l'ACCP survient alors que le gouvernement fédéral entame ses consultations en matière de cybersécurité, notamment par rapport à l'équilibre entre les besoins des policiers et les libertés fondamentales. Ces consultations se poursuivront jusqu'au 15 octobre. Presse canadienne (L'Actualité) ; Canadian Press (CTV News, News 1130, iPolitics); CHED 630 AM

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Severe summer storm in the Prairies causes more than $48 million in insured damage
Insurance Bureau of Canada (IBC) reports a severe storm that swept through Alberta, Saskatchewan and Manitoba during the second week of July has resulted in more than $48 million in insured damage according to Catastrophe Indices and Quantification Inc. (CatIQ). From July 8 - 11, a low pressure system caused severe thunderstorms in the Prairies. The storms produced strong winds, hail, lightning, heavy rainfall, and funnel clouds. This system also caused significant flooding in Estevan, SK and produced a brief tornado touchdown in Humboldt, SK on July 10. Insurance Bureau of Canada News Release (Montreal Gazette)

B.C. Hydro concerned earthquakes from fracking could damage Peace River dams
Internal documents show B.C. Hydro officials have had concerns since at least 2009 that earthquakes triggered by fracking are a potential risk to its Peace River dams. The electricity-generating dams in northeastern B.C. include one of the largest earth dams in the world, the W.A.C. Bennett Dam, as well as the smaller Peace Canyon Dam, and the $9-billion Site-C dam, which is under construction. The Crown agency has not discussed the issue publicly. But as a result of its concerns, B.C. Hydro worked out an agreement, possibly as early as 2014 with the B.C. Oil and Gas Commission (BCOGC), to create five-kilometre buffer zones around dams where no new fracking and drilling rights are issued, according to a report released today from the Canadian Centre for Policy Alternatives, a left-wing think-tank. Financial Post

Wildfires north of Kamloops caused by lightning, people
Lightning in the Kamloops region over the past few days has led to a number of new wildfire starts, but at least one blaze north of the city is believed to have been caused by people. The BC Wildfire Service is fighting two fires east of Barriere, one at the north end of East Barriere Lake, and the other near Momich Lakes Provincial Park. Both are about one hectare in size, and both are classified as lightning-caused. A very small fire has been noted in the O'Connor Lake Road area north of Kamloops, also caused by lightning. CFJC Today

ATV found, but search continues for overdue Kugluktuk hunter
A search is underway for a hunter reported overdue in Kugluktuk, Nunavut. RCMP say Allen Kudlak Jr. left the community on Thursday Aug. 11, travelling on his ATV with a rifle, but no other supplies or equipment. Kudlak was reported missing to the RCMP the following day when he failed to return home. Local search and rescue started searching for Kudlak on Saturday when his ATV was found in Kugluk territorial park, about 10 kilometres southwest of the community. CBC News

Volunteer marine unit in Grimsby suffers serious setback
Members of the Grimsby Auxiliary Marine Rescue Unit hoping to get a short term loan of a rescue boat after their 22 foot Zodiac suffered what they call a catastrophic failure Saturday. The Zodiac experienced a massive breach of its fibreglass hull while towing a disabled boat during a rescue mission on Lake Ontario. The Zodiac, or GAMRU 334, is one of only two vessels available to the group during boating season and allows the unit to respond quickly in shallow water. nit leader Bob Gordon calls it a significant setback to the only dedicated marine search and rescue organization on the south shore of Lake Ontario that services an area from Hamilton to Port Weller. CKTB News Talk 610

NATIONAL SECURITY / SÉCURITÉ NATIONALE

ISIL supporter Aaron Driver was killed by police gunfire, not explosive device he detonated, family says
An ISIL supporter who died during a confrontation with an RCMP tactical team outside his home in Strathroy, Ont. was killed by a police bullet, his family said Tuesday. Wayne Driver said an autopsy had determined that his son Aaron had been shot two times and that one of the bullets had struck his liver and traveled to his heart. The other hit his spleen, he said... Following the incident, the RCMP said it was unsure whether Driver had died as a result of his own bomb or police bullets but the father said the autopsy had put that question to rest. “It was the police officer’s bullet that killed him,” the father told the National Post. “The bomb that exploded he could have walked away from with minor to severe injuries they said.” National Post; CBC News; Canadian Press (London Free Press, Kingston Whig-Standard, CTV News); Radio-Canada

Quebec funding program for at-risk youth in St-Léonard
The province will be funding a prevention program to help keep at-risk youth out of trouble, officials announced Monday. Quebec Public Security Minister Martin Coiteux said the government will invest $625,000 over five years into thwarting youth delinquency in the northern Montreal borough of St-Léonard. The project brings together the municipal group Prévention Jeunesse - which addresses issues of radicalization in Montreal - and the YMCA Quebec to run programs aimed at preventing youth involvement in street gangs and radicalization. "(This initiative) will allow us to act locally and in a succinct manner in order to prevent and intervene directly within a population of youth who are vulnerable to violence, delinquency and radicalization," said Anie Samson, the city's executive committee member responsible for public security. Montreal Gazette

Countering extremism
A letter to the editor states, “Re: Young terror supporter had troubled upbringing (Aug. 30). I am absolutely shocked that the RCMP identified a homegrown extremist originally from Winnipeg who was planning to attack a public area in Canada. It is quite scary, in fact, to see the power of social media and how it is being manipulated to serve the interests of ideological extremist recruiters. Aaron Driver, a 24-year-old living in a town in Ontario, had shown support for ISIS in the past and was thus being monitored.

I am thankful this situation did not escalate to an attack and was mitigated immediately. Although there may be many solutions to homegrown extremism, the most effective one is having a true and powerful counter-narrative. One example of such a narrative is the Ahmadiyya Muslim Youth Association, which is known for giving back to society through blood drives, food drives, city cleanups and much more. These counter-narratives will help put an end to homegrown extremism and continue to make Canada great…" Winnipeg Free Press

Broadcast media / Médias télédiffusés :

The Ontario provincial police released a statement today saying a gunshot wound killed ISIS supporter Aaron Driver. Driver was killed in the southwestern Ontario city of Strathroy on August 10. It was the result of an RCMP investigation into a national security threat. (CBC News, 10:00ET, 12:00ET; CTV 12:30ET)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CBSA Proposes Amendments to NEXUS and Other Trusted Traveler Programs
The Canada Border Services Agency ("CBSA") recently announced that it was proposing changes to its Trusted Traveller Programs ("TTPs"), which include CANPASS, Free and Secure Trade ("FAST"), and NEXUS. In furtherance of this proposal, CBSA intends to amend the Presentation of Persons (2003) Regulations (the "POP Regulations"), which were implemented under the Canadian Customs Act. A summary of these proposed amendments appears below. Lexology

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Cybersécurité: les chefs de police réclament l'accès légal aux mots de passe
Les chefs de police canadiens réclament une loi pour contraindre les gens à révéler leurs mots de passe aux forces de l'ordre avec l'approbation d'un juge. L'Association canadienne des chefs de police (ACCP) a adopté une résolution incitant le gouvernement à prendre des mesures législatives pour faciliter l'obtention de preuves électroniques. L'ACCP estime que les criminels ont de plus en plus recours au chiffrement pour dissimuler leurs activités illicites en ligne. Le commissaire adjoint de la Gendarmerie royale du Canada (GRC), Joe Oliver, a déclaré qu'aucune loi canadienne ne contraignait actuellement le détenteur d'un mot de passe à le révéler aux policiers dans le cadre d'une enquête. Lors d'une conférence de presse mardi, M. Oliver a soutenu que les criminels, qu'ils soient membres de la mafia ou pédophiles, bénéficiaient d'un anonymat quasi absolu en ligne. Cette résolution de l'ACCP survient alors que le gouvernement fédéral entame ses consultations en matière de cybersécurité, notamment par rapport à l'équilibre entre les besoins des policiers et les libertés fondamentales. Ces consultations se poursuivront jusqu'au 15 octobre. Presse canadienne (L'Actualité) ; Canadian Press (CTV News, News 1130, iPolitics); CHED 630 AM

Largest ransomware-as-service scheme pulls in US$195,000 a month: Report
Canadians are among those who have fallen victim to a global ransomware-as-a-service scheme which targeted tens of thousands of users in 201 countries and territories in July alone, according to security researchers. The researchers at Check Point Software and IntSights Cyber Intelligence of Israel released a report Tuesday saying the service, which it calls Cerber, is currently running 161 active campaigns with a total estimated profit of US$195,000 last month alone. In July an estimated 150,000 devices were infected. Each day an average of eight new campaigns on average are launched, Check Point says. The biggest percentage of victims so far are in South Korea (29 per cent), the U.S. (14 per cent), Taiwan (9 per cent) and China (eight per cent). However, Check Point says there's evidence to support the developer's claim that Americans are among the top people willing to pay up. IT World Canada

LAW ENFORCEMENT / APPLICATION DE LA LOI

$19K found inside Hamilton man's car on Trans-Canada Highway
A man from Hamilton, Ont., faces criminal charges after RCMP in Manitoba pulled a car over for speeding, only to find "stacks of cash" exceeding $19,000 in cash along with some marijuana inside. RCMP say they stopped a 2007 Cadillac on the Trans-Canada Highway near Headingley, which is just west of Winnipeg, around 1 p.m. CT on Aug. 11. Officers found a small quantity of marijuana and "stacks of cash in excess of $19,000" inside the vehicle, RCMP said in a news release Tuesday. Both the money and the car were seized. Police say they believe the cash was obtained through criminal activity. An RCMP spokesperson says the vehicle is being held as part of the investigation, which will determine whether or not it came from proceeds of crime. CBC News; Global News; Winnipeg Free Press; Radio-Canada

La GRC se penche sur la vente de blindés canadiens en Libye
Le gouvernement libéral est préoccupé par un rapport des Nations unies (ONU) qui déplore qu'une compagnie canadienne ait livré plusieurs dizaines blindés en Libye, alors qu'un embargo commercial interdit la vente d'armements à ce pays déchiré par la guerre. Le ministère des Affaires mondiales a ainsi demandé à la Gendarmerie royale du Canada (GRC) de se pencher sur le document produit par le comité de l'ONU chargé de faire le suivi des sanctions imposées à la Libye. On ignore toutefois pour l'instant si la GRC va lancer une enquête en bonne et due forme sur les agissements du constructeur de véhicules blindés Streit Group. Le gouvernement libéral a dit vouloir laisser l'affaire entre les mains de la police. « Il appartient à la GRC d'enquêter sur d'éventuelles violations à la loi canadienne, et c'est le Service des poursuites pénales du Canada qui doit déterminer, en s'appuyant sur les éléments disponibles, si le Canada a la juridiction pour poursuivre les contrevenants », a indiqué François Lasalle, porte-parole du ministère des Affaires mondiales dans un communiqué. Le ministère n'a pas précisé quand le rapport produit en mars dernier avait été transmis à la police fédérale. La nouvelle intervient moins d'une semaine après que la CBC eut diffusé série de reportages sur les activités de Streit en Libye, mais aussi au Soudan du Sud. Rencontre avec Streit Le comité des Nations unies a reproché à l'entreprise canadienne, qui a une usine à Innisfil, en Ontario, le « transfert illicite » de 131 véhicules de transport de troupes (VTT) en 2012. Des représentants de Streit ont rencontré les enquêteurs de l'ONU en 2014 et leur ont remis plusieurs documents portant sur la livraison de blindés de modèles Cougar, Spartan et Cobra à la Libye en 2012, de même que des déclarations de douanes. Radio-Canada

Broadcast media / Médias télédiffusés :

Global Affairs Canada gave a copy of a UN report on the Streit Group sale of armored vehicles into Libya in 2012 over to the RCMP for review. (CBC News, 12:00ET, 11:00ET, 10:00ET, 8:00ET)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Mission mayor wants answers from Corrections Canada about sex offender
The mayor of Mission is demanding answers and he's hoping to get them as he meets with Corrections Canada to talk about a high-risk sex offender who has been living in his community for two weeks now. Mayor Randy Hawes says he wasn't told the truth about James Conway's relocation from Abbotsford. "I keep being told by Corrections that they had no choice, that it was completely the decision of Conway, The William James Society and the courts. Well, now I am finding out that there were quite a number of other options put forward and Corrections rejected them all," Hawes tells NEWS 1130. "I feel like we haven't been told the truth and I'm not very happy about that." Conway, a convicted pedophile with a long criminal history, has been the target of protests since moving to Mission. (…)He was convicted of sex crimes against children three times and is considered at high risk to re-offend. BC Corrections says he is under 24-hour surveillance and he can't leave his home unsupervised. News 1130

"Balaclava Rapist" to live in Vancouver while serving day parole
Vancouver Police have confirmed to Global News that the man known as the "Balaclava Rapist" will be serving his day parole at a correction halfway house in that city. The 63-year old was serving three life sentences, having admitted to raping at least 30 women in Edmonton in the 1970's and 80's. In 1984, Takahashi was convicted of 14 charges, including four counts of rape, sexual assault with a weapon, aggravated sexual assault and six counts of disguise with intent. CKNW

Indigenous relationships to be focus for justice system changes
Canada's federal Minister of Justice and Attorney General Jody Wilson-Raybould told a crowd of hundreds of lawyers that the federal government is committed to improving relationships with indigenous people, as well as promoting diversity on the bench. "Many of the issues we face as a country have a justice element to them, and which is why our government has embarked on a very ambitious agenda, and an effort to reform our justice system," Wilson-Raybould said to lawyers from across Canada gathered in Ottawa last week for the Canadian Bar Association's annual conference. Wilson-Raybould was the conference's keynote speaker Friday morning. (…)"It is a sad reality that many members of indigenous communities are among the most marginalized segments of our population, and that they are over-represented both as offenders and victims in the justice system," said Wilson-Raybould. (…)Wilson-Raybould pointed to a report from the federal Office of the Correctional Investigator that illustrated the gap. From 2005 to 2015, she said, the indigenous inmate population increased by 50 per cent, compared with the overall growth rate of 10 per cent. She also noted that while indigenous people make up 4.3 per cent of the population, they represent more than 25 per cent of inmates. She also said that indigenous women comprise 37 per cent of all female inmates serving a sentence of more than two years. "This is totally unacceptable," she said. Canadian Lawyer Magazine (2016-08-15)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Crime in Canadian cities: 'Perceptions do not necessarily match the reality,' pollster says
The statistics say Saskatoon, Regina and Edmonton have the most severe crime but Canadians believe Winnipeg, Toronto and Montreal are the most dangerous cities, according to a new poll from Mainstreet Research. "The results paint an interesting portrait of how we see each other," Mainstreet president Quito Maggi said in a release. "Perceptions do not necessarily match the reality of crime and safety." Ottawa was perceived as the safest city of 15 included in the poll, followed by Charlottetown and Moncton. According to Statistics Canada, however, the cities with the least severe crime last year were Quebec City, Toronto and Ottawa, respectively. Canada's biggest city had the biggest perception-reality gap - despite having the second-lowest crime severity index, Toronto was perceived as the second most dangerous city, behind only Winnipeg. And Manitoba's capital, despite its unsafe reputation, had less severe crime than Vancouver, Edmonton, Regina and Saskatoon. CBC News

His family called 911 for help with a seizure but this man claims police beat him instead
The family of a man with epilepsy says police beat him severely in his home then arrested him after they had called 911 for help with violent symptoms from a seizure. And his was the second case like it in Edmonton within a week. Neil Ryley, 49, has epilepsy, a brain disorder characterized by recurring seizures. At the end of June, his ex-wife Tracey Schimpf suspected he was having a medical episode when he started acting erratically. "He was upset. Freaking out," she said. Ryley has seizures often, but it's only about three times a year that he displays defensiveness, violence or anger, Schimpf said. Symptoms such as hallucinations, confusion and violence can occur during and after certain types of epileptic seizures, according to the Edmonton Epilepsy Association. Schimpf said she called 911 for an ambulance three times. She also recommended the paramedic crew bring police officers with them. In the past, officers had helped the paramedic team restrain Ryley and bring him to the stretcher when he had aggressive episodes during or after seizures. (…)Edmonton police spokesperson Cheryl Sheppard said Ryley head-butted one of the officers, breaking his nose, and bit another. Police offered no comment on Schimpf's claim that it took 90 minutes for police to arrive after she first called 911. The officers charged Ryley with assaulting a peace officer. They took him to hospital, arrested him, then put him in jail for eight days. His lawyer got him out on bail after producing a letter that verified his medical condition. CBC has

also confirmed a second man with epilepsy was arrested and charged with assaulting a peace officer six days earlier, while displaying symptoms linked with epileptic seizures. CBC News

Canadians see Winnipeg as most dangerous city in country, poll says
Winnipeg is seen as the most dangerous city in Canada, a poll released Tuesday suggests. The Mainstreet/Postmedia poll of 4,213 Canadians ranks Ottawa as the safest among 15 major cities while Winnipeg sits dead last. The survey is based on the perceived safety of cities, not the actual data, said Quito Maggi, president of Mainstreet Research, who noted that numbers recently released by Statistics Canada show Saskatoon actually has the highest crime rate in the country. In the Mainstreet poll, that city ranks 12th out of 15 cities for safety. "Perceptions compared to Statistics Canada's Crime Severity Index yields some interesting comparisons," Maggi said. Toronto, for example, ranks 14th out of 15 in terms of perceived safety in the Mainstreet poll. But when it comes to actual crime statistics, it is one of the safest cities. It has the second best crime severity index, behind only Quebec City and ahead of Ottawa, which Canadians perceive to be the safest. And Winnipeg's actual crime severity index is better than Vancouver, Edmonton, Regina and Saskatoon in terms of safety. CBC News; Winnipeg Free Press; Winnipeg Sun; iNews 880; Radio-Canada

Not just perception: Winnipeg is a violent city
There's a reason Winnipeg is perceived as the most unsafe city in Canada — because it is. A new Mainstreet Research Poll has found that Winnipeg is perceived by Canadians as the most dangerous city in the country. And while general crime rate data does show crime in Winnipeg is less severe than in cities like Vancouver, Saskatoon and Edmonton, it's the amount of violent offences — and the severity of those offences — that shows people's perceptions of Winnipeg as the most unsafe city in the country are well founded. According to Statistics Canada's violent crime severity index, Winnipeg had the most violent crime of any city in Canada in 2015 with a value of 122.1. Thunder Bay had the second highest violent CSI at 119.2 and Saskatoon ranked third at 113.5. Winnipeg's violent crime index actually rose 5% last year, according to StatsCan. So it's not just people's perceptions that Winnipeg is a violent city. The stats back up how people see this city. Winnipeg Sun

Canadians perceive Calgary as Canada's sixth least safe city, poll finds
Canadians perceive Calgary to be one of the country's less safe cities, ranking it 10th out of 15 major centres in a new poll. The poll comes after last month's release of Statistics Canada crime stats, which showed a 29 per cent increase in the severity of crime in Calgary. Based on StatsCan's Crime Severity Index, Calgary ranks ninth among the 15 cities covered by the poll (it ranks seventh for overall crime rate, regardless of severity). Winnipeg was seen as Canada's least safe city by poll respondents, followed by Toronto and Montreal. But Quito Maggi, Mainstreet's president of research noted that perceptions were considerably different from the statistics. Calgary Herald

Disconnect between perceptions and crime data: poll
It seems there is a difference between how dangerous you think Metro Vancouver is and what the statistics actually show. A new national poll suggests there's a disconnect between our perceptions and what the data proves. Vancouver ranked ninth in the poll among 15 major cities, while Victoria was just one spot better according to the research from Mainstreet. But pollster David Valentin says the crime rate trends according to Statistics Canada don't quite back that up. "It's interesting that Victoria actually saw its crime rate go up last year by 10 per cent. It's interesting that even though the crime is increasing in Victoria, people do rank it as safer than Vancouver." Saskatoon has been deemed the most dangerous city in this research. News 1130

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Reasonable Doubt: the history of marijuana law in Canada
The 1908 Opium Act was the first Canadian law that prohibited drugs, and it was at least a partially racist response to Chinese immigrants associated with opium use at the time. It was a tough economic time, and resentment was growing toward Chinese and other immigrants working for low wages. After race riots in 1907, Mackenzie King, the deputy minister of labour at the time, visited opium dens in Vancouver and became concerned with apparent increased opium use, particularly by white people and women. That visit is said to have been a catalyst for the Opium Act. In 1923, the government added marijuana to the schedule of prohibited drugs in the Opium and Narcotic Control Act. Some people point to The Black Candle, a (very racist) book by so-called and famed feminist Emily Murphy, who linked drug use to specific risks to white women. It is hard to know with any certainty how much of an influence this book had on drug legislation, but it certainly contributed to the reactionary, often racist, anti-drug sentiment of the time. To be fair, there were also international discussions occurring at the time over the evils of drugs and virtues of prohibition. (...)In 1972, the Le Dain Commission published a report on the non-medicinal use of drugs and recommended decriminalizing cultivation and possession of marijuana for person use. Instead, what followed was nearly thirty years of prohibition. (...)In 2012, the Harper government introduced mandatory minimum prison sentences for possessing set amounts of marijuana or plants. Over the next three years, several courts deemed several of these mandatory minimum laws unconstitutional. (...)Next year, the Liberals are set to introduce laws legalizing and regulating marijuana use. The plan will likely earn the government millions in tax revenue and save the considerable cost of prosecuting and jailing people for marijuana offences. NOW Toronto

PUBLIC SERVICE / FONCTION PUBLIQUE

Canada.ca web renewal costs soaring with more expenses coming
Expenses related to the federal government's web renewal project are already skyrocketing and the initiative is only in its second official year. The push to gather a vast majority of the government's departments and agencies under the Canada.ca web address - as opposed to the various disparate websites they previously had - has already cost the federal government at least $9.2 million, of which $5.4 million has been paid. The contract, which was awarded to Adobe Corp. in March 2015, was originally valued at $1.54 million... Debi Daviau, president of the Professional Institute of the Public Service of Canada, the union representing more than 57,000 professional staff across the country, said government has only begun to see the true expenses associated with outsourcing a massive initiative like the switchover to Canada.ca. Ottawa Citizen

OTHER / AUTRES

Special forces soldier from Petawawa charged with sexual assault
A soldier who served with Canadian special forces in Petawawa has been charged with sexual assault. The Canadian Forces National Investigation Service laid charges under the National Defence Act against Cpl. Simon Cadieux. The charges relate to an alleged sexual assault that took place while Cadieux, then a member of the Canadian Special Operations Regiment, was on an exercise in Jamaica in November 2015. The alleged victim is also a member of the Canadian Forces, the military has confirmed... For the last several years, members of the Canadian Special Operations Regiment have been training Jamaican forces in counter-terrorism techniques. Ottawa Citizen

INTERNATIONAL

Bosnian authorities arrest alleged IS recruiter
Bosnian authorities say they have arrested a man suspected of recruiting members for the Islamic State group. The prosecution office said Nedzad Mujic is also believed to have fought for the group in

Syria. Mujic was arrested near the northeastern town of Zvornik and is under investigation for financing terrorist activities and organizing terrorist groups. Intelligence agencies say the number of people leaving Bosnia to fight in Syria or Iraq has dropped significantly since it introduced jail terms two years ago for those who fight in foreign wars. Of the 130 Bosnian citizens who had previously left, nearly 50 reportedly died in battles. Associated Press (Metro News)

IS attack kills nine Iraqis near Jordan border
Fighters of the Islamic State group attacked an Iraqi border guard base near Jordan on Tuesday, killing at least nine people before being beaten back, officers said. The early morning attack involved heavy mortar fire and saw clashes between jihadists and border guards defending their position near Rutba, the last town on the desert road before the Trebil border crossing. Agence France-Presse

Persecution of Christians in Middle East is profoundly un-Islamic
An opinion piece states, ""Are you Muslim?" asks a Daesh member to a Christian couple. When the husband answers in the affirmative, the terrorist instructs him to recite from the Quran. The man recites from the Bible. Upon hearing the Arabic, the guard says "Yallah" and motions them through. The man's wife later says: "I can't believe the risk you just took. Why did you lie? If he knew, he would have killed us." The punchline: "Don't worry! If they knew the Quran they would not indiscriminately kill people," answered the husband. A Leger poll commissioned by the Knights of Columbus released earlier this month revealed that a majority of Canadians (51 per cent) believed that Christians and other minorities face genocide in large parts of the Middle East…" Toronto Star

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

RalphGoodale
Today GofC launched a public consultation to engage with Canadians on #cybersecurity. Have your voice heard news.gc.ca/web/article-en…

RalphGoodale
Gouv du Can lance une consultation publique pour engager Canadiens sur cybersécurité. Faites valoir votre opinion! bit.ly/2bkJZT8

Amnesty Canada
Tell @RalphGoodale that Canada needs to stop detaining refugee and migrant children ACT NOW>>http://amn.st/6018B2rh4

NAACJ
Yes @RalphGoodale: "ensure that #detention is truly a #LastResort." It *isn't* the only game in town! http://bit.ly/2aQXtX9 #CJR @Puglaas

Tonda MacCharles
Goodale's overhaul of immigration detention system, new prisons, criticized for going in wrong direction.

metromorning
After a hunger strike by detainees, the gov't announces a change to how it treats immigration detainees. Ralph Goodale is here at 8:10.

RenuMandhane
I realize it's not perfect (no end to indefinite imm detention) but @RalphGoodale showing bold leadership on a file with few political wins.

AM980News
Ralph Goodale outlines intention to combat radicalization across Canada. am980.ca/2016/08/16/pub…

HuffPostCanada
Canada must become a leader in countering radicalization: Goodale #cdnpoli huff.to/2biXynb

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Sécurité publique
#SARscène2016 se tiendra du 15 au 17 oct. à #Edmonton. Pour détails et inscriptions, consultez http://ow.ly/e4vs303i3MV #RechercheSauvetage

Public Safety Canada
#SARscene2016 is from October 15-17 in #Edmonton. For details and to register visit http://ow.ly/ardY303i3p3 #searchandrescue #SAR

Global Saskatoon
@InsuranceBureau says severe storms that swept across the Prairies in July caused more than $48M in insured damage:

IAEMCdnCouncil
Do earthquake swarms signal that "The Big One" is coming?

IBC
Proud to wear our new #ymmstrong bracelets. Thanks @RMWoodBuffalo for creating and sending these over.

IBC
Severe summer storm in the Prairies causes more than $48 million in insured damage http://www.ibc.ca/ via @IBC_West

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Phil Gurski
Some idiot is posting fake terrorist attacks in Ottawa on Facebook

CTV News
Aaron Driver died from gunshot wound: RCMP

Desmond Cole
This Toronto woman lost her job at the airport, partly because of #carding. She deserves to be working again.

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

John Howard Society
Ottawa to overhaul immigration detention system

Nicholas Keung
Immigration detention reforms fall short on oversight, critics say http://on.thestar.com/2b9xYiM @TorontoStar

Cdn Council Refugees
"#Immigration detention reforms fall short on oversight, critics say" @TorontoStar - http://on.thestar.com/2bkjheH #cdnimm

Cdn Council Refugees
CCR Resources: #Immigration detention statistics 2015 http://bit.ly/2bkk5zT #Canada #cdnpoli #cdnimm

Cdn Council Refugees
"Photo Essay: Ontario's migrant workers tell their stories" - @TorontoLife http://bit.ly/2bkFrgN

No One Is Illegal
Dans Le Devoir aujourd'hui: La détentions des immigrants remise en question. « J'avais un bon réseau de soutien...

CYBER SECURITY / CYBERSÉCURITÉ

cforcese
Looks like @Safety_Canada has kicked off a public consult on cyber security, http://www.publicsafety.gc.ca/cnt/cnslttns/cbr-scrt/cbr-scrt-en.pdf …

GC Newsroom
Gov't of Canada launches a #cybersecurity public consultation. Have #YourCyberSay http://ow.ly/9L6s100hjON

Sécurité publique
Nous tenons consultation publique sur #cybersécurité. Donnez votre #OpinionCyberSécurité! http://ow.ly/GVXc303hKsv

Public Safety Canada
We've just launched a public consultation on #cybersecurity. Have #YourCyberSay! http://ow.ly/K7Rs303hK4w

SCRS Canada
Voulez-vous voir du pays? Le SCRS a des bureaux partout au Canada et à l'étranger @carriereauscrs

Michael Kaiser
On 9/7 the @FTC will host experts to look at the growing threat of #ransomware https://www.ftc.gov/ #cybersecurity #CyberAware

LAW ENFORCEMENT / APPLICATION DE LA LOI

Connie Walker
Sask. RCMP investigate suspicious death of 20-year-old woman

Global Winnipeg
RCMP seize drugs,19K in cash after traffic stop near Winnipeg

Nunatsiaq News
RCMP student Emma Inookee directs #Iqaluit kids through safety training rodeo Aug. 16 PHOTO/@thomas_rohner

Hache Arlene
Emma Inookee, 19, plans a career with the Nunavut RCMP

Surrey RCMP
Receive the latest policing info from the Surrey RCMP by e-mail. Sign up for ENews: http://ow.ly/Uvs6303g6oj

CACP/ACCP
This year's theme at #CACP2016 is Public Safety in a Digital Age: Real Victims - Real Crime.

CACP / ACCP
@TheIACP President, Chief Cunningham joined by @rcmpgrcpolice Asst Commr Joe Oliver - "Going Dark" #CACP2016

CACP/ACCP
Media Release: Directeur Mario Harel Becomes New CACP President - discusses key issues moving forward #CACP2016 https://cacp.ca/

The OACP
OACP 1st Nations Director @NAPS_Police Chief Armstrong: chronic underfunding of FN services #Unacceptable #CACP2016

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

OFOVC BOFVAC
Here are first steps for adults to stop bullying and harassment for youth aged 12 to 17 @Safety_Canada http://bit.ly/1oj5Mv0

NSPS (CBoC)
Has crime been decreasing or has it just been moving online? We need good #cybercrime statistics to understand the trends #CACP2016 #lesm

NSPS (CBoC)
Some interesting #statistics from @Telus on electronic bullying #CACP2016 #teluswise #cyber #lesm

INTERNATIONAL

Amarnath Amarasingam
The secret meeting that led to the creation of ISIS. Very interesting by @HaraldDoornbos and @jenanmoussa. #ISIS #IS

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

Today's News / Actualités
August 19, 2016 / le 19 août 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Peterborough plane crash: Should there be more security at private airports?
Security concerns are being raised at some of Canada's smaller, private airports after a 20-year-old man with mental health issues stole a plane from a small airport in Markham before crashing it in Peterborough last week. On Thursday, Global News revealed the RCMP was investigating the crash as a "national security issue" and had met with the father of suspect Mohammad Hassan Chaudhary multiple times to discuss his son's involvement... Chaudhary's father Afzal Chaudhary told Global News he was outraged his son, who lived with schizophrenia and other mental health issues, was able to break into the airport, steal a small aircraft and crash into the streets of an Ontario city without any intervention from

police or security officials. "This is a national story. They're spending billions and billions of dollars on the airports. He opened the airport here. Not a fence, not any gate, [nor] any guard, and he left an airplane over there," he said..."These more regional, perhaps almost part-time airports where there is not a lot of activity, it's not fully under CATSA's mandate for standards of protection. The security gets quite a lot lower and certainly in some cases can lead to concerning incidents like this one." According to its website, CATSA is responsible for security screening of people and baggage at 89 designated airports in Canada. Mathieu Larocque, a spokesperson for CATSA, said the agency is not responsible for perimeter security at airports. "The airports where we are present we are not responsible for the security of the airport," said Larocque. "The security of the airport itself, like the airport perimeter, access to the tarmac, security guards at the airport, that is local responsibility handled individual airport authorities."... In a statement to Global News, Transport Canada said said any "operator of an aerodrome must have, at all times, at least one security official or acting security official" under Canadian Aviation Security Regulations. "Canada has a risk-based approach to aviation security, and within this framework, Transport Canada works in partnership with airport associations and regional airport councils to maintain and improve the safety and security of civil aviation at aerodromes in Canada," said a spokesperson for Transport Canada in an email. **Public Safety Minister Ralph Goodale** told Global News there is currently an investigation into the Peterborough crash and wasn't able to comment specifically on private airport security measures. ***"[Transportation Minister Marc Garneau] pays very close attention to these things,"*** **he said.** ***"The safety regime is designed to protect Canadians. Accidents happen, and we'll have to determine what was the nature of this particular incident. Canada overall has a very safe and secure and strong air safety regime and Minister Garneau is determined to keep it that way."*** Patrick Gillian, vice president of operations with the Canadian owners and pilots association, said the theft of planes is so rare most private airports and aerodromes (small general aviation airfields) don't need additional private security. Global News

Fighting terrorism requires outreach as well as policing
An editorial states, "Police were both skilled and lucky when they narrowly stopped Aaron Driver from inflicting major damage last week in the name of a radical jihadist ideology. We can applaud their quick work in derailing Driver's violent plan, but we should not be relying on luck to stop such threats. **Public Safety Minister Ralph Goodale** was right this week when he acknowledged that the peace bond imposed on Driver was not enough to deter him. Despite a court order requiring him to stay away from jihadist propaganda on the Internet, not touch any weapons, and check in regularly with police, the young man came close to setting off an explosion in a crowded public space before he was killed by police..." Toronto Star

The unflappable Ralph Goodale - Trudeau's point man on terrorism is also the minister in charge of not freaking people out
An opinion piece states, "Every government has to have a steady hand on the wheel. In the current Liberal government, it's Ralph Goodale, minister of Public Safety. In a speech to the Canadian Association of Chiefs of Police the other day, Goodale took his audience through the hot files that have landed on his desk since the Liberals took office last fall: re-settling 25,000 Syrian refugees in Canada; the Black Friday terror attack in Paris last November and the attack in Nice on Bastille Day; wildfires in northern Alberta and the evacuation of 90,000 people from Fort McMurray — the biggest Canadian natural disaster of modern times. Just last week, of course, there was the coordinated police takedown of Aaron Driver, a 24-year old ISIS sympathizer with an improvised explosive on his person. The device went off in a cab near London, Ontario; Driver evidently was on his way to a mall there, having made a video promising to shed Canadian blood for the terrorist cause. To every one of these situations, Goodale has brought his characteristic phlegmatic demeanour: Keep calm and carry on. In the case of Driver, police were acting on information posted to social media by the ISIS acolyte and picked up by the FBI. Asked about cooperation between the RCMP and FBI, Goodale replied that it happens all the time — the Americans share information with us, we share it with them. Next question.Driver had frequently broken the terms of his court-ordered peace bond, which barred him from weapons and proselytizing for ISIS on social media. Goodale mused that the government may look at revising the law to compel terror suspects under peace bonds "to engage with counter-radicalization professionals." In any event, Goodale said, the Driver incident demonstrated the need to "up our game" in deprogramming potential homegrown terrorists. He repeated the Trudeau government's promise to hire a deradicalization adviser with an

annual budget of $10 million and a mandate to work with cities on their own deradicalizing efforts..." iPolitics

MP Kerry Diotte fires at Ralph Goodale over 10/22 magazine controversy
Another Member of Parliament has spoken out against the reinterpretation of legality surrounding the Ruger 10/22 magazines A user, who wishes to remain anonymous, took to a Canadian firearms forum board to share the letter he received from his Member of Parliament, Conservative Kerry Diotte representing Edmonton Greisbach, on the issue of the 10/22 magazine controversy. According to Diotte, he has received many correspondences from his constituents on the matter, prompting him to urge the **Minister of Public Safety and Emergency Preparedness, Hon. Ralph Goodale**, to reverse this bureaucratic decision that was without any proof of enhanced public safety. Dear [redacted]: Thanks for your correspondence regarding the classification of the 10/ 22 Ruger Magazine. I hear you. It is unfair that with just a stroke of a pen, law – abiding firearm owners can be criminalized for owning property that they purchased legally. The RCMP Canadian Firearms Program's decision to prohibit the 10/ 22 Ruger Magazine does just that, while doing nothing to promote public safety. Prime Minister Justin Trudeau and his cabinet have the authority to undo this classification... On behalf of the many constituents I've heard from on this classification decision, I've written the attached letter to the **Hon.Ralph Goodale, Minister of Public Safety and Emergency Preparedness**. I encourage you to also make your views known to the **Hon.Ralph Goodale.** As your Member of Parliament, I'm proud to stand up for common sense firearm regulations that prioritize public safety without penalizing law- abiding hunters, farmers and sport shooters. Sincerely, Kerry Diotte... They also included Diotte's letter to **Hon. Ralph Goodale**, which echos almost entirely the same sentiment held by MP Bob Zimmer in his letter to the Minister last month. Dear **Minister Goodale:** The RCMP Canadian Firearms Program's decision to prohibit the 10/22 Ruger Magazine is unfair to law-abiding firearms owners. I've heard from many of my constituents, who have expressed sincere disapproval of this bureaucratic decision... I urge **you** to reverse the classification of the 10/22 Ruger Magazine or introduce an amnesty for those who purchased this magazine legally, Sincerely, Kerry Diotte... While we need to continue fighting this battle, it's clear that writing to your Member of Parliament is not a useless tactic. The more MPs we have writing to the Minister on this matter, the more likely it is we will be able to overcome this obstacle and once again be able to use magazines with capacities greater than 10 rounds in our 10/22s without being a criminal for doing so. Canadian Firearms Blog

(MIS À JOUR) : Pas de cause unique à la radicalisation des jeunes, mais des constantes
Il n'y a pas de cause unique à la radicalisation, pas plus qu'il y a de portrait type de la personne radicalisée, mais certaines constantes se dégagent tout de même d'une recherche détaillée menée après que des jeunes du Collège de Maisonneuve et d'ailleurs eurent tenté d'aller faire le djihad en Syrie. Le Centre de prévention de la radicalisation menant à la violence (CPRMV) a présenté à Montréal, vendredi, le rapport d'analyse réalisé à la demande du Collège de Maisonneuve... Le maire de Montréal, Denis Coderre, a également salué le travail du Centre et a noté que les services policiers, le Collège de Maisonneuve et les gouvernements avaient déjà amorcé des démarches de toutes sortes. Il a rappelé que **le ministre fédéral de la Sécurité publique, Ralph Goodale**, avait manifesté son appui et même sa volonté de s'inspirer de l'expérience québécoise pour le reste du Canada. Presse Canadienne (La Presse) ; Montreal Gazette

Broadcast media / Médias télédiffusés :

CBC News' Power & Politics interviewed Christianne Boudreau, mother of Damian Clairmont who was killed fighting for ISIS, regarding the radicalization of Aaron Driver. **Public Safety Minister Ralph Goodale** was mentioned during this segment. Rough Transcript

TOP STORIES / MANCHETTES

No signs that plane crash linked to national security: RCMP
RCMP probing a fatal crash in southern Ontario involving a stolen plane say there is no indication that the incident is linked to national security. RCMP released a statement into the investigation into the Aug. 12

crash in which 20-year-old Markham Ont. man Mohammad Hassan Chaudhary was killed. Chaudhary was the sole occupant of the Piper aircraft, which crashed on a street in Peterborough, Ont. after it was allegedly stolen from an airport in Markham. Authorities said Friday that they have "no information to indicate there is a link with national security. "The investigation has not revealed the motive for the theft and all indications are that the young man acted alone." RCMP is working with local authorities, including York Regional Police, to investigate the crash in Peterborough, Ont. CTV News

Aaron Driver's dad believes alleged terrorist wanted 'suicide by cop'
The father of a suspected terrorist shot dead by police in Strathroy, Ont. last week believes his son didn't want to kill anybody other than himself when he set off a homemade explosive in the backseat of a cab as Mounties pulled their guns on him. In an interview Friday, Wayne Driver said his youngest son Aaron - who police allege planned to attack an urban centre during rush hour - built a bomb that wasn't strong enough to severely injure anyone. Based on a note that Aaron left behind, Wayne Driver said he's convinced his son wanted instead to commit "suicide by cop." Toronto Star

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Dalhousie professor calls for 'controlled, prescribed burns' after Nova Scotia wildfires
The majority of Nova Scotia is once again under burn restrictions as the dry weather creeps back in. A Dalhousie University professor says the province should be more proactive when it comes to preventing wildfires. Global News

Five things to know about wildfires as hot, dry, windy weather sparks warning from B.C. Wildfire Service
British Columbia is experiencing a mild forest fire season compared to last year's record-breaker, but B.C. Wildfire Service officials are warning this weekend's predicted hot, dry weather could see a spike in fires throughout the province. Here are five things about the fire season you should know: Fires this year are well below B.C.'s long-term average. Vancouver Sun

What you need to know about home disaster restoration
On August 13, Ontario's uncharacteristically dry summer was interrupted by a torrential downpour and extremely high winds. Environment Canada issued a severe thunderstorm watch for much of southern Ontario, while Guelph, Erin, Southern Wellington County, Region of Waterloo, Kitchener and Cambridge were on alert for the possibility of a tornado. Toronto Star

This Is What the Ice-Free Northwest Passage Looks Like
An ice-free Northwest Passage was once the stuff of legend. But it's now becoming the norm thanks to global warming, and commercial freighters to luxury cruise ships are racing to turn a profit off the newest frontier on earth... The Crystal Serenity, a hulking 820-foot, 13 deck cruise ship, set out earlier this week from Anchorage on a 32-day voyage that will end in New York. It's the largest ship to ever pass through the Northwest Passage. But with a driving range on board, the cheap berths going for $22,000 and $50,000 emergency evacuation insurance policies required for each passenger, it's made, shall we say, waves. Bonner County Daily Bee; Climate Change News; Gulf News

Thank you for a magnificent response to wildfires
An opinion piece states, "During the more than 50 years that I have lived in Queens, I have often been impressed by the resilience and bounce-back of its residents, but never more so than recently, during huge fight against the forest fires. While some of the fires were in Annapolis County, they were all fought from bases in Queens..." Chronicle Herald

NATIONAL SECURITY / SÉCURITÉ NATIONALE

No signs that plane crash linked to national security: RCMP
RCMP probing a fatal crash in southern Ontario involving a stolen plane say there is no indication that the incident is linked to national security. RCMP released a statement into the investigation into the Aug. 12 crash in which 20-year-old Markham Ont. man Mohammad Hassan Chaudhary was killed. Chaudhary was the sole occupant of the Piper aircraft, which crashed on a street in Peterborough, Ont. after it was allegedly stolen from an airport in Markham. Authorities said Friday that they have "no information to indicate there is a link with national security. "The investigation has not revealed the motive for the theft and all indications are that the young man acted alone." RCMP is working with local authorities, including York Regional Police, to investigate the crash in Peterborough, Ont. CTV News

Aaron Driver's dad believes alleged terrorist wanted 'suicide by cop'
The father of a suspected terrorist shot dead by police in Strathroy, Ont. last week believes his son didn't want to kill anybody other than himself when he set off a homemade explosive in the backseat of a cab as Mounties pulled their guns on him. In an interview Friday, Wayne Driver said his youngest son Aaron - who police allege planned to attack an urban centre during rush hour - built a bomb that wasn't strong enough to severely injure anyone. Based on a note that Aaron left behind, Wayne Driver said he's convinced his son wanted instead to commit "suicide by cop." Toronto Star

Terrorists don't speak for me
An opinion piece states, "Aaron Driver does not speak in my name, the name of my community and my faith, Islam. His views are strange, illogical, unethical, dangerous and contradict all what I know about my faith and my community. As a Canadian Muslim and a spiritual leader of the Canadian Muslim community, I pledge here and now to stand firm against the evil of terrorism and terrorists. I also applaud the efforts of the RCMP and its partners in thwarting a planned attack..." London Free Press

Preventing another Aaron Driver
Letters to the editor state, "Re: 'We are thirsty for your blood," Aug. 12. One needs to only look at Aaron Driver's history. His family home burned down at the age of 4, his mother died when he was 7. He was part of a military family that moved around frequently. All the things that were supposed to provide him with safety were gone... Can terrorism be justified? Is hatred more powerful than love? As an Ahmadi Muslim, the answer is clear that terrorism has no place in Islam or any religion..." Toronto Star

Letters to the Editor: Aug. 20
A letter to the editor states, "We're all responsible. I applaud and feel we as a community should support and call for programs that will alert all citizens to the increasing danger of our youth being radicalized by cleverly disguised recruiters in our community or via the Internet. It is not the responsibility of our Muslim community and the London Muslim Mosque alone. The responsibility lies with each one of us, regardless of our ethnic and religious affiliation... Monitor mosques. Aaron Driver, the 24 year old ISIS sympathizer, came from a good family but soon found himself striving for the wrong cause. The problem, in my opinion, is that too many youth are disenfranchised within their communities. They have nowhere to go, nowhere to belong, and that's exactly what ISIS is looking for. Extremism gives these youth a purpose, albeit a terrible one, and a sense of belonging... Counter toxic narratives. It is really shocking to see that a youth who was born and raised in Canada had fallen prey to the toxic ideology of ISIS. The recent public endorsement of ISIS by Aaron Driver is yet another warning that home-grown terrorism has infected our country and we need to be extremely vigilant..." London Free Press

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Trial data set for alleged fentanyl importer
A September 2017 trial date was set Friday for suspected fentanyl importer Kasimir Tyabji-Sandana. Lawyer Janna Watts appeared for defence counsel Hersh Wolch and Tyabji-Sandana to schedule the hearing, which will be before a judge sitting without a jury...Tyabji-Sandana, 27, was arrested July 23, not

long after Canadian Border Services Agency officers in Vancouver intercepted a package destined for Calgary from China. Calgary Herald

Un argument anti-immigration qui se déguise
Présentement, l'Assemblée Nationale tient des consultations publiques sur les politiques d'immigration au Québec. Quand on jase d'immigration, il y a plusieurs conceptions erronées (ou tout simplement fausses) qui sont répétées. La journaliste Josée Boileau, associée avec le journal Le Devoir, a donné une entrevue ce matin à Gravel le Matin dans laquelle elle répétait l'un de ces mythes. Elle soulignait avoir peur « qu'on vide les pays étrangers des meilleurs » personnes qu'elles ont. Parmi les mythes qui me dérangent le plus, c'est celui-ci qui me dérange le plus! Soyons clairs, je me fous de la Tunisie ou de Haïti. Je me soucie des Tunisiens et des Haïtiens. Après tout, ces pays ne sont que des bouts de terre, c'est le bien-être des individus qui me préoccupe. Dès qu'un Tunisien ou un Haïtien arrive ici, son revenu augmente dramatiquement. Pour un Haïtien, cette augmentation est d'un facteur de 22! Pour un Tunisien, ce ratio est de 3.20! Ces chiffres sont basés sur le revenu moyen per capita, mais même au revenu moyen du bas 20% de la distribution des revenus au Québec, il s'agit d'une amélioration significative du niveau de vie ! Agence QMI (Journal de Montréal, Journal de Québec)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

New Snowden docs support claim of NSA cyberweapon hack
The latest documents from Edward Snowden, published by The Intercept on Friday, appear to support earlier reports that the National Security Administration's "secret" cyberweapons are anything but. The Intercept, whose reporters have access to files Snowden took from the agency in 2013, says a top-secret NSA manual contains the same 16-character alphanumeric tracking code that appears throughout a portion of code released online earlier this week by a group called The ShadowBrokers. The group was auctioning off the code, which it said was stolen from the NSA. CNET News

IPhone hackers pick wrong target — a UW expert
apil Haresh Vigneswaren was just scribbling in a University of Waterloo lab, trying to finish a grad student assignment on cryptography and network security. That's when the tinny little red-alert klaxon in his nearby iPhone went off... He dismissed the alert. It reappeared an instant later. This was trouble. His phone was in "lost" mode. A message on the screen playfully taunted him. Hey why did you lock my iPhone ha-ha. Call me. 1(234)567-890. Vigneswaren quickly realized he was being hacked. The phone number, with its obvious Sesame Street construction by The Count himself, felt vampire phoney. The Record

LAW ENFORCEMENT / APPLICATION DE LA LOI

Coquitlam RCMP car struck at intersection
Four people — including a child and two Coquitlam Mounties — were rushed to hospital this afternoon (Friday) following a collision on Barnet Highway in Coquitlam. Police say the accident happened shortly before 1 p.m. as the female driver of a white Hyundai was turning northbound onto Falcon Drive and struck a Coquitlam RCMP cruiser travelling west on Barnet, near Eagle Ridge GM. The woman also had a young child in the backseat, Cpl. Neil Roemer told The Tri-City News at the scene. The four occupants sustained minor injuries and were transported to the nearby Eagle Ridge Hospital in Port Moody. The incident remains under investigation. Barnet Highway reopened to traffic at around 1:20 p.m. Tri-City News

RCMP search rural B.C. property after receiving tip about girl missing since 1993
Mounties in Comox Valley have searched and excavated a rural property after receiving a tip from the public about a 23-year-old missing person's case. Fourteen-year-old Lindsey Nicholls was last seen walking down the street to meet friends at a B.C. Day Celebration in Comox on Aug. 2, 1993. RCMP say next month would be her 38th birthday and her family has never given up hope that one day they would have answers about her disappearance. RCMP say 20 forensically trained police officers spent two days

this week searching a rural property with an excavator in response to a tip. Mounties say the search has been completed but the results cannot be shared as the investigation is ongoing. Canadian Press (Toronto Sun, Canoe.ca)

RCMP arrest man wanted on nation-wide warrant in Sorrento
The Salmon Arm RCMP arrested Richard Robert Taylor, 28, wanted on a Canada-wide warrant for parole violations in Sorrento on August 10. Taylor was recently released from custody in the Lower Mainland and is alleged to have fled from police and damaged an RCMP vehicle in Salmon Arm on July 25. Salmon Arm Observer

#FraudRedFlags: RCMP enlist helpers to prevent phone fraud
Fraudsters targeting vulnerable Nova Scotians are prompting the RCMP to enlist friends and family to address the scourge. "We want Nova Scotians to have the conversation about these phone scams and #FraudRedFlags," said RCMP Cst. Tammy Lobb. Chronicle Herald

Port Hawkesbury man arrested for child sex charges
The RCMP Provincial Internet Child Exploitation Unit has arrested and charged a Port Hawkesbury man after an online child exploitation investigation. On Thursday, 28-year-old Malcolm Smith was arrested and has been charged with making arrangements to commit a sexual offence against a child. Chronicle Herald

Warrant execution nets $220,000 in drugs - police
Approximately $220,000 in drugs was seized by Kingston Police after a drug warrant was executed on Vine Street. Officers entered the residence at approximately 4 a.m. on Friday utilizing members of the drug enforcement unit, street crime unit and the emergency response unit, said a news release. Inside they located two kilograms of crystal methamphetamine and one-third a kilogram of cocaine. Officers also located about $15,000 in Canadian and American currency, digital scales, packaging materials, a vacuum sealer, and cell phones. Whig-Standard

OPP bust $1.7M marijuana grow-op at Ruthven greenhouse
Two men from the Greater Toronto Area are facing charges after OPP busted a $1.7 million marijuana grow operation at a greenhouse in Ruthven. On Aug. 17 around 9:30 a.m., Ontario Provincial Police executed a search warrant in the 1500 block of Essex County Road 34. Windsor Star

Edmonton-area father charged with incest, sexual exploitation
An Alberta father has been charged with incest and sexual exploitation for offences allegedly committed against his own daughter. The charges are the result of an investigation by ALERT's Internet Child Exploitation team. CBC News; Edmonton Journal

Saskatoon man, 43, charged with making and accessing child pornography
A 43-year-old man from Saskatoon has been charged in connection to a child sexual exploitation case. The Saskatchewan ICE unit received a complaint from a U.S. internet provider regarding a user that had saved child sexual abuse images to their account. The account was subsequently shut down. CBC News; StarPhoenix

Ottawa mayor Jim Watson blasts police union over treatment of chief
Ottawa Mayor Jim Watson says he's concerned criticism levelled against the city's police chief by the head of the union representing officers could undermine public confidence in the force. In a strongly worded letter sent to Ottawa Police Association president Matt Skof Thursday, Watson waded into the fracas and sided with police Chief Charles Bordeleau. CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Alberta dangerous offender who disappeared during powwow has violent, brutal past
A dangerous offender who escaped during an escorted visit to an Alberta powwow on Saturday has a history of "brutal" and "sadistic" violent assaults, according to documents from the Parole Board of Canada. Darrell Moosomin, 54, was at a powwow at the Samson Cree First Nation in Maskwacis, south of Edmonton, on Saturday evening when he walked away from the elder escorting him. RCMP have issued a Canada-wide warrant for his arrest. In 1994, Moosomin confined and tortured a woman for eight hours before she was able to escape, according to a parole board decision from May 2016, which denied him requests for full parole, day parole or the right to unescorted temporary absences. CBC News

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NIL

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Police need legal counsel on marijuana dispensary
Merritt RCMP are waiting to get legal counsel before taking any action against a medical marijuana dispensary that reopened last Thursday despite being denied a business license. "Everything seems — on the face of it — not up to par from a business license standard [and] from a lawful dispensary standard, so I think there has to be some research into what it is they're doing, what they are providing [and] what the purpose of the society itself is," said RCMP Sgt. Norm Flemming. Merritt Herald

Kelowna considers position on legalization of marijuana for task force
City staff have outlined how they view the legalization of marijuana for the federal legalization task force and are seeking council support for their position. Urban planning manager Ryan Smith in a report to council says with legalization sometime in 2017 assumed, staff believe minimum age of consent should be the same or higher than alcohol. Infotel.ca

Medicinal marijuana task force
An editorial states, "On Aug. 22, the City of Fernie has their next Committee of the Whole meeting. I attend these meetings regularly, and I'm expecting this upcoming one to be a little different. The City is planning to participate in the federal government's marijuana task force, and is hoping to incorporate the views and opinions of Fernieites in their form. The federal government has set up a task force of eight experts from a variety of fields, including doctors, lawyers and policy makers. The job of the task force is to collect information from across Canada in regards to the legalization of cannabis before submitting a report to Trudeau's cabinet. Essentially, this task force is laying the foundation for the legalization of marijuana in Canada. This proves that it isn't a question of if for the federal government – it's a question of when..." The Free Press

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Immigration minister hesitant to discuss Calgary imam held in Turkey
Canada's immigration minister says it's best if he doesn't say much about a Canadian imam who was jailed in Turkey shortly after last month's failed coup. "It might not be good for him or his family if we talk about details of this case in public," Immigration and Refugees Minister John McCallum said Friday.
Hamilton Spectator

INTERNATIONAL

NIL

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

ipoliticsca
The unflappable Ralph Goodale | iPolitics ift.tt/2bs0ii9

canfirearmsblog
MP Kerry Diotte fires at Ralph Goodale over 10/22 magazine controversy canadianfirearmsblog.ca/kerry-diotte-f…

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

CBCNB
42,000 uninsurable N.B. homes expected to get flood coverage

NATIONAL SECURITY / SÉCURITÉ NATIONALE

PnPCBC
Now on #pnpcbc: @ChristianneBoud of @Mothers_4_Life on what the govt needs to do to better counter radicalization efforts

PnPCBC
Counter radicalization efforts? @ChristianneBoud: The gov't failed Aaron Driver & his family; the haven't been handling the issue #pnpcbc

PnPCBC
On losing her son, @ChristianneBoud: "Knowing what we know today, we could have saved Damian" #pnpcbc

TorontoStar
Aaron Driver's dad believes alleged terrorist wanted 'suicide by cop' on.thestar.com/2btJ5DQ pic.twitter.com/cxioh5QyXi

CTVNews
No signs that plane crash linked to national security: RCMP ow.ly/k9VR303p0j4 pic.twitter.com/X4P4LVAhiH

StewartBellNP
Plane crash not a national security investigation: RCMP.

StarOpinion
Reader letter: Preventing another Aaron Driver: on.thestar.com/2bjOWLr

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

globalnews
Peterborough plane crash: Should there be more security at private airports? glbn.ca/dt8AXT

HeraldHeadlines
Trial data set for alleged fentanyl importer dlvr.it/M4LXtm

LAW ENFORCEMENT / APPLICATION DE LA LOI

calgaryherald
Okotoks RCMP are looking for Sharita Dakota Ahpay who was last seen Saturday ow.ly/xvjy303pi4l

calgarysun
RCMP search B.C. property after receiving tip about girl missing since 1993 ow.ly/ghLw303p4Nl pic.twitter.com/nuwKC3D5Am

chronicleherald
#FraudRedFlags: RCMP enlist helpers to prevent phone fraud herald.ca/8kJ

chronicleherald
Port Hawkesbury man arrested for child sex charges herald.ca/7vC

TheWindsorStar
OPP bust $1.7M marijuana grow-op at Ruthven greenhouse ow.ly/QFZX303oc6h pic.twitter.com/wqMsxB7yWo

CBCCalgary
Alberta man charged with incest, sexual exploitation ift.tt/2b4ErxV pic.twitter.com/l2omFT2cTb

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

CBC_Aboriginal
Alberta dangerous offender who disappeared during powwow has violent, brutal past ift.tt/2b2NKOH pic.twitter.com/9ud2RI40P7

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

Today's News / Actualités
August 22, 2016 / le 22 août 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Security experts laud Liberals' go-slow approach to reviewing Conservatives' anti-terror laws
The Liberal government's unhurried approach to its promised reform of national security laws is appropriate given the dangers of getting it wrong, say security policy experts. The Aug. 10 police killing of would-be jihadi bomber Aaron Driver in Strathroy, Ont., renewed questions about the Grits' campaign-trail pledge to dismantle parts of the contentious Anti-terrorism Act, previously Bill C-51. The legislation was rushed into law by the former Conservative government in June 2015 with the qualified support of the then-opposition Liberals, who promised to fix several "problematic elements" if elected. The new government has delivered on a commitment to table legislation to create a special committee of parliamentarians to review select activities and the strategic direction of the country's expanding national

security apparatus. But the planned changes to C-51 remain in a state of flux and secret, with Public **Safety Minister Ralph Goodale** suggesting last week that proposed reforms won't be put before Parliament until next year. **Goodale** said officials will need the rest of this year to consult with security experts, rights advocates and the public on the broader question of how to structure the post-9/11 national security state. That's expected to hit high gear this fall with the anticipated release of national security framework consultation paper. Postmedia Network (National Post)

TOP STORIES / MANCHETTES

Canadian Police Don't Want to Talk About How They Spend Surveillance Dollars
Police in Ontario's biggest cities have received hundreds of thousands of dollars in grants to deploy unspecified surveillance equipment as part of an obscure provincial program. The problem is, no one knows exactly what they're buying with all that money. Police in Toronto, Ottawa, and the municipalities of Peel and York (near Toronto) have received hundreds of thousands of dollars each to pay for the Provincial Electronic Surveillance Equipment Deployment Program (PESEDP). This little-known project is described by police as "funding for the purchase of, or improvements to, equipment used in the investigation of organized crime", which doesn't reveal much. Mentions of the program can be found in publicly-available meeting agendas and reports dating back to 2011. Between February and June of this year, the Toronto police spent $100,000 on PESEDP, although they won't publicly offer any specifics. Documents produced by the York Regional Police Services Board and the Peel Police Services Board show that both forces received $200,000 each to fund PESEDP, in 2011 and 2013, respectively. York Regional Police got another $100,000 in 2016. (…) The Ottawa Police Service, Toronto Police Service and the York Regional Police all refused to answer questions about PESEDP. Toronto Police Service spokesperson Mark Pugash replied to questions about PESEDP by stating that "[Toronto Police Service does] not discuss investigative techniques or equipment." (…) In December 2015, Toronto Police Service denied having or using Stingrays or cell-site simulators, but a 2016 court case forced the TPS to reveal that they applied for permission to use a Stingray-type device as part of a gang investigation. The Vancouver Police Department has also admitted to using a Stingray device on loan from the Royal Canadian Mounted Police, Canada's federal force. (…) Many experts believe that local police departments borrow such devices from the RCMP, instead of owning them, adding to the mystery of what kinds of surveillance equipment local police are spending so much money on. Motherboard

Corrections officials reviewing case of dangerous offender who escaped custody
Correctional Service Canada is reviewing the case of Darrell Moosomin, a dangerous offender with a violent history who escaped custody in Maskwacis, Alta., during an escorted temporary absence. Moosomin, who had been wanted on a Canada-wide warrant, was arrested without incident around 6 p.m. Sunday on Highway 13 just east of Daysland. A member of the public had reported to police that a man matching Moosomin's description was hitchhiking on the highway. Moosomin, 54, remains in police custody awaiting a hearing, Killam RCMP said. He had been unlawfully at large for eight days. A review of Moosomin's escape is being conducted, Jeff Campbell, regional communications manager for Correctional Service Canada, said Monday. "Part of the information gathering that comes as an early part of that review is already underway and will certainly be augmented now that the offender who was at large is now back in custody." Campbell said. "We will speak with him and gather up some more information as part of that investigation." Escapes and other serious incidents are reviewed as a matter of standard operational procedure, he said. "We look to see if there are any changes that need to be made in terms of maintaining public safety." Campbell didn't speak to the specifics of Moosomin's case. But he said that when an offender is taken into custody after being unlawfully at large, "one of the efforts we undertake is to ascertain what he or she was doing while they were at large. "(They) could also be facing some new criminal charges," he said. "We are getting input from an offender themselves, typically we'd also talk to police, and there may be a role for courts involved as well." CBC News; Radio-Canada; Winnipeg Sun (Toronto Sun, Ottawa Sun, Edmonton Sun, Calgary Sun); 660 News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Garneau says he'll act fast to figure out what caused Toronto train derailment
Transport Minister Marc Garneau says he intends to act swiftly if it's determined safety lapses caused a Toronto train derailment over the weekend. Part of a Canadian Pacific freight train derailed in the city's mid-town early Sunday, but police and railway officials said the incident posed no threat to public safety. Canadian Press (iPolitics, Winnipeg Sun, Calgary Sun, Ottawa Sun, Edmonton Sun)

Crews clean up freight train derailment in midtown Toronto
Crews are cleaning up after a Canadian Pacific Railway train derailment in midtown Toronto on the weekend that resulted in a leak of 1,200 litres of diesel fuel next to a residential area... Coun. Josh Matlow, who represents Ward 22, St. Paul's, told CBC's Metro Morning on Monday that the derailment raises serious concerns. "Having this derailment happen so close to home, certainly I hope it serves as a wake-up call to the federal government to accelerate their commitments on improving safety standards as we requested," he said. CBC News

Bear Creek Provincial Park campground evacuated due to wildfire risk
Central Okanagan Emergency Operations says it has evacuated the Bear Creek Provincial Park campground because of a wildfire that appears to be steadily growing along Westside Road in West Kelowna. CBC News; Canadian Press (Vancouver Sun, Whig-Standard, London Free Press)

Luxury cruise to Arctic sails into controversy and opportunity
For the 1,000 passengers aboard the Crystal Serenity cruise ship, climate change has brought a luxurious opportunity: to sail into the history books on the largest passenger vessel to traverse the once unnavigable Northwest Passage. The historic voyage has never before been possible for such a large ship, but climate change has nudged open the door to the Arctic. The arrival of the massive 820-foot ship and its wealthy passengers (each paying from $20,000 to $120,00 for the month-long journey) has brought a flurry of excitement and tourist income to the remote town of Nome, Alaska. But it has also brought intense scrutiny from the critics, who say Crystal Cruises is capitalizing on the destruction of the planet. Christina Science Monitor; The Week; Tech Times

Broadcast media / Médias télédiffusés :

Fire crews in British Columbia's Okanagan Valley were hard at work over the weekend. Multiple wildfires have forced dozens. People from their homes and residents there remain on alert. (CBC News Network, 11:45 ET; CTV Vancouver, 9:30 ET, 11:00 ET, 11:30 ET; CityTV Vancouver, 9:00 ET)

The federal minister of Transportation, Marc Garneau, says he wants to learn why two trains collided near a densely populated part of Toronto. It happened in what's called the annex area. It's in a central part of the city just northwest of the downtown core. A westbound train struck an eastbound one that was changing tracks at the time. (CBC News Network, 10:00 ET, 11:00 ET, 12:30 ET; CP24, 12:30 ET; CHCH News 12:00 ET)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Is Richard Bain a terrorist?
On election night 2012, Richard Bain opened fire on a group of people he believed were Parti Québécois supporters, killing one man and severely injuring another, as premier-designate Pauline Marois gave her victory speech inside the Metropolis nightclub. At the time, Bain seemed to claim responsibility on behalf of all disgruntled anglophones. "The English are waking up!" he cried upon his arrest. Then in a variety of Facebook posts, jailhouse interviews and letters, he spoke alternately about his "vision" for a separate Montreal - his mission from God - and how he wanted to kill as many separatists as possible. So why didn't the charges against him include terrorism? (...)Bain's entire defence consisted in pleading that he wasn't anti-PQ or anti-francophone - he worked and lived with francophones all his life - but he was ill. "As

far as I'm concerned you're dealing with a lunatic, not a terrorist," Bain's lawyer, Alan Guttman, told the Gazette. "A guy goes on a shooting spree in a blue bathrobe. You're dealing with a madman." Terrorists, on the other hand, "are recruited and brain-washed," Guttman said. After evaluating Bain, psychiatrist Marie-Frédérique Allard concluded he was "most likely" suffering from an undiagnosed mental illness, possibly bi-polar disorder, at the time of the incident. But Bain's written responses to Allard two months after the incident seem to speak of a political agenda. Montreal Gazette

Yes, the threat of terrorism is real Mr. Prime Minister
An opinion piece states, "You can hardly blame Canadians if we continue to have lingering doubts about just how serious Justin Trudeau is about terrorism. His delayed response in even commenting on the alleged plot that led to the death of Aaron Driver in Strathroy Ontario is hardly reassuring. Immediately after this serious near miss with Driver headlines like "PM Justin Trudeau marches in Montreal Pride parade" and "Justin Trudeau to apologize for historic persecution of gay Canadians" and frivolous stories about a "shirtless" Prime Minister in Tofino were grabbing the attention of the mainstream media. (…)Interestingly enough the anti-terroism bill brought in by the Harper government that Justin Trudeau campaigned against and which the Liberals continue to threaten to water down may have at least been partially responsible for thwarting the Aaron Driver attack. Just maybe Erin O'Toole, the public safety critic for the Conservative Party is correct that his party's Bill C51 already provides the right "balance" in giving police needed powers in cases of suspected terrorism. Contrastingly Trudeau rammed through his controversial, radical and politically motivated Bill C-6 which gives a convicted Islamist terrorist Canadian citizenship most certainly making Canada more vulnerable to a terrorist attack." Canada Free Press

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Deputies: Man accused in school threats allowed to enter Canada after arrest
The man arrested after he was accused of threatening to place bombs and shoot students at several Orange County schools has been released, deputies say. Jesus Kong, 23, who is also known as as Jessie Eloah Calix and Jesus Matute, was arrested while attempting to cross the Canadian border. He was questioned and then allowed to enter Canada, Sheriff's Office spokesman Jeff Williamson said. Williamson did not specify where the border was. When he was arrested, he "appeared to be in some form of distress," Williamson said, adding the warrant charges were not out of Florida. Details of the arrest were not available Sunday. It's not clear if any charges will be filed. Orlando Sentinel

Canadian border agency: Leave your guns at home, America
The Canada Border Services Agency is reminding residents of the United States that bringing guns over the border is a major no-no unless you have the required permits and store them properly. The CBSA issued a statement Monday afternoon announcing it is launching "a firearms awareness campaign" to gently remind U.S travellers about Canadian law. "It is strongly recommended that you not carry your firearm when travelling to Canada and/or transiting through Canada to reach another U.S. destination." The reminder comes less than ten days after two men from Texas tried to bring hidden guns across the border on separate Canadian vacations. Global News

Canadian border services looking at steel rebar imports in anti-dumping probe
The Canada Border Services Agency (CBSA) has launched an anti-dumping investigation into concrete reinforcing bar, or rebar, shipped into Canada from several areas of Europe and Asia. With a special import measure currently in place on rebar from China, South Korea and Turkey, the border service will investigate whether or not rebar is being sold in Canada at unfair prices, and in turn, hurting Canadian producers. Working on a complaint filed by three Canadian steel companies, the CBSA probe will look into rebar from Belarus, Portugal, Spain, Japan, Taiwan and Hong Kong. The Canadian International Trade Tribunal will also play a role in the investigation. According to the Canadian Steel Producers Association, the probe will be the second Canadian investigation into unfairly imported rebar in as many years. "It is vital for domestic steel producers and their employees that market-based competition in Canada is preserved," the organization's President, Joseph Galimberti, said. "This is an important investigation for the 22,000 Canadians employed directly and the 100,000 employed indirectly in steel." Canadian Manufacturing

City: Riverside Park fixes ahead of schedule
Mayor Mike Duggan and owners of the Ambassador Bridge say part of a $5 million plan to overhaul a riverfront park in southwest Detroit is two years ahead of schedule. On Monday morning, Mayor Duggan, representatives from the Detroit International Bridge Co. and neighborhood residents gathered at Riverside Park to watch the demolition of the final wall of a former Detroit News warehouse on West Jefferson. The warehouse, owned by an subsidiary of the bridge company, was originally planned to be razed in 2018. The warehouse is on 4.8 acres of land next to Riverside Park. The bridge company agreed to give that land to the city to expand the park. The bridge company, owned by members of the Moroun family, will also pay up to $5 million to overhaul the park. Riverside Park is a somewhat plain strip of 20 acres where West Grand Boulevard meets the Detroit River. Planned upgrades include a baseball diamond, soccer field, picnic and fishing areas and a riverside promenade. In September, the bridge owners paid $3 million toward the park upgrades. The park deal sparked controversy when it was unveiled in April 2015. That's partly due to the fact it keeps the bridge owners' hopes alive of building a second private span to the Ambassador Bridge. As part of the park deal, the city will transfer three acres of city-owned land to the bridge company, land it needs for the second span. Detroit News; Detroit Free Press; Windsor Square

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

China edges ahead in the race to build hack-proof cyber security systems
The international power struggle for the control of data has intensified with a number of Chinese companies now trying to challenge entrenched cloud vendors such as Microsoft, Google and Amazon. The growing market, targeted by Chinese players such as Huawei, Alibaba and Baidu, has raised serious questions about security of data storage and whether tech firms in China or elsewhere are vulnerable to attack. The National UAE

China's proposed cyber law unnerves foreign players in cloud
International platforms such as Google, Facebook and Twitter are already banned in China. But there are worries about a new cyber security law being formulated in Beijing that would require data collected in China to remain in the country. The National UAE

Commentary: Evidence points to another Snowden at the NSA
An opinion piece states, "In the summer of 1972, state-of-the-art campaign spying consisted of amateur burglars, armed with duct tape and microphones, penetrating the headquarters of the Democratic National Committee. Today, amateur burglars have been replaced by cyberspies, who penetrated the DNC armed with computers and sophisticated hacking tools... Now, in the latest twist, hacking tools themselves, likely stolen from the National Security Agency, are on the digital auction block. Once again, the usual suspects start with Russia – though there seems little evidence backing up the accusation..." Reuters

LAW ENFORCEMENT / APPLICATION DE LA LOI

Canadian Police Don't Want to Talk About How They Spend Surveillance Dollars
Police in Ontario's biggest cities have received hundreds of thousands of dollars in grants to deploy unspecified surveillance equipment as part of an obscure provincial program. The problem is, no one knows exactly what they're buying with all that money. Police in Toronto, Ottawa, and the municipalities of Peel and York (near Toronto) have received hundreds of thousands of dollars each to pay for the Provincial Electronic Surveillance Equipment Deployment Program (PESEDP). This little-known project is described by police as "funding for the purchase of, or improvements to, equipment used in the investigation of organized crime", which doesn't reveal much. Mentions of the program can be found in publicly-available meeting agendas and reports dating back to 2011. Between February and June of this year, the Toronto police spent $100,000 on PESEDP, although they won't publicly offer any specifics. Documents produced by the York Regional Police Services Board and the Peel Police Services Board

show that both forces received $200,000 each to fund PESEDP, in 2011 and 2013, respectively. York Regional Police got another $100,000 in 2016. (…) The Ottawa Police Service, Toronto Police Service and the York Regional Police all refused to answer questions about PESEDP. Toronto Police Service spokesperson Mark Pugash replied to questions about PESEDP by stating that "[Toronto Police Service does] not discuss investigative techniques or equipment." (…) In December 2015, Toronto Police Service denied having or using Stingrays or cell-site simulators, but a 2016 court case forced the TPS to reveal that they applied for permission to use a Stingray-type device as part of a gang investigation. The Vancouver Police Department has also admitted to using a Stingray device on loan from the Royal Canadian Mounted Police, Canada's federal force. (…) Many experts believe that local police departments borrow such devices from the RCMP, instead of owning them, adding to the mystery of what kinds of surveillance equipment local police are spending so much money on. Motherboard

News In Brief: $90,000 grant opens more counselling services for veterans in Winnipeg
Canadian Legion Manitoba/Northwest Ontario Command will mean more counselling services for local veterans. The command provided the grant to the Veterans Transition Network and will fund counselling and transition services for veterans who are not covered by Veterans Affairs Canada or the Department of National Defence. The Veterans Transition Network is a Canadian charity that delivers group-based programs to assist current and former members of the Canadian Forces and RCMP struggling with the transition to civilian life. Winnipeg Free Press

Grande Prairie RCMP seek assistance in finding 16 year-old girl
Grande Prairie RCMP are asking for the public's help in locating a missing 16 year-old girl. Madelyn Whyte (16) was reported missing on August 20th 2016. Whyte is from Dawson Creek but police think she may be in the Grande Prairie area. Madelyn Whyte is described as: Aboriginal; Shoulder length blonde/faded orange hair; Brown eyes; 5'2" tall; 130 lbs; Multiple scars on both arms; Possibly wearing a wrist brace. Energetic City

Glenn Bauman charged with murder in case of missing Wellesley mother Linda Daniel, daughter Cheyenne Daniel
Waterloo Regional Police detectives, with help from the RCMP, have charged an Alberta man with two counts of first degree murder and two counts of indignity to a body in connection with the disappearance of a mother and daughter from Waterloo region. Linda Daniel and Cheyenne Daniel were 47 and 13 years old, when they disappeared in July, 2011. Their last known address was in Wellesley Township. Police arrested Glenn Kraemer Bauman, 43, on Friday in Valleyview, Alta., a town about three hours northwest of Edmonton, on a Canada-wide warrant. CBC News

Old bomb disposed of by Gagetown team
A team from CFB Gagetown disposed of an old military ordnance Monday morning that had been stored in outbuilding in Goose River, near St. Peter's, P.E.I., for years. RCMP received the call to get rid of the device on Sunday. It was determined it was safe to wait until a team could arrive from New Brunswick to dispose of it. The area was secured until the team arrived. "It appeared to be a bomb of sorts, maybe an airplane bomb with fins on it. It was about 12 inches [30 cm] long and four inches [10 cm] wide," said RCMP Cpl. Ron MacLean. MacLean said the bomb was likely decades old. The ordnance was originally found many years ago, RCMP said. RCMP reminded the public that military ordnance can be volatile and should not be handled or moved. CBC News; Journal Pioneer

New Kings RCMP district commander takes the helm
The Kings District RCMP is welcoming a new district commander who begins working out of the New Minas detachment today, Aug. 22. S/Sgt. Dan Morrow, a 23-year veteran of the force, comes to Kings District from Eskasoni First Nation in Cape Breton where he was posted for nine years. "I'm really looking forward to taking on this new and challenging role within Kings District," Morrow said. "I want to ensure the RCMP continues to be an integral part of the community while meeting the needs of those we serve." Morrow grew up in Manitoba and enrolled with the RCMP in 1992. Since then, he has gained diverse experience working in the RCMP's General Investigative Services, Traffic Services Unit, Customs and Excise Program and Undercover Operations. His role in New Minas marks his tenth detachment with the force. As district commander, Morrow will be promoted to the rank of Inspector, responsible for

monitoring and guiding administrative and operational functions in Kings District and working with stakeholders to identify and implement local policing priorities. "It's very important for me to get to know the stakeholders and citizens in the area so I encourage them to take a minute to stop by the detachment to introduce themselves and say hello," Morrow said. Nova News Now (Kings County News)

RCMP investigates threats made to Brazeau County Council
The Brazeau County Council received threats via text on Aug. 12 at 6 p.m. Drayton Valley RCMP reported that investigations led to the arrest of an individual in Edmonton on Aug. 16. The local RCMP was also present at the Brazeau County Council meeting on Aug. 16. The case is still under active investigation. Drayton Valley Western Review

Hate speech vs. freedom of speech in the age of social media
The social media firestorm following the shooting death of Colten Boushie, 22, has prompted questions of what constitutes hate speech in the digital age. The racist and hateful statements in some comment sections have prompted Premier Brad Wall to speak out, writing on his Facebook page "racism has no place in Saskatchewan" last weekend. The RCMP have stated they are actively investigating all social media posts that could be considered hate speech. Ken Norman is a professor at the College of Law at the University of Saskatchewan. He said that for a comment to be considered hate speech, certain elements must be at play in the statement. (…) Norman added our law does not allow people to say the most violent kinds of racist things without the law stepping up and that posts on social media can constitute hate speech as they are public statements. "RCMP I think are rightly looking into this and should take very seriously this kind of level of hatred," he said. CBC News

Broadcast media / Médias télédiffusés :

It's not just on Canadian university campuses that the issue of rape culture is being debated. The RCMP and the Canadian military have both been criticized for harassment and sexual assault within their ranks. (CPAC, 3:33ET)

CBC Vancouver reported on the death of a man in Terrace, B.C. last week who died after RCMP hit him with a Taser. (CBC Vancouver, 10:00ET)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Corrections officials reviewing case of dangerous offender who escaped custody
Correctional Service Canada is reviewing the case of Darrell Moosomin, a dangerous offender with a violent history who escaped custody in Maskwacis, Alta., during an escorted temporary absence. Moosomin, who had been wanted on a Canada-wide warrant, was arrested without incident around 6 p.m. Sunday on Highway 13 just east of Daysland. A member of the public had reported to police that a man matching Moosomin's description was hitchhiking on the highway. Moosomin, 54, remains in police custody awaiting a hearing, Killam RCMP said. He had been unlawfully at large for eight days. A review of Moosomin's escape is being conducted, Jeff Campbell, regional communications manager for Correctional Service Canada, said Monday. "Part of the information gathering that comes as an early part of that review is already underway and will certainly be augmented now that the offender who was at large is now back in custody." Campbell said. "We will speak with him and gather up some more information as part of that investigation." Escapes and other serious incidents are reviewed as a matter of standard operational procedure, he said. "We look to see if there are any changes that need to be made in terms of maintaining public safety." Campbell didn't speak to the specifics of Moosomin's case. But he said that when an offender is taken into custody after being unlawfully at large, "one of the efforts we undertake is to ascertain what he or she was doing while they were at large. "(They) could also be facing some new criminal charges," he said. "We are getting input from an offender themselves, typically we'd also talk to police, and there may be a role for courts involved as well." CBC News; Radio-Canada; Winnipeg Sun (Toronto Sun, Ottawa Sun, Edmonton Sun, Calgary Sun); 660 News

Détenu mort à Dorchester: des gardiens ont fait usage d'une « force inappropriée » selon un rapport

Étendu sur le sol d'une douche du pénitencier de Dorchester, au Nouveau-Brunswick, Matthew Hines a prononcé ces mots qui ont peut-être été ses derniers : « S'il vous plaît, je vous en supplie, je vous en supplie. » Les gardiens du pénitencier de Dorchester ont alors ouvert le robinet de la douche.Trente secondes plus tard, ils le refermaient. Le détenu de 33 ans semblait pris de convulsions.Il a été conduit à l'Hôpital de Moncton - à une demi-heure de route de Dorchester - où on a constaté son décès.Depuis 13 mois, la famille de Matthew Hines, qui vit au Cap-Breton, croyait la version des faits rapportée par Service correctionnel Canada. L'agence avait conclu que Matthew, qui avait déjà eu des épisodes de convulsions dans le passé, était mort des suites d'une surdose de drogue qui aurait déclenché les convulsions. Les services correctionnels se sont faits avares de commentaires au sujet de cette mort, survenue le 27 mai 2015. Au moment du décès, l'agence avait publié un communiqué disant que Matthew Hines « avait eu besoin d'attention médicale » et que le personnel avait procédé « immédiatement » à des manoeuvres de réanimation cardiorespiratoire. (...)Service correctionnel Canada a refusé une entrevue sur cette histoire. Dans une déclaration écrite, la porte-parole Lori Halfper précise qu'elle ne peut discuter des détails entourant la mort de Matthew Hines, ni d'éventuelles mesures disciplinaires contre des membres du personnel, à cause des lois sur la protection de la vie privée. Elle ajoute que l'enquête en cours sur la mort du détenu a déjà permis de cibler des procédures qu'il est possible d'améliorer, sans fournir plus de détails. Service correctionnel Canada a également refusé de fournir à CBC des copies des vidéos montrant l'altercation entre Matthew Hines et les agents, citant à nouveau la confidentialité de l'enquête entourant la mort du détenu. Radio-Canada

Calgary police say 'high-risk' serial rapist re-released

Convicted serial rapist James Alexander Parent has been re-released in Calgary. Parent was arrested last week after being released on Aug. 5. Police said Monday that Parent has been released after further investigation. Parent's convictions include the 1987 sexual assault of a woman inside her Calgary home. He stormed into the house wearing a mask and gloves, holding a knife to the victim's throat and threatening to kill her as he repeatedly raped her. He was convicted in 2011, identified over two decades later by DNA evidence from a rape kit. Parent was also previously found guilty on charges of indecent assault and kidnapping of two girls, ages eight and nine, in incidents from 1980 and 1982. He was convicted of break-and-enter with intent against two women in 1988. Parent will continue to be monitored by Correctional Service Canada, including electronic monitoring. Calgary Herald; CBC News; CTV News

Canada-wide warrant issued for Nunavut offender Willie Ishulutak

A Canada-wide warrant has been issued for a Nunavut man convicted of setting fire to an Iqaluit jail for breaching parole, according to a news release by the Ontario Provincial Police. The OPP is looking for Willie Ishulutak, a 36-year-old repeat offender who pleaded guilty to arson in May 2014 for setting a fire inside a washroom at Nunavut's Baffin Correctional Centre. Ishulutak is described as an aboriginal male, five feet four inches tall and 136 pounds. He has tattoos on both forearms and "INUKSTA" tattooed on his back. Police say he is known to frequent the Greater Toronto Area. The OPP say Ishulutak is serving a sentence of two years and five months for arson endangering human life, assault and intimidation. CBC News

Jeffrey MacLean's plea relating to Dorchester prison breakout delayed

A federal inmate accused of assaulting two women before stealing their car during an alleged breakout of Dorchester penitentiary had his pleas on the charges delayed again on Monday. Jeffrey MacLean will be back in court on Sept. 19 to answer charges of robbery, forcible confinement, assault with a weapon, flight, resisting arrest and theft over $5,000. The charges relate to incidents on Feb. 12 after an inmate escaped the Dorchester Penitentiary at 3:15 p.m. The inmate led police on a chase that ended on Charlotte Street in Fredericton. (...)While MacLean isn't being remanded into custody on these charges, he will remain behind bars at the Atlantic Institution in Renous where he is serving a previous sentence for armed robbery, robbery with violence and disguise with intent. CBC News

Broadcast media / Médias télédiffusés :

Police are warning the public again about the re-release of James Alexander Parent. He was arrested last week but released without any charges after an investigation. Parent will continue to be monitored by Correctional Service Canada. (CHQR-AM, 10:02)

L'ex-enquêteur du SPVM, Benoit Roberge demande son transfert en maison de transition. Benoît Roberge a été condamné à huit ans d'incarcération pour avoir vendu des informations aux Hell's Angels. Il aurait l'intention de demander à la Commission des libérations conditionnelles du Canada une semi-liberté. (RDI en direct, 10:35 ET)

A Sydney family is calling for change after learning details about the death of their brother, Matthew Ryan Hines, in Dorchester Penitentiary last year. After his death Correctional Services Canada originally said Hines was found in need of medical attention and CPR was started immediately, but more than a year later his family received an investigation report that told a different story. (CBC R1 St. John, 6:11, 6:31, 7:12, 7:31, 7:38; CBC R1 Fredericton, 6:12, 6:31, 6:58, 7:01, 7:15; CBC R1 Halifax, 6:32, 6:58; CBC R1 Windsor, 6:34; CBC R1 Moncton, 6:31; CBC R1 7:05

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Elizabeth Fry Society seeks clothing for newly released women
Tamara Delorme was wearing shorts and sandals when she was arrested last August, so when she was released from Pine Grove women's jail in February, the only clothes she had were the institutional grey sweat pants and sweat shirt she'd worn inside. "I came here to Elizabeth Fry and they gave me decent winter clothing I can wear. It builds up your self esteem if you have nice clothes to wear," Delorme said. The non-profit advocacy organization for women involved with the court system and corrections is now building on its practice of helping women find donated clothing when they're released or when they're going to court, said executive director Sue Delanoy. They've worked with Pine Grove director Michelle Gaudet to expand a small clothing depot at the institution and formally create institutional jobs for inmates who sort, fold and repair the items if necessary, Delanoy said. StarPhoenix

Peel Police Weigh in on Gun Crime Increase in Mississauga
The reveal didn't come as a terrible shock, as Peel Police Chief Jennifer Evans mentioned the worrying uptick earlier in the year and shooting incidents are dominating the news a little more than usual. But while the news is not good by any means, it's important to remain calm in the face of troubling statistics -- and to remember that Mississauga (and Ontario overall) is very safe. "Ontario [in general] is very safe," says Constable Mark Fischer, public information officer, corporate communications with Peel Regional Police. "Crime rates have been going down, so [this increase] could be an anomaly or a spike, but we're taking notice and want it to improve." According to the documents, there were 23 shooting victims in Peel in the first seven months of the year. That's an increase of 187 per cent from 2015 to 2016. In 2014, there were four victims and in 2015, there were eight. In 2014, there were 18 total incidents of shots being fired. In 2015, that number increased to 21. This year, there have been 43 incidents (this number does not include the very recent shooting at Sugar Daddy's night club over the weekend). As for stabbings, those are on the rise, too. Insauga

Les jeunes et les réseaux sociaux: quelques outils pour les parents
Facebook, Twitter, Instagram, Snapchat, pour de nombreux parents d'enfants et d'adolescents, il est plutôt difficile de se retrouver dans cet univers virtuel en constante évolution. Bruno Guglielminetti, spécialiste des nouvelles technologies et des médias numériques, nous éclaire quant aux règles d'or et aux précautions à prendre afin que soit saine l'utilisation des technologies numériques à la maison. Le Huffington Post l'a rencontré. (...) Bruno Guglielminetti l'a répété à de nombreuses reprises lors de notre entretien, «tout est dans la discussion et non dans l'oppression» en ce qui concerne l'utilisation des réseaux sociaux par les adolescents. «Rien ne sert de démoniser tout cela. C'est la discussion qui est la clé et qui contribuera à faire avancer le jeune dans sa réflexion.» Pour ce père de deux enfants, les dangers reliés à cette pratique sont similaires à ceux se retrouvant dans la société. «On ne fait que les

déplacer dans le monde virtuel. La grosse différence, c'est la portée qui est beaucoup plus grande si l'on compare, par exemple, avec l'enfant qui se faisait intimider en petit groupe à l'école jadis.» Cybersécurité, cyberintimidation (qui touche 1 jeune sur 10 au pays), communication et prédateurs sexuels, facilité de diffusion; ces dangers sont bien réels. Huffington Post

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Trudeau discusses China trade, marijuana legalization, and Donald Trump
In an interview that touched on everything from marijuana legislation to the inquiry into missing and murdered women, Prime Minister Justin Trudeau said he was looking forward to strengthening trade ties with China while also "challenging" the nation on human rights and other issues. Trudeau is set to embark on an eight-day visit to the Asian giant next week, and told CTV's Your Morning in a wide-ranging interview that China presents an opportunity for Canadian businesses to expand their exports Here's a sampling of what he had to say: (…)On why the inquiry into missing and murdered Aboriginal women is not looking into police conduct: "The idea that we would create an inquiry that would dive into individual cases would make it so cumbersome and would take so much time and resources, we wouldn't be able to have the same kind of impact we need to have to make those changes as quickly as we can." (…)On whether Canada has a problem with racially biased policing: "Yes, there are real challenges in our justice system that we have to address. But a lot of them, when you look at the root causes, have to do with education and opportunities and investment in those communities." (…)On why the federal government chose not to decriminalize marijuana while it works on legalizing it: "The reason why legalizing marijuana is the right step for us is because of two things: One, it will be make it harder for young people to access marijuana, because whatever you say about marijuana compared to alcohol or cigarettes, we know that the impact on the developing brain is something we need to prevent. Right now, young people have easy access. Controlling and regulating it will make it more difficult for them." CTV News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Le gouvernement du N.-B. s'apprête à annoncer son investissement dans le projet Zenabis
Radio-Canada a appris que le gouvernement du Nouveau-Brunswick annoncera mardi le montant de son investissement pour l'installation d'une usine de culture de marijuana médicinale à Atholville, dans le nord de la province. L'annonce devrait avoir lieu mardi à 9h, à l'intérieur de la future usine de Zenabis, située dans le parc industriel d'Atholville, au Nouveau-Brunswick. La province doit révéler le montant de sa contribution financière au projet. Radio-Canada

Saint John medical marijuana storefront operating illegally
The medical marijuana store that recently opened in Saint John might say it's going by the books to stay open but the location is still operating illegally in Canada, according to one lawyer. Medicinal Grounds Cannabis Centre owned and operated by Ryan Francis only allows in those over 19 years of age with a certified prescription from a doctor or a card from Health Canada. But the only licensed provider of medicinal marijuana in New Brunswick is currently OrganiGram, located in Moncton, according to Health Canada's website. Kathryn Wells, a criminal defence lawyer at Wells Frost Litigation Group in Toronto, told *Information Morning Saint John* the rules are clear when it comes to selling medicinal marijuana. "There's no grey area, either you have the exemption and the ability to obtain it for medicinal purposes or you're breaking the law," Wells said. She says despite the federal Liberal campaign promise to legalize marijuana, it is still an illegal substance under the Controlled Drugs and Substances Act. CBC News

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

NIL

INTERNATIONAL

NIL

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

Ralph Goodale
My letter to the editor in @WhigStandard thanking everyone who participated in #prisonfarm townhall http://bit.ly/2bbXzVb #cdnpoli

Ralph Goodale
Dans @WhigStandard je remercie participants à l'assemblée sur fermes penitentiaries (langue de parution originale) http://bit.ly/2bbXzVb

NAACJ
Another #heartbreaking story of #deathincustody http://bit.ly/2bO4R5P When will it end? #useofforce @RalphGoodale #OCI

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

BC Wildlife Service
URGENT: Amphibious aircraft en route to Bear Creek #BCwildfire near West #Kelowna. Boaters - please clear the area

IBC_West
Do you have an #emergency kit? It's never too late - shop or build your own! Easy as ABC123. http://goo.gl/jZFUVl

Canadian Red Cross
Download our Be Ready #app to prepare for disasters such as fires and floods: http://bit.ly/2bx3d6Z #beready

Public Safety Canada
Know someone with a lifetime of service to #SAR? Nominate them for the SAR Award for Exemplary Service http://ow.ly/eoK9303sRTb

Get Prepared
Before a severe thunderstorm, unplug radios, televisions and appliances. More steps to take: http://www.getprepared.gc.ca/cnt/hzd/svrstrms-bfr-eng.aspx …

NSPS (CBoC)
'It shouldn't happen': Transport minister wants to know what caused Toronto #derailment

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Amarnath Amarasingam
This ISIS video justifying attacks on coalition countries feat. quick clip of Aaron Driver. https://twitter.com/pieternanninga/status/767117165325615104 ...

Phil Gurksi
Where does research on radicalisation need to go?

Stewart Bell
...the same lawyer who argued Driver wasn't a threat and the peace bond violated his rights. http://www.lfpress.com

Mubin Shaikh
RequiredReading: On TerrorismPeaceBonds TPB's - Do we learn or do we jump2 "Insta-Conclusions" & how2do more of 1st. http://craigforcese.squarespace.com

BORDER SECURITY / SÉCURITÉ FRONATLIÈRE

Martin MacMahon
CBSA launches Firearms Awareness campaign for Americans tomorrow--last month I reported 100s of guns coming up here:

GC Newsroom
CBSA recommends leaving your firearms at home when travelling to Canada http://ow.ly/uwwD100hLBK

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

York U Continue
Canada Govt: #cybersecurity job market to rise by 6 mill in the next 4 years: http://ow.ly/Uwv1303sUYr Get qualified: http://ow.ly/E8lj303sV42

Public Safety Canada
The Government of Canada's public consultation on cyber security is underway. Have #YourCyberSay! http://ow.ly/5sy1303sHtt

Pensez cybersécurité
Quel site de magasinage en ligne utiliseriez-vous? Celui de gauche ou de droite? http://www.pensezcybersecurite.gc.ca/cnt/prtct-yrslf/prtctn-mn/nln-shpng-fr.aspx ...

Colin Freeze
NSA no longer to distinguish b/w offense (spying) & defence(cybersecurity) ops (& as it goes the other FVEYS follo)

Digital Forensics
#cybersecurity Security soars as a priority, but providers struggle to use tech… http://dfi.io/M5Hn3D #infosec

NatlCyberSecAlliance
#ICYMI Here's all the great tips from last week's #ChatSTC! Understanding the Digital Disconnect: https://staysafeonline.org/blog/chatstc-twitter-chat-understanding-the-digital-disconnect-parents-teens-and-the-internet/ … #CyberAware

LAW ENFORCEMENT / APPLICATION DE LA LOI

CJFE
No one other than the police forces involved know what kinds of surveillance equipment is being bought http://bit.ly/2bpWmq4 @motherboard

Jordan Pearson
York police and OPP have an agreement to "share services" to intercept and monitor personal communications:

CRCVC
Meet the pug and Schnauzer puppies joining the RCMP victim services in Prince George

OPP_Aboriginal Bureau
Starting another great week of learning & sharing #NiiganMosewak @ChiefDay @AnishNation @CBC_Aboriginal @APTN

GRC, Nouvelle-Ecosse
Le sergent d'état-major Dan Morrow, nouveau chef du District de Kings de la #GRCNE http://bit.ly/2bGUWLS

Youth in Policing
Chief @marksaunderstps and the #YIPI students continue in an open and honest discussion about #TheWayForward.

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

CBC – The Current
8:37am: As inmates die in overheated prisons, should air conditioning be a human right?

John Howard Society @ReducingCrime 3h3 hours ago
Ottawa and Ontario should make sure solitary is truly a last resort: Editorial http://on.thestar.com/2bjBF5B via @torontostar

John Howard Society
How many times will solitary confinement be misused before someone does something?

CRCVC
Calls for review of inmate escape after horrific crimes revealed in parole

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

CCJC
Crim instructor @Carleton_U calls 4 culturally sensitive police training when dealing w/new immigrants & refugees

NAACJ
Liberals eye exceptions to #MMPs http://bit.ly/2bwO0ml Great news! @puglaas @johnhoward_can @cancivlib @ipolitics #SafetyValve #cdnpoli

Sécurité publique
Vous êtes témoin de cyberintimidation? Prenez position! Vous avez le pouvoir de faire une différence! / c @cyber_securite

Public Safety Canada
If you see cyberbullying happen, don't stand by & remain silent! You can make a difference! #BystanderAwarenessMonth / c @getcybersafe

PUBLIC SERVICE / FONCTION PUBLIQUE

Alex Boutilier
The trick to ATIP is filing a bunch of requests and then going on three weeks vacation.

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

Today's News / Actualités
September 11, 2016 / le 11 septembre 2016
9:00 - 18:00 ET

This collection contains news items that appeared online between 9:00 a.m. and 6:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 9h00 et 18h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Les Canadiens se souviennent des événements du 11-Septembre
Alors que les États-Unis commémorent dimanche les attentats terroristes du 11 septembre 2001, les Canadiens souligneront également la mémoire de cet événement, qui a eu des résonnances chez eux également. Le premier ministre Justin Trudeau a tenu à rendre hommage aux victimes et à leurs proches, rappelant que 24 Canadiens avaient péri dans les attaques. **Le ministre de la Sécurité publique Ralph Goodale** a pour sa part soutenu que cet événement ***«brutal»*** avait permis de connaître ***«des héros»,***

soulignant par ailleurs la contribution des habitants de Gander, à Terre-Neuve. Cette ville située dans le nord-est de la province avait accueilli près de 7000 passagers qui avaient dû rester trois jours alors que leurs avions étaient cloués au sol. Plusieurs événements se tiendront à Gander dimanche. La Presse Canadienne (La Presse); Canadian Press (Brandon Sun, Metro News, London Free Press, Toronto Star, Chronicle-Herald); Radio-Canada

Montreal airport customs lineups are just the beginning
An opinion piece states "For all those first-time visitors arriving at Trudeau airport in Dorval these days, Montreal is blowing it. International passengers touching down at YUL this summer have faced customs lineups of epic proportions. The wait times can often run up to two hours. What impression does that make? But as returning Montrealers well know, that's just the tip of the iceberg. Or, should I say, the orange cone? Last week, a group of civic leaders sounded the alarm. A letter was sent to the federal minister of public safety, **Ralph Goodale**, on behalf of representatives of Aéroports de Montréal, Montréal International, Tourisme Montréal, the Board of Trade, Palais des congrès and carriers serving the airport. Together, they are calling on the federal government to find a durable solution to the problem of long delays in the international arrivals hall that have worsened since the beginning of the summer. Mayor Denis Coderre has also added his voice to those appealing to Ottawa for help." Montreal Gazette

TOP STORIES / MANCHETTES

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fort McMurray residents claim 'nightmare' dealing with insurance
Some Fort McMurray residents repairing homes damaged by May's wildfire say they've had it with insurance companies that don't return calls and emails, pressure them to accept low settlements or have been rude and unprofessional. "Horrible from the beginning. From mass evacuation, it's been absolutely a horrible nightmare," said Terena Gunderson, a homeowner in the Timberlea neighbourhood. Gunderson's claim is among the 27,000 residential claims filed due to the wildfire. It is Canada's costliest disaster with damages estimated at $3.58 billion, according to the Insurance Bureau of Canada. The bureau's latest stats show clients have filed 45,000 claims as of July, with the majority being residential. CBC News

Broadcast media / Médias télédiffusés

CBC News reports on insurance compensation issues faced by Fort McMurray residents. Rough Transcript

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Why the former CSIS director says the Liberals shouldn't touch Bill C-51
The former director of Canada's Security Intelligence Service says Bill C-51 should remain untouched. He does, however, support the government's plan to re-examine the controversial piece of anti-terror legislation. "I would leave it as it is, but as a Canadian, I'm glad the government's carrying through on its promise to review things," Richard Fadden told the West Block's Tom Clark this weekend (…) Last week, the Liberals formally announced a review of the law as part of an overall consultation on national security. Fadden said he is aware that many Canadians have concerns about parts of the law that allow agencies and government bodies to share information. Privacy is an important consideration, he acknowledged, but it must be balanced with security. Global News

Broadcast media / Médias télédiffusés

CBC News' Sunday Scrum held a panel discussion on this week's launch of the public consultation on national security. Some criticism was raised around the complexity of consultation questions. Rough Transcript

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Oliver Stone on Canadian surveillance and 'Snowden"s timing
Canadians who take in the new film "Snowden," about National Security Agency whistleblower Edward Snowden, should know they're not immune to the online privacy issues raised in the drama, says director Oliver Stone. "Canadians are part of the Five Eyes," Stone noted in an interview at the Toronto International Film Festival, referring to the intelligence alliance comprised of Australia, Canada, New Zealand, the United Kingdom and the United States. "(They) trust each other to the degree that apparently they share quite a bit together. However, it's hard to believe that the U.S. gives everything away." "Snowden" made its world premiere at the Toronto film fest on Friday. Canadian Press (Ottawa Citizen)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Toronto's Pearson International Airport could break passenger record
A boom in summer travel is propelling Pearson International Airport in Toronto to record levels of passenger traffic, bolstering the airport's goal of becoming one of the world's elite international airports by 2020. About 9.6 million people travelled through the airport between Canada Day and Labour Day, putting Pearson on pace to break its 2015 record of 41 million passengers annually. The Greater Toronto Airports Authority (GTAA) envisions Pearson reaching the status of "mega-hub" by the end of the decade – an airport that handles at least 50 million passengers a year, with 20 million of those travelling to or from international destinations... In a submission made to the federal government last month, the GTAA said Pearson needs $2-million for new Canada Border Service Agency officers so that 90 per cent of passengers are screened in 20 minutes or less. Another $20-million is needed to reduce security wait times so that 95 per cent of passengers wait 10 minutes or less to go through the Canadian Air Transport Security Authority screening process, the GTAA submission said. Globe and Mail

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

CIA head warns of Russian hacking, says US must be on guard
IA Director John Brennan is warning that Russia has "exceptionally capable and sophisticated cybercapabilities" and that the United States must be on guard. Brennan was asked in a television interview Sunday whether Russia is trying to manipulate America's presidential election. Brennan didn't say, but he noted the FBI is investigating recent computer intrusions at the Democratic National Committee. He also cited Moscow's aggressive intelligence collection. Brennan said: "I think that we have to be very, very wary of what the Russians might be trying to do in terms of collecting information in a cyber-realm, as well as what they might want to do with it." Associated Press (Seattle Times, Yahoo! News, Global News)

LAW ENFORCEMENT / APPLICATION DE LA LOI

Creep Catchers: UBC law professor warns of vigilantism's dangers
A University of B.C. law professor has warned that stings conducted by vigilante groups to shame child predators could backfire with violent results. On Friday, Surrey RCMP announced that an officer had been taken into custody following a livestream of a sting by the vigilante group Creep Catchers. The unidentified officer was released from custody Saturday and is suspended from duty. Police said they are

continuing to work with Crown counsel with respect to criminal charges. Posing as minors, the Creep Catchers set up fake online-dating profiles to lure suspected predators to meeting spots. They then film the interaction and post footage online to shame the suspect. Similar stings were used in the controversial reality series To Catch A Predator and have been conducted by other groups in B.C. Benjamin Perrin, an associate professor at UBC's Peter A. Allard School of Law, said that while such stings uncovered the "really horrific behaviour" of Internet child luring, "the end doesn't justify the means." Perrin, an expert on human trafficking and child sexual exploitation, warns that the use of such tactics to solve serious crimes poses a series of problems, particularly the lack of legal safeguards that police must have in place during an investigation. Ottawa Citizen

RCMP looking for cause of explosion reported in Aldergrove
Startled families in Aldergrove are dealing with a bit of a mystery as they try to figure out the cause of what sounded like a loud explosion at 8 p.m. Langley RCMP tell NEWS 1130 ground and air searches as well as interviews in the neighbourhood have yet to pinpoint a cause. At this time there have been no reports of anyone hurt although some parents say their kids were frightened out of bed and had to be calmed down. Some people are comparing the noise and vibration to being near a large fireworks show. News 1130

Walk for Valour aims to raise funds for service personnel support centre
Recovery is often a one-step-at-a-time process. This weekend, Edmontonians are being asked to take a few of those steps for someone else. The third annual Walk for Valour is set to raise money to help military members, veterans and RCMP have a place to stay while they deal with medical treatments. "We call it hope away from home," said Dennis Erker, chairman of Valour Place's board of directors. "At Valour Place you have people with similar situations hurting too. So the home is designed to encourage interaction between our guests. Everyone has a reason for staying there." Edmonton Journal

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

NIL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Canada's most dangerous cities 2016: How safe is your city?
For the first time in 15 years, crime has risen in Canada. A look at the 2015 data from Statistics Canada reveals the jump is driven significantly by increased violations in Western Canada. Case in point: For the second year in a row, Grande Prairie, Alta., was the worst among Canada's 100 largest cities and police districts in all three major crime categories: overall, violent and non-violent. In addition, it tops the list of total drug crimes. (Methodology at the end). While the focus is on this small Albertan city, let's not forget about the unlawful acts committed in other cities and communities. Does Ottawa reveal itself on any of the top 10 lists? (No.) Where are you most likely to have your identity stolen? (Longueuil, Que.) In Ontario, is your car safer in Barrie or Brantford? (Barrie, by a lot.) The tools below allow you to compare illicit activities in the top 100 largest cities and police districts in Canada. How does your hometown fare compared to such crime heavyweights as Grande Prairie, Prince George and Victoria? Maclean's

Conference aims to stop human trafficking between Manitoba, North Dakota
A conference in Winnipeg aims to establish a protocol between Manitoba and North Dakota to help end cross-border human trafficking. Organizers say thousands of Canadian teens are lured into empty hotel rooms every year and end up being moved around circuits across Canada and the United States. Barb Gosse, CEO of the Canadian Centre to End Human Trafficking, says the goal of the conference's participants is to set up a collaborative and responsive system of dealing with that. She says that will include training border control officers to be able to spot potential cases of human trafficking. Gosse

hopes the event will be the first of many across Canada and in the United States. Canadian Press (Metro News)

'Hide everything': Report finds silence prevails in N.W.T. sexual assaults
"Elders have worked to keep sexual assaults secret. It has always been 'Hush. Hush."' "The community attitude is to hide everything." Those are quotes from women and service providers who took part in a two-year study looking at the needs of women who have been sexually assaulted in the Northwest Territories. Lani Cooke, author of the new report Hush Hush No More, was commissioned by the YWCA to work on the project. She spoke with 10 women from five N.W.T. communities who have been sexually assaulted (...) Of the 10 women interviewed, only one had reported her sexual assault to RCMP (...) Cooke's report offers nine recommendations, which she points out all came from the people involved in the study. They include a dedicated 24/7 toll free N.W.T. Rape Crisis Line, more training for service providers, better collaboration among services, and a territory-wide sexual violence awareness campaign. CBC News

Do more to stop online predators
With online predators just a few mouse-clicks away, young people can be victimized with tragic ease, even from the far side of the world. That's why it's essential to have strong protections in place. And why it's so troubling to find "serious gaps" in existing efforts to shield kids from cyber-exploitation. "Much more needs to be done" to keep vulnerable children safe, according to a consultant's study prepared for the federal government in March and revealed by The Canadian Press. That's a sobering finding, especially in light of an earlier memo indicating that police have insufficient resources to keep pace with this threat. Commissioned by Public Safety Canada, and obtained through the Access to Information Act, the newly released study is meant to guide federal funds to where they're most needed to combat online sexual exploitation. Existing resources are "are being strained," according to the study, with CP's Jim Bronskill reporting that kids in parts of Canada, especially in rural areas and the north, at risk of being underserved by counselling, prevention programs, victim treatment and other initiatives. This is especially worrisome given evidence that rural and other isolated kids are particularly vulnerable. The heart-rending fate of Port Coquitlam teenager Amanda Todd is stark evidence of what can happen when kids fall prey to computer predators. Manipulated by an online tormentor, she committed suicide at the age of 15 after years of cyberbullying, including the repeated circulation of nude photos. No child, or parent, deserves to go through that. Hamilton Spectator

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Two of Canada's big five banks backing away from marijuana industry
Scotiabank and the Royal Bank of Canada say they aren't providing accounts to companies associated with the marijuana industry, leaving some business owners scrambling to find alternate arrangements. After a decade-long relationship with Scotiabank (TSX:BNS), Hemp Country owner Nathan MacLellan says he received a letter from the bank late last month stating his account was being cancelled. The store in Woodstock, Ont., sells marijuana-related items such as pipes and bongs but no actual cannabis, MacLellan says. "It's kind of insulting really, especially when legalization is right on the horizon," he says. Canadian Press (Yahoo! News); Presse canadienne (Radio-Canada)

PUBLIC SERVICE / FONCTION PUBLIQUE

Ex-CIDA staffers need 10 years to adapt to department merger: report
Former employees of now defunct Canadian International Development Agency might need as long as a decade to get used to the idea they have been subsumed by the larger foreign ministry. That is a key finding of an internal government report on the 2013 decision by the former Conservative government to merge CIDA with the larger Department of Foreign Affairs and International Trade, as it was then known. Consultant Alain Jolicoeur wrote in a report delivered to the government last year that it could take five to 10 years for CIDA employees to accept the "cultural change" associated with the merger. The Canadian Press obtained a copy of Jolicoeur's report under access to information. Canadian Press (CTV News)

OTHER / AUTRES

WestJet passengers arriving Sunday evening after emergency landing in Iceland
Westjet passengers forced to spend the night in Iceland after an emergency landing will arrive back in Alberta on Sunday evening. On Saturday morning, a WestJet flight bound from London Gatwick to Edmonton was forced to make an unscheduled stop in Reykjavík. WS27 was diverted to Keflavík International Airport after crews detected a potential mechanical issue. Passengers were put up in hotels for the night and the plane was grounded for maintenance. Global News

INTERNATIONAL

Fifteen years after 9/11, the jihadist threat looms larger than ever across the globe
Nine days after the Sept. 11, 2001, attacks, President George W. Bush stood before Congress to outline a two-pronged response to history's deadliest terrorist act: dramatic improvements in security at home and an all-out assault against what he called a "fringe form of Islamic extremism" at war with the West. Fifteen years later, the first goal arguably has been met, as Americans by almost every measure are safer today from another 9/11-scale attack than in 2001. Yet the struggle to defeat the global network of violent, rabidly anti-Western jihadist groups has recorded fewer successes. Indeed, the problem appears to have grown bigger (...) There is little to show for more than a decade's worth of U.S.-sponsored programs aimed at countering extremist messages, terrorism experts say, and U.S. officials have struggled to block the jihadists' use of social media or disrupt international funding and support for extreme interpretations of Islam (...) despite gains in safeguarding the U.S. homeland, efforts to counter the root causes of violent jihad largely have fallen flat. The National Counterterrorism Center (NCTC), which was created by the post-9/11 wave of intelligence reforms, mounted a series of efforts to map the radicalization paths of Islamist militants. But there are divided opinions on what came of that work. Michael Leiter, who led the NCTC from 2007 to 2011, said the research produced important insights that have helped guide U.S. counterterrorism policy, but never led to the discovery of sequences or patterns that would reliably signal an individual's intent to carry out an attack. Washington Post

Homeland Security secretary: 'Lone wolf' threat different than 9/11
Homeland Security Secretary Jeh Johnson said Sunday the threat of terrorist-inspired "lone wolf" attacks is "the thing that keeps me up at night" 15 years after the September 11, 2001, terrorist attacks. "It's a new environment. It's a new phenomenon," Johnson told CNN's Jake Tapper on "State of the Union," when Tapper asked if the United States is safer now than it was then. "So the answer to your question is really a mixed one," Johnson said. "We're better now at detecting the 9/11-style attacks, but it's more challenging with this new environment that we're in." Johnson said he could see the towers collapse from his Manhattan office window on 9/11, when he was an attorney in private practice. He said the biggest difference in terms of security threats since then is that terror groups can now "literally into our homeland through the internet with social media to recruit and inspire people here." CNN

On 15th anniversary of 9-11, 'the grief never goes away'
The U.S. marked the 15th anniversary of 9-11 on Sunday, with victims' relatives reading their names and reflecting on a loss that still felt as immediate to them as it was indelible for the nation... The 15th anniversary arrives in a country caught up in the campaign, keenly focused on political, economic and social fissures and still fighting terrorism. But for those who lost relatives, the fraught passage of 15 years

feels "like 15 seconds," said Dorothy Esposito, who lost her son, Frankie. Over 1,000 victims' family members, survivors and dignitaries at ground zero under an overcast sky. "It doesn't get easier. The grief never goes away. You don't move forward -- it always stays with you," Tom Acquaviva, who lost his son, Paul Acquaviva. James Johnson was there for the first time since he last worked on the rescue and recovery efforts in early 2002, when he was a New York City police officer. "I've got mixed emotions, but I'm still kind of numb," said Johnson, now a police chief in Forest City, Pennsylvania. "I think everyone needs closure, and this is my time to have closure." Nearly 3,000 people died when hijacked planes slammed into the World Trade Center, the Pentagon and a field near Shanksville on Sept. 11, 2001. It was the deadliest terror attack on American soil. Homeland Security Secretary Jeh Johnson said on Sunday news shows that the United States is safer now than it was in 2001 against another 9-11-style attack but continues to face the challenge of potential attacks by solo and homegrown violent extremists. Associated Press (Whig-Standard)

15-year-old boy arrested in France for planning 'imminent' Paris attack
A 15-year-old boy has been arrested in Paris suspected of preparing imminent "violent action", two judicial sources said, the second alleged plot with links to Islamic State discovered in France this week. Last Sunday, a car loaded with gas cylinders was found near Notre Dame cathedral and jerry cans of diesel, leading to the discovery of a plot to attack a Paris railway station under the direction of Islamic State. Seven people, including four women, were arrested. The boy had been under house arrest since France declared a state emergency after Nov. 13 attacks in Paris in which Islamic State militants killed 130 people, two sources said on condition of anonymity. They did not say why he was under house arrest. Reuters (Global News)

Magnitude-5.3 quake hits Macedonia; at least 30 injured
An earthquake with a preliminary magnitude of 5.3 struck on the outskirts of Macedonia's capital on Sunday, injuring at least 30 people and causing minor damage to buildings, authorities said. The quake occurred just after 3 p.m. (1300 GMT; 9 a.m. EDT), seismologist Dragana Cernih from the national seismological observatory told The Associated Press. She said she received reports of cracks in the walls of buildings or collapsed chimneys, as well as damage to roofs in villages around Skopje. At least 30 people were slightly injured leaving their homes in panic, crisis management department spokeswoman Nadica V'ckova told The Associated Press late Sunday. Associated Press (Thunder Bay Chronicle-Journal)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

CBCCanada
Fort McMurray residents claim 'nightmare' dealing with insurance http://ift.tt/2cnDr6n

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Global News
Former CSIS director: Don't touch Bill C-51 #cdnpoli

The West Block
Welcome back. Former CSIS director Richard Fadden is here to talk Bill C-51 and whether spies should still be able to act outside the law.

The West Block
Should Cdn spies still be allowed to operate outside the law. Former CSIS director Richard Fadden talks to @TheWestBlock this a.m. 11ET/10PT

Canadian PM
"I encourage Canadians to remember the tremendous outpouring of goodwill shown on 9/11" –PM Trudeau

Canadian PM
"On this solemn day, we join with the families and friends of the victims to remember and honour those who fell"

CanadianPM
Today, we mark the 15th anniversary of the terrorist attacks in the U.S. that killed nearly 3,000 innocent victims.

iciottgat
Les pompiers canadiens se souviennent de leurs collègues morts le 11 septembre http://bit.ly/2cc1Rlo

CKNW
9/11 victims remembered in both B.C. and across Canada http://bit.ly/2cw6uGz

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

TheTyee
Privacy Advocates Fear Bill C-51 Consultations Will Be Skewed http://thetyee.ca/News/2016/09/09/Bill-C-51-Consultations-Skewed/?utm_source=twitter&utm_medium=social&utm_content=091116-1&utm_campaign=editorial-0916 … #cdnpoli

canadaCJFE
Thousands signed petition 308 and helped put #C51 back on the agenda. Thank you all!
http://cjfe.org/stoptheclock_C51 …

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Ann Cavoukian
Time to get serious about proactively embedding #security and #privacy into #IoT, especially #IIoT.

Global Montreal
CIA Director John Brennan warns of Russian hacking

LAW ENFORCEMENT / APPLICATION DE LA LOI

The Georgia Straight
Creep Catchers, an arrested Mountie, the premier's refusal to look at policing problems http://ow.ly/2xkc30461Yy

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Maclean's Magazine
We charted crime rates in Canada's 100 biggest cities. See how your city ranks:

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Yahoo Canada News
Two of Canada's big five banks backing away from marijuana industry http://yhoo.it/2cbKO2X

INTERNATIONAL

cnni
Homeland Security Secretary Jeh Johnson says the nation is safer from 9/11 style attacks http://cnn.it/2cOn7th

RT_com

'We are a target': French PM warns 15,000 people on police radar, 1,400 probed amid foiled terror plots https://t.co/imaoil0BMn

globalnews
15-year-old boy arrested in France for planning 'imminent' Paris attack https://t.co/HO4a9lva5w

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

Today's News / Actualités
September 14, 2016 / le 14 septembre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Expulsé du pays après avoir purgé sa peine

Une pétition circule toujours et une centaine de personnes sont attendues pour manifester devant les bureaux montréalais de l'Agence des services frontaliers du Canada (ASFC) ce jeudi 15 septembre après que Michele Torre eut reçu son avis d'expulsion assorti d'un billet d'avion pour l'Italie. Installé dans Vimont depuis 30 ans, résident permanent au Canada depuis 1967, le père de 3 enfants, tous mariés et parents, devra quitter son foyer ce vendredi 16 septembre à moins que les ministres John McCallum

(Immigration) et **Ralph Goodale (Sécurité publique)**, ou le premier ministre Justin Trudeau, ne soient cléments à son endroit. (…) Condamné pour trafic de cocaïne en 1996, une accusation à laquelle il avait plaidé coupable aux côtés du chef mafieux Frank Cotroni sénior et le fils de celui-ci, sans oublier Giovanni Marra, propriétaire du café qu'il lui avait acheté deux ans auparavant, Michele Torre a purgé une peine de huit ans et neuf mois. «Après ma sentence, je n'ai eu que des bons rapports de mon agent de libération conditionnelle André Harvey, de dire M. Torre. On m'avait même dit que je n'étais pas considéré comme une personne à risque. Pourtant, ils ne trouvent aucun des documents qui plaidaient tous en ma faveur.» Du côté du gouvernement fédéral, «la décision de renvoyer une personne du Canada n'est pas prise à la légère, répond brièvement Dominique McNeely, conseiller en communications de l'Agence des services frontaliers du Canada. L'ASFC accorde une très grande priorité aux cas de renvoi portant sur des questions liées à la sécurité nationale, criminalité organisée, aux crimes contre l'humanité et à la criminalité». «Selon la Loi sur l'immigration et la protection des réfugiés, les mesures de renvoi doivent être exécutées le plus tôt possible, ajoute-t-il. L'ASFC est déterminée à le faire.» Notons qu'en 2006, Michele Torre avait été arrêté dans le cadre de l'opération Colisée qui visait la mafia italienne. Cependant, il n'avait été reconnu coupable d'aucune infraction. Courrier Laval

MP Zimmer concerned by minister's decision on AR-15

Local Conservative MP Bob Zimmer says he's concerned with **Canada's Public Safety Minister's** decision to give Mounties the authority to classify weapons. Zimmer was responding after **Minister Ralph Goodale** said the government had no plans to change the classification of the Armalite AR-15 rifle. "Before, when we were in government we had a group of … firearms experts, Canadian sport shooters, RCMP, different groups that were represented, advising us about firearms issues," Zimmer said. "When only one of those user groups is giving advice and making decisions on firearms, you're going to get only one perspective, and that's concerning." In May, Zimmer sponsored and presented an e-petition in the House of Commons to reclassify the rifle, popular with sports shooters, from its restricted status. The petition garnered 25,000 signatures nationwide. (…) Zimmer and gun advocates, say the rifle is popular for sports and hunting, and is only classified as restricted due to its design. But in his response, **Goodale** said ***"the AR-15 is restricted because of its lineage to the military-issued M-16 assault rifle." "The Government is committed to putting decision-making authority about weapons classification back into the hands of police, not politicians,"*** **Goodale** wrote in his decision earlier this month. ***"The Royal Canadian Mounted Police is responsible for the technical determination of the classification of firearms in accordance with the criteria stipulated by Parliament in the Criminal Code."*** Alaska Highway News

Pot question bans some Canadians from U.S. for life

In case you missed this story percolating to our north on CBC News, Canadians are being banned from entering the U.S. if they admit to customs agents that they've recreationally used marijuana. **Canada's Public Safety Minister Ralph Goodale** called the lifetime bans ***"ludicrous,"*** especially in light of ***"certain ironies about the current American position."*** Adults, including foreigners, are allowed to consume pot in Washington state (as well as Colorado, Alaska, Oregon and Washington, D.C.). But the U.S. federal government still considers pot illegal. Customs agents may ask Canadians coming into the Washington, such as Matthew Harvey, if they've consumed pot in the past. Harvey, on his way from Vancouver, B.C. to a concert in Seattle, answered affirmatively. He was hit with a lifetime ban because the feds treat such an admission as if it were a criminal conviction. Canadians can apply for a waiver to enter the U.S. but it costs $585 and has to be renewed. With Canada planning to legalize pot, and research showing that 44 percent of the country's residents have tried pot, there's a concern more and more Canadians could face bans for answering a seemingly harmless question. While every country has the right to determine who can cross their border, **Goodale** said he would urge U.S. officials to use common sense ***"instead of the rather ridiculous situation that has emerged."*** Seattle Times

National security consultations must make good on Liberal promise to restore civil liberties, says rights group

An opinion piece states, "Canadian Journalists for Free Expression (CJFE) is encouraged by the long-awaited announcement by the **Minister of Public Safety** and Justice of a consultation on reforming Canada's national security framework. "This consultation is an important first step in building a national security system that truly protects our rights and undoes the dangerous failures of previous legislation,"

says Tom Henheffer, CJFE's Executive Director. "Our current framework undermines free expression rights, civil liberties and the rule of law. The government must listen to the voices of Canadians calling for a real, substantive change to our national security regime. We can and must do better." The review process comes one year after the Liberal Party released its election platform that included a pledge to "repeal the problematic elements of Bill C-51, and introduce new legislation that better balances our collective security with our rights and freedoms." Since the day the Anti-terrorism Act, 2015 - or Bill C-51 - was announced, CJFE has worked to stop, and then overturn, this dangerous, reckless and ineffective legislation. In July 2015, CJFE and the Canadian Civil Liberties Association (CCLA) launched a Charter challenge on the grounds that five sections of Bill C-51 unjustifiably violate the Canadian Charter of Rights and Freedoms." CJFE (2016-09-12)

TOP STORIES / MANCHETTES

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fort McMurray will review wildfire rebuild fees after complaints from homeowners
Facing a swell of complaints, councillors with the Regional Municipality of Wood Buffalo have agreed to review the fee structure for rebuilding homes leveled by May's wildfire. On Tuesday, municipal councillors asked administrators to re-evaluate the fees associated with inspections, demolition, and redevelopment of damaged properties. The motion, proposed by Counc. Sheldon Germain and co-authored by councillors Keith McGrath and Allan Vinni, passed unanimously after a rigorous discussion about the financial challenges facing homeowners. CBC News

Lightning the 'deadliest summer weather threat' in Canada
It's been a tumultuous year for thunderstorms. Big storms have caused damage across the country this season. Just last weekend, much of southern Ontario was under a severe thunderstorm warning. In July, 20,000 Nova Scotia Power customers were left in the dark as lightning strikes fried transformers. That same month, intense thunderstorms swept across the Prairies, causing $48 million in insured damage. "It's been a very active year for a summer severe weather point-of-view across all of the Prairies, and specifically in southern Alberta," said Environment Canada meteorologist Brian Proctor. Alberta is always an active area, and on average gets 400,000 lightning strikes over the summer. Last year there was 358,753 lightning strikes in the province, but this year that number was up to 576,721 as of Sept. 9. The number of severe thunderstorm warnings and watches more than doubled in southern Alberta this summer, and summer storms felt like a daily occurrence in Calgary. The public doesn't always take weather alerts seriously, but Proctor says they should. CBC News

Cloudy with a chance of icebergs
From flying planes over the Arctic's vast surface to crunching numbers with cutting-edge technology, a small but growing group of young engineers are keeping ships safe from the hazards of ice while working at the forefront of computer science. In Canada, ice forecasting dates back to the Cold War, when the government needed safe routes to install missile radar in the Far North. It has since grown with recent developments in computing capacity and weather modelling-not to mention interest in tourism, shipping, and oil and gas exploration in the Northwest Passage. With changing climate and an estimated 90 billion barrels of oil buried under the Arctic, ice forecasting promises hot salaries and rapid career advancement (…) The technology could prevent the fate of the Franklin expedition (icebound) or the Titanic (iceberg collision) befalling the crew and passengers of a much more modern ship, such as the 1,070-passenger cruise liner Crystal Serenity, the largest vessel ever to navigate the Northwest Passage. It just completed its maiden voyage. On rare occasions, engineers plant acoustic sensors on the Arctic seabed to calculate ice thickness, or fly in planes outfitted with devices to measure ice drifts. But ice forecasting isn't solely for fans of cold climates; most of the work involves processing statistics from satellites, weather stations and historical databases. Maclean's

Massive submarine war games launched in Nova Scotia
The largest anti-submarine warfare exercise hosted in Canadian waters in two decades is now underway off Nova Scotia's coast. The exercise is called Cutlass Fury. Eleven warships and more than 24 aircraft are simulating military activities approximately 160 kilometres southeast of Halifax. "As this exercise progresses, it becomes more complex," said Petty Officer Shawn Swinimer, the underwater warfare director onboard HMCS Fredericton (…) Swinimer said the exercises are starting with simple search and recognizance. As the exercise progresses, it will escalate to full war games with simulated weapons launches. CBC News (Yahoo! News)

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

National security consultations must make good on Liberal promise to restore civil liberties, says rights group
An opinion piece states, "Canadian Journalists for Free Expression (CJFE) is encouraged by the long-awaited announcement by the **Minister of Public Safety** and Justice of a consultation on reforming Canada's national security framework. "This consultation is an important first step in building a national security system that truly protects our rights and undoes the dangerous failures of previous legislation," says Tom Henheffer, CJFE's Executive Director. "Our current framework undermines free expression rights, civil liberties and the rule of law. The government must listen to the voices of Canadians calling for a real, substantive change to our national security regime. We can and must do better." The review process comes one year after the Liberal Party released its election platform that included a pledge to "repeal the problematic elements of Bill C-51, and introduce new legislation that better balances our collective security with our rights and freedoms." Since the day the Anti-terrorism Act, 2015 - or Bill C-51 - was announced, CJFE has worked to stop, and then overturn, this dangerous, reckless and ineffective legislation. In July 2015, CJFE and the Canadian Civil Liberties Association (CCLA) launched a Charter challenge on the grounds that five sections of Bill C-51 unjustifiably violate the Canadian Charter of Rights and Freedoms." CJFE (2016-09-12)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Un adolescent de Brandon plaide coupable d'avoir soutenu le groupe armé État islamique
Un adolescent de Brandon, au Manitoba, qui a été arrêté l'an dernier pour avoir utilisé les médias sociaux afin d'exprimer son appui au groupe armé État islamique, recevra sa peine le mois prochain pour des accusations de terrorisme. Le jeune homme, qui avait 16 ans lorsqu'il a été arrêté dans la ville de l'ouest du Manitoba en novembre dernier, a plaidé coupable lundi à des accusations d'avoir conseillé la perpétration d'un acte criminel au profit ou sous la direction d'un groupe terroriste ou en association avec lui. L'adolescent, qui ne peut être identifié à cause de son âge, est derrière les barreaux depuis son arrestation et y demeurera jusqu'à ce que sa peine soit connue, affirme le procureur de la Couronne Ian Mahon Aucun détail sur ce qui a mené à l'arrestation du jeune homme n'a été révélé en cour lundi. La Couronne et la défense ont convenu de le juger comme un adolescent puisqu'il a reconnu sa culpabilité. S'il avait été jugé comme un adulte, la peine maximale pour son crime aurait été l'emprisonnement à vie. Radio-Canada

Broadcast media / Médias télédiffusés :

A vast majority of real estate firms are not complying with anti-money laundering and antiterrorist rules set out to protect Canadians. FINTRAC finding that 60% of real estate companies are not following the rules. (CBC News, 8:30ET)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Canada customs: Carried firearms must be declared
The Canada Border Services Agency wants U.S. travelers to be informed about Canadian firearms laws. On Aug. 23 the agency launched a firearms awareness campaign in Western Canada. Most undeclared firearms seized by the CBSA at land border ports of entry in British Columbia and Alberta are personal firearms belonging to travelers arriving from the United States. From Jan. 1 to July 31, 2016, the CBSA Pacific Region saw a 116 percent increase in the number of firearms seized in the Pacific Highway District, compared to the same period last year. The CBSA Prairie Region has seen a 10 percent increase in the number of firearms seized in southern Alberta. Canadian firearms laws are clear. American travelers who do not declare firearms upon arrival can face seizure, criminal prosecution and deportation from Canada. All firearms must be declared. “Firearms and weapons are high-risk commodities and their interdiction is a CBSA enforcement priority. The CBSA is Canada’s second largest federal law enforcement agency and our officers are Canada’s first line of defence in protecting Canada from illegal weapons and other contraband,” said Roslyn H. MacVicar, Pacific Region director general. Lynden Tribune

Côte d'Ivoire: Canada, un ex rebelle soupçonné de crime de guerre expulsé vers à Abidjan
Abou Fofana membre de l’ex rébellion Search rébellion est soupçonné de crime de guerre par les autorités Canadiennes lors de la crise survenue en Côte d’Ivoire dans la nuit du 18 au 19 septembre 2002, comme révélé par des médias canadiens. Selon le nouvelliste, qui a relayé mardi l’information sur son site, l’ex élément des forces nouvelles a été extradé lundi soir vers la Côte d’Ivoire. Ses proches, qui ont espéré jusqu'à la dernière seconde un revirement de situation, ont dû se résigner au pire scénario qu'ils avaient envisagé. «C'était plein d'émotions. Je n'ai pas amené les enfants car c'était trop difficile. C'était dans la même salle que d'habitude. Il n'y a pas eu d'extra. Je n'ai pas pu l'accompagner à l'aéroport», a-t-elle confié d'une voix tremblotante, a expliqué sa conjointe Geneviève Trottier, comme rapporté par ledit media. (...) Au moment où nous publions, nous ne pouvons confirmer si Abou Fofana Search Abou Fofana a réellement foulé lundi le sol ivoirien suite à son expulsion annoncée vers son pays d’origine. Koaci

Canada faces big questions about the future of immigration
Canada's immigration policy is at a crossroads. As other countries turn away refugees or have divisive debates on limiting newcomers, Canadians will welcome as many as 300,000 immigrants to the country this year, up from a cap of 285,000 in 2015. Immigration Minister John McCallum, who is fresh off of a Canada-wide summer consultation on immigration policy, is looking to boost that number even higher next year. "We are in need of new blood because Canadians aren't having enough babies," he said in Calgary in August. "The labour force growth depends very much on the entrance of immigrants." At the same time, the Liberal government is looking to overhaul many parts of the immigration system, from the controversial Temporary Foreign Worker Program to how skilled immigrants get into the country. A key focus is "breaking down the barriers so we can have the ability to seek out the best and brightest," said McCallum over the summer in Ottawa. The government's current review, which is expected to lead to policy changes within months, comes on the heels of dramatic changes by the former Harper government to almost every aspect of immigration policy. A year-long Postmedia investigation shows the consequences of current policies range from a spurt in the number of temporary foreign workers overstaying their four-year limit - and an ensuing growth in the underground economy - to constraints on how wealthy immigrants interested in investing in Canadian businesses can settle in the country. Calgary Herald

Desperate Canadian businesses seek changes to temporary foreign worker program
The workers move quickly at Sunterra Farm's pork processing plant in the central Alberta town of Trochu. Dressed in white overcoats, blue aprons, rubber boots and hard hats, dozens of butchers and meat packers, mostly from Mexico and the Philippines, rapidly debone, sort and package cuts of pork into boxes destined for Japan. It's a promising export for Canada, but one struggling to expand its market abroad because the meat-packing industry doesn't have enough people to do the gruelling work. At Sunterra, there are only enough employees to handle basic primal cuts like loins, butts and shoulders. Secondary cuts that are delicacies abroad, including hearts, livers and feet, don't make it down the processing line. "We're throwing food away," laments Mark Chambers, senior production manager at Sunterra. For years, the agri-food company relied on temporary foreign workers to fill ongoing labour

shortages in facilities around Alberta. Most obtained permanent residence and stayed. But the flow of migrant workers has slowed after a series of restrictions enacted between 2011 and 2014 on how employers can use the Temporary Foreign Worker Program. Margie Badao moves boxes of meat along the packing line at Sunterra Meats in Trochu, Alta. Badao originally came to the company from the Philippines as a temporary foreign worker and now has permanent status. (Ted Rhodes/Postmedia) Meat packers aren't the only ones hurting. From the ski slopes of Whistler in the West to the shores of the Bay of Fundy in the East, Canadian businesses say they are desperately looking for employees and blame restrictions on the temporary foreign workers for costing the national economy jobs, productivity and revenue. Calgary Herald

Fort McMurray rebuild gets more expensive

Fire-ravaged Fort McMurray is one of several Canadian cities and towns being impacted by skyrocketing drywall costs. Builders and suppliers blame new anti-dumping tariffs on US gypsum board products for the price spike over the past week. Canada Border Services Agency slapped tariffs up to 276% on US products imported to Canada to offset dumping following complaints filed in April. The industry says the surprise ruling could disrupt the supply of drywall and risks bankrupting contractors working under fixed-price contracts. There is some production in Western Canada, but an industry official says they can only meet 40% to 60% of the needed supply, so extra product must be imported from the US. The CBSA decision is under review for the next three months, but the import duty will remain in effect until a final decision is made. iNews 880

Trucker fined for guns found at Osoyoos border crossing

A South Carolina trucker is paying a fine and is unable to return to Canada after prohibited and restricted weapons were found in his truck after lying to border agents in Osoyoos. Marion Furman Taylor Jr., 55, was sentenced to pay a fine of $7,500 after pleading guilty to charges of making a false statement at the border, possession of a loaded, prohibited firearm and possession unauthorized overcapacity magazines in Penticton Provincial Court on Sept. 12.Taylor Jr., a U.S. citizen with no prior record in Canada or the U.S., was hauling a load of canoes and kayaks into Canada with his business partner for a U.S. company, Landstar Rover Inc. on April 3. After an initial inspection by a Canada Border Services Agency (CBSA) employee, the tractor-trailer was given a secondary inspection after Taylor Jr. told border security there were no firearms to declare in the vehicle. In a duffel bag located under the bottom bunk of the sleeper cab border agents found a loaded Beretta PX Storm pistol, three loaded, overcapacity magazines, a box of 50 rounds of .38 ammunition and a loaded .38 special Smith and Wesson revolver. Also located in the truck were two canisters of mace, a canister of bear spray as well as a switchblade, which are prohibited items in Canada. Taylor Jr. admitted he was the owner of the weapons to border agents after confronted and he was arrested and eventually released — paying $7,000 for the release of his truck. Penticton Western News

Cross-border companies join forces

Eschewing their patchwork approach of the past, leading cross-border trade organizations in the US and Canada have organized a united front in their efforts to reach the hearts and minds of governments and legislators. The inaugural 2016 US-Canada SAGE Summit, which took place at Ohio State University's Columbus campus in late June, featured delegates representing 60 leading cross-border business organizations as well as policy and political leaders from both countries. SAGE is an acronym for "strategies, advocacy, gateways, engagement," the organization's action pillars. "This summit marked the first time that these organizations came together under one roof to chart a course for the future of the Canada-US relationship," says Columbus-based Daniel Ujczo, a summit co-founder and an international trade lawyer at Dickinson Wright, a firm with offices in Canada and the US whose practice includes a significant focus on cross-border law and trade. "With a new government in power in Canada and American elections on the horizon, we needed to come up with a new way to manage this relationship." The timing was right. "The cross-border scene has been racking up a lot of losses, including the rejection of the Keystone Pipeline, the dispute over country-of-origin labelling, and the fight over who would pay for the Gordie Howe Memorial Bridge," he says. "We definitely needed a new approach." The new Canadian government, it turns out, was a key catalyst for SAGE. Lexpert

Why it's so important for Trudeau to fix the Canada-U.S. border

An opinion piece by Colin Robertson of the Canadian Global Affairs Institute states, “Call it the 9/11 effect. Fifteen years on we are still paying the price of that tragic day. It changed how we trade. Tourism to Canada by Americans has never recovered. It also altered, probably permanently, the easy trust that characterized what was once the "longest undefended border." The trade effect with the United States is the most evident. A smart and secure border must be the Trudeau government's priority with the next administration. Notwithstanding a series of initiatives - Smart Border, Security and Prosperity, and now Beyond the Border, the border has thickened. While rail shipments have increased, especially for oil in the absence of new pipelines, trucks remain the primary mode of cross-border transport although truck traffic is down almost 20 per cent since 9/11. A study concluded that the premium paid to move goods across the border rose, from 0.3 per cent of the value of goods shipped prior to 9/11, to about 0.6 per cent after 9/11 because of inspection and a surge in paperwork required for passage. Verification programs for "secured" carriers and goods and regulatory co-operation have mitigated border delays. But we are still awaiting the promised single electronic portal that will satisfy the information requirements of governments and their agencies.” Globe and Mail (2016-09-13)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Volkswagen sets up cyber security firm with ex-Israeli spy chief
Volkswagen is forming a company with the former head of Israel's Shin Bet intelligence agency to develop cyber security systems for Internet-connected cars and self-driving vehicles, the partners said in a statement on Wednesday (…)"To enable us to tackle the enormous challenges of the next decade, we need to expand our know-how in cyber security in order to systematically advance vehicle cyber security for our customers," said Volkmar Tanneberger, Head of Electrical and Electronic Development at Volkswagen. Reuters; PC World

GCHQ creating national firewall to stop cyber criminals
The UK’s intelligence agency GCHQ is stepping up the fight against cyber criminals with plans to launch a national firewall to block malicious websites and emails. GCHQ will work with internet service providers such as BT, Talk Talk and Virgin Media to filter websites set up by scammers that download malware onto victims' computers. For the firewall to work, the surveillance agency wants to create a national domain name system (DNS) that can be used to block suspicious sites. Telegraph UK; IT Pro UK; Tech Radar

LAW ENFORCEMENT / APPLICATION DE LA LOI

Fort Simpson mayor says RCMP used excessive force in detaining her intoxicated brother
The mayor of Fort Simpson, N.W.T., has filed a complaint against the RCMP, alleging an officer was too aggressive when dealing with her intoxicated brother. "It was humiliating. To me, I would have been humiliated just by how he was treated," said Darlene Sibbeston. She didn't see the incident herself, but arrived minutes later to find her brother Darrell Sibbeston pinned to the ground by an RCMP officer, with a knee in his back. "Part of his pants were, like they were falling down," she said. "He was lying on his right side. His face was down and there was just blood covering his forehead, his eyes and around his nose. Around his head was a pool of blood." Darlene Sibbeston is one of two community members who have filed complaints with the Civilian Review and Complaints Commission for the RCMP about the incident last Friday. (…) In an email response to CBC, RCMP say senior management are "aware" of the incident and an internal review has been started. A media spokesperson said "RCMP have not received any formal complaints from any members of the community." It could take a few days before they are notified of any formal complaints. In the meantime, Darlene Sibbeston, and other local Indigenous leaders plan to meet with RCMP members from Fort Simpson and Yellowknife later today to talk about the incident. CBC News

Déploiement des Casques bleus canadiens: le Mali largement favori
Tout indique que le réengagement du Canada dans les opérations de paix de l'ONU se fera au Mali, en Afrique. Le gouvernement Trudeau annoncera d'ici quelques semaines à quel endroit seront déployés les

Casques bleus canadiens, et plusieurs sources ont mentionné à L'actualité que la liste des destinations est maintenant très courte. Il ne reste que quatre possibilités: le Mali, le Soudan du Sud, la République démocratique du Congo et la République centrafricaine. Et de ces options, le Mali est largement en tête. Au début octobre, le chef d'État-major de la Défense, le général Jonathan Vance, remettra au ministre de la Défense, Harit Sajjan, son analyse militaire sur la situation dans ces quatre pays et le rôle que le Canada peut y jouer. Le ministre Sajjan devra ensuite discuter des possibilités avec le ministre des Affaires étrangères, Stéphane Dion, et la ministre du Développement international et de la Francophonie, Marie-Claude Bibeau. Le cabinet Trudeau devrait trancher d'ici la fin du mois d'octobre. (…) Le gouvernement Trudeau a envoyé une équipe de reconnaissance au Mali au début du mois de septembre, composée d'experts du ministère de la Défense, du ministère des Affaires étrangères et de la GRC, afin d'évaluer la situation sur place. L'ONU n'a pas demandé au Canada de fournir des fantassins qui seraient directement impliqués dans le conflit, dans le nord du pays. Elle souhaite qu'Ottawa fournisse des troupes spécialisées, notamment des ingénieurs de combat et des hélicoptères. Le Canada pourrait d'ailleurs déployer un peu moins que les 600 soldats annoncés à la fin du mois d'août. Le chiffre de 400 militaires est évoqué. «Les 600 soldats, c'est la capacité canadienne pour les missions de paix sur une année. Il n'est pas dit qu'ils seront tous déployés au même moment, au même endroit», mentionne d'ailleurs une source bien au fait des discussions au sein du gouvernement. L'actualité

RCMP officers tell their story of being exposed to fentanyl
Some B.C. RCMP officers are speaking out about the dangers of fentanyl exposure after nearly overdosing on the job. At least three B.C. officers are known to have had contact with the deadly drug while on duty. "They did an EKG [electrocardiogram] and my heart rate was elevated and blood pressure. They also did a urine test and all that and there was trace opiates," said Cst. Rob Dupis with Kamloops RCMP. "That was just from a 15 minute exposure in a vehicle." Global News

Williams Lake RCMP issue fentanyl warning to parents
A letter by Inspector Pelley states, "Dear Parents: Thank you for taking time to read this important notice. Being a parent is the most important job any of us will ever have. As some of you may be aware through media, friends or family, more than 433 people in the Province of British Columbia have died between January and July 2016 as a result of an overdose. According to the BC Coroner fentanyl was detected in approximately 62 per cent of those cases. The families of these people have been left devastated and their lives will never be the same. After examining several recent fentanyl-related calls for service, the Williams Lake RCMP is issuing a warning to parents about the dangers of fentanyl and other drug use. Fentanyl, new fentanyl equivalents, and W compounds are appearing in the illegal market. Williams Lake Tribune

RCMP searching for missing teen girl from Cowessess First Nation who may be in Regina
Broadview RCMP is asking for the public's help in locating a missing 16-year-old girl from the Cowessess First Nation. Norma Sheperd was last seen at a residence on the Cowessess First Nation on Sept. 9, and left the location with a man in a blue pickup truck. She was reported missing on Monday, and so far RCMP members have been unable to locate her. The RCMP said Sheperd may be in Regina, but that has not been confirmed. Leader-Post

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Accused in Kelowna fentanyl bust was former Hells Angels 'middleman'
A Kelowna man charged in connection with a massive fentanyl bust was a former 'middleman' for the Hells Angels, according to parole documents. Leslie John McCulloch was charged with possession for the purpose of trafficking this summer following a raid in which RCMP seized two industrial pill presses and hundreds of fake OxyContin and Percocet pills made out of fentanyl. According to parole documents obtained by the CBC, the 38-year-old was on parole from a four-and-a-half year sentence for possession for the purpose of trafficking cocaine at the time of the alleged offences. McCulloch is slated to appear in Kelowna provincial court on Wednesday. CBC News

Alberta appeals court hears of brutal death of Calgary girl killed by dad, stepmom

The Alberta Court of Appeal has reserved its decision on appeals in the convictions of a Calgary couple found to have killed the man's 6-year-old daughter, Meika Jordan. The Crown wants the appeal court to find Spencer Jordan and Marie Magoon guilty of first-degree murder instead of the original trial judge's finding of second-degree murder. Jordan and Magoon want to be acquitted or face new trials. Last September, the pair were sentenced to life in prison with no chance of parole for 17 years in the death of Meika, who was killed in 2011. Appeal prosecutor Jolaine Antonio told the panel of three justices on Tuesday that the original trial judge erred by not finding the element of unlawful confinement in the conviction. Canadian Press (Toronto Star)

Angela Nicholson launches appeal after found guilty of conspiring to kill husband
A woman found guilty of plotting to kill her husband and her lover's wife is appealing her conviction. In June, Angela Nicholson was found guilty of conspiracy to commit murder and then, earlier this month, was sentenced to three years in prison. Today, Nicholson will be formally appealing her conviction and will be asking to be granted bail. In 2013, Brigitte Vey, the wife of Nicholson's lover, secretly recorded the couple talking about a plot to kill her in a house fire. They also talked about killing Nicholson's husband. During the trial, Nicholson, and co-accused Curtis Vey, argued they weren't serious about killing their spouses. The appeal centers around the trial judge's charge to the jury. CBC News

Full parole for Calgary woman in drunk driving crash that killed friend, other driver
A young woman convicted of impaired driving causing death in a 2012 crash that killed two people has been granted full parole. Amie Nottebrock was at the wheel when she ran a red light at Shaganappi Trail and Country Hills Boulevard in January 2012. Her vehicle hit another car, killing her passenger, Danielle Russell. Arsh Brar, the driver of the other vehicle involved in the crash, also died from his injuries. (…)Nottebrock, 29, had been serving a four-year-and-six-month sentence for two counts of causing death by criminal negligence and two counts of impaired driving causing death, according to Parole Board of Canada documents. The sentence began in November 2014. Global News

More freedom for killer of 16-year-old Stephanie Spooner
A teen killer, who is now 44, has again gained more freedom from prison. Bradley Paetsch, who changed his name to Tristan Ryan, was 18-years-old when he killed his then 16-year-old on-again off-again girlfriend Stephanie Spooner in her Okotoks home. Ryan was granted unescorted temporary absences 48 hours per month at a parole hearing Sept. 8. The visits will allow him to visit his wife, who he married in prison two years ago, and re-integrate into the community. The unescorted absences will last for six months, but can be revoked by his case management team. He was seeking 72 hours per month outside the prison unescorted, but board members called that amount of time excessive. Two of Spooner's relatives were at the hearing, but did not speak. Stephanie's father, Bob Spooner, was not at the hearing, but has repeatedly said he opposes any form of release for his daughter's killer. Ryan told two Parole Board of Canada (PBC) members he was feeling hopeless, suicidal and was drinking daily when he killed Spooner. (…)He was convicted of first-degree murder and is serving a life sentence. Western Wheel

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Thunder Bay police respond to allegations trainer was verbally assaulted in race-relations course
Allegations that a facilitator was verbally assaulted by police officers while conducting race-relations training in Thunder Bay are the result of a "misunderstanding", according to the police service. "You can misread people's tone, attitude and body language in these kinds of sessions," said Chris Adams, executive officer with the Thunder Bay police service. A training session with police officers in July was shut down after "things just got really bad" during a discussion on missing and murdered Indigenous women, the facilitator said. CBC News has agreed not to name the facilitator because she fears that speaking out could have implications for her employment. She described "disruptive and dismissive" behaviour by officers throughout the session and said they accused her of lying about the statistics on missing and murdered Indigenous women and asked her for proof of differential police treatment of Indigenous and non-Indigenous people. "The concerns were dealt with by the [police] training unit, administration and the city," Adams said. The city of Thunder Bay trains local volunteers who are paid an

honorarium to conduct training sessions for all city staff, including first responders such as police, using the Walk a Mile film series, created by local filmmaker Michelle Derosier. CBC News

Fentanyl involved in at least 32 Maritime drug deaths
Jenn Perry doesn't believe her fiancé knew what fentanyl was before it took his life. Two years ago, Perry stood outside a Moncton apartment building, clutching a picture of 29-year-old Julien Gould and waiting to hear if he was alive. She hadn't heard from Gould for five days, silence she said was out of character for him. A few hours later, she identified his body by the tattoos on his hands. Gould and his 36-year-old friend were found dead on an apartment floor on Nov. 9, 2014, after ingesting a white, crystallized powder in a clear plastic bag. That powder tested positive for a derivative of fentanyl, a powerful drug that can be deadly even in tiny doses. (...)Fentanyl has wreaked havoc across New England and in British Columbia, where officials declared a public health emergency after hundreds were killed by overdoses earlier this year. Like Gould, some of those people died after taking the drug for the first time. While fentanyl abuse hasn't reached epidemic levels in the Maritimes, Gould and his friend are not the only people in the region to die after taking the drug. CBC News has analyzed the details of hundreds of drug-involved deaths in New Brunswick, Nova Scotia and Prince Edward Island dating back to 2008. The data shows fentanyl was involved in at least 32 drug-involved deaths. CBC News

Delta holds fentanyl forums to warn community of the deadly drug
In response to the fentanyl health crisis in B.C., two forums are being held in Delta this week to educate the community about the dangerous synthetic opiate showing up in a variety of street drugs. The first of two Fentanyl Forums, hosted by police, city officials and the school district, will take place Wednesday evening at 6 p.m. at the South Delta Secondary School. The second forum will be held Thursday, also at 6 p.m., at North Delta Secondary School . Delta police say speakers will discuss a range of topics including what fentanyl is, why it's dangerous, how prevalent it is, and how it can impact recreational users and their families. Members of the community can also ask the speakers some questions. Two weeks ago, a group of nine friends overdosed within 20 minutes in Delta after snorting cocaine believed to be laced with fentanyl. They all survived after paramedics administered the opioid antidote naloxone. Police believe the 20-something revellers were casual cocaine users and not habituated opiate users. Vancouver Sun

Canada and Muslims: "partners against radicalization, not the problem
A new survey of Canadian attitudes towards the Muslim community shows a slight majority see them as partners in the fight against radicalization, and not part of the problem. However, the survey also shows a distinct desire for the Muslim leaders here to do more to denounce acts of terrorism. Two domestic attacks, the Parliament Hill shooting, and a hit-and-run vehicle killing of a soldier were identified by police as being motivated by violent political ideology related to Islam. When Canadians were asked how they view the Muslim community and its leaders in light of those tragedies, 58 percent said the community and leaders were partners in fighting radicalization, while 42 percent felt the community was part of the problem. In either case, a strong majority (73%) responded that Muslim leaders here were not speaking out enough against homegrown terrorism. Another slight majority, just over 50 percent also believe there are radicalized individuals already in their communities or people in the process of becoming radicalized. As for what people thought caused someone to become radicalized, 47 percent cited religion/culture, 37 percent cited mental illness, and feelings of marginalization were listed by 34 percent of respondents Other causes cited were 'internet recruitment', 'old country beliefs', and 'economic/financial problems'. As to confidence in police ability to stop radicalized Canadians from carrying out acts of violence, the numbers were fairly, with 50 percent saying they felt confidence in police ability, while 43 percent said they were not confident the police can stop radicalized violence. RCI

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Chambers want consultation on marijuana
Local chambers are urging the provincial government to begin a consultative process aimed at developing a regulatory framework for the distribution of medical marijuana. Both the Belleville and District and the Quinte West chambers of commerce are standing behind a letter, authored by Ontario Chamber of Commerce (OCC) President and CEO Allan O'Dette and directed to Premier Kathleen Wynne. on the issue of recreational marijuana. In light of recent commitments from the federal government to legalize marijuana, the OCC is calling on the province to immediately begin a robust consultative process aimed at developing a regulatory framework for the distribution of recreation marijuana. The letter outlines key messages (see fact box on Page A4 for more details) that the collective business community thinks the province should consider. According to the OCC, the government needs to ensure – if recreational marijuana becomes available – that the underground economy is eliminated, access points are limited and that communities have decision-making power. Addiction prevention and treatment programs need to be invested in and the government needs to ensure marijuana products are subject to best-practice health regulation. Intelligencer

Alberta producer launches medical marijuana app
An Alberta-based pot producer has launched a mobile app to make it easier for patients with a prescription to purchase federally-regulated medicinal weed. Cam Battley, of Aurora Cannabis, said the idea was to give customers the same service as giant online retailers such as Amazon. "As far as we know, it is the first legal app for Android and Apple for federally-approved legal medical cannabis," Battley said. "The fact is that people live on their phones and tablets. They use them to shop for everything from consumer products and health products to medicine. It is an acknowledgment of the reality of how people operate today." Canadian Press (Global News)

PUBLIC SERVICE / FONCTION PUBLIQUE

Public service jobs appealing to majority of Canadians: survey
Public service employers that offer job stability, workplace flexibility and technological resources are likely to attract new talent, according to a new survey by global professional services company Accenture. Of the 1,000 Canadians surveyed, 64 per cent said they would consider working for a government department, Crown corporation or agency in the future. Candidates are likely to take a job due to a good salary, benefits and pensions (94 per cent), technology that would improve their productivity and ability to succeed in a role (82 per cent) and the option to work from home or outside the office (93 per cent). Benefits Canada

OTHER / AUTRES

Le premier ministre chinois sera au Canada dès la semaine prochaine
Trois semaines après avoir accueilli Justin Trudeau à Pékin, le premier ministre de la République populaire de Chine, Li Keqiang, visitera Ottawa et Montréal la semaine prochaine. Ce voyage officiel, du 21 au 24 septembre, fait immédiatement suite à la visite d'une semaine du premier ministre Justin Trudeau en Chine, au début du mois. Le cabinet du premier ministre canadien a indiqué mercredi que les deux chefs de gouvernement continueront « à approfondir une relation plus solide et plus stable entre le Canada et la Chine ». Presse canadienne (La Presse)

Ex-UN investigators call for release of Canadian academic jailed in Iran
Twenty former United Nations special human rights investigators added their voices on Wednesday to the growing calls for Iran to release a jailed Canadian-Iranian academic. They raised Homa Hoodfar's case as the UN continued its general assembly in New York. The 65-year-old, who taught at Montreal's Concordia University, has been held at Tehran's notorious Evin prison since June 6. The former

rapporteurs said Hoodfar's academic work poses no threat to Iranian security and that she should be released immediately. "We stress that Iran is breaching its national constitutional principles by arbitrarily arresting and detaining people for simply expressing their opinion and conducting academic research, as is their professional right and duty," they said in a statement. Chronicle-Herald

Canadian Citizen Homa Hoodfar Has Been Detained in Iran for 100 Days
An opinion piece states, "Skull fracture, broken fingers, missing fingernails, severe abdominal bruising, burst ear membrane, broken ribs, broken nose, flogging to the legs, evidence of a brutal rape—that is what the doctor described the night the body of 54-year-old Canadian photojournalist Zahra Kazemi was brought into a Tehran military hospital. Kazemi endured four days of torture inside the Islamic Republic of Iran's notorious Evin prison, before arriving brain dead to the hospital. No one has ever been found guilty or held to account for her death. Thirteen years later, a similar situation is unfolding. Today marks 100 days since Canadian academic Dr. Homa Hoodfar was illegally detained and imprisoned in Iran. She is being held in solitary confinement in the same prison as Kazemi, and last week Canadians were told that Dr. Hoodfar had been taken to hospital in Iran. The press release distributed by her family described Dr. Hoodfar as being "barely able to walk or talk." (…)Dr. Hoodfar is not the only Canadian languishing in an Iranian prison. For the past eight years, Saeed Malekpour, a Canadian resident since 2004, has been imprisoned in Iran on trumped up charges of operating a pornographic website that was "operated by western influences and made to corrupt Iranian youth," the indictment read. Malekpour had made an urgent trip to Iran to visit his dying father in 2008 when he was imprisoned. His sister, Maryam Malekpour lives in Edmonton and told me recently that despite all the letters she has written to Foreign Affairs Minister Dion, their response continues to be that they cannot help her brother because he is not a Canadian citizen. But Homa Hoodfar is a citizen of Canada, and any consideration of re-establishing diplomatic relations with the Islamic Republic of Iran must include both her and Malekpour's immediate release from prison and safe return to Canada." VICE News

INTERNATIONAL

Pardon for former NSA contractor Snowden seen unlikely
The U.S. government will not budge on its demand that former National Security Agency contractor Edward Snowden return to face prosecution for stealing thousands of classified intelligence documents, despite new calls for President Barack Obama to pardon him, U.S. officials said on Tuesday. The officials said they expect Snowden's supporters to use the Thursday release of "Snowden" - directed by veteran filmmaker Oliver Stone - to mount a public campaign demanding a pardon before Obama leaves office in January. Reuters

Paris police arrest second teenager with suspected terrorist links in five days
Counterterrorism police in Paris arrested a 15-year-old on Wednesday on suspicion of having links to the so-called "Islamic State" and plotting terror attacks. This is the second time that a 15-year-old with suspected ties to "IS" has been arrested in just five days. French Interior Minister Bernard Cazeneuve confirmed the arrest and said that intelligence services were working harder than ever to prevent future attacks. "We're working with extreme intensity to identify those we think are likely to carry out an attack," Cazeneuve told reporters. "[France] is in an exceptional level of mobilization." Deutsche-Welle

The young women behind France's 'terrorist commando' network
The recent arrest of four Frenchwomen linked to a failed Paris terror plot has exposed the increasing role women are playing in conducting attacks as the Islamic State (IS) group comes under increasing pressure (…) The high-profile roles that women have played in the latest plot – as well as the resistance some of them put up during their arrest – have raised eyebrows in anti-terror circles. Paris prosecutor François Molins has called the young female suspects a "terrorist commando" network, a label quickly adopted by journalists attempting to unravel the links between the women and Rashid Kassim, a well-known jihadist, as well as other Frenchmen and women involved in a number of terror attacks in France over the past two years. France 24

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

toholdaquill
What are you doing to protect Canada from this threat to our freedom, @RalphGoodale?

Zaigham J Kayani
Attention #RalphGodale are we serious to REPAIR the DAMAGE done already By #C51?

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Maclean's Magazine
New federal tariffs have raised drywall prices. Now Fort McMurray's rebuild could take even longer:

CanRedCrossPEI
Early bird special for the Disaster Management Forum ends Sep 15! http://www.dmforum.ca #DMForum10 #Moncton

CBC Aboriginal
'I'm not a squatter,' says Lake St. Martin evacuee as she fights to stay in vacant home http://ift.tt/2csAtM4

GC Newsroom
@Transport_gc : conducting a #Emergency Exercise at St. Anthony Airport today. No impact to airport services. #NFLD http://ow.ly/180C304cVum

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Rabble.ca
Ah yes, what to repeal of Bill C-51, what to repeal. Spoiler alert: all of it. http://buff.ly/2clno6d

Rabble.ca
The long-awaited C-51 consultation launched Sept 8—@OpenMediaOrg has some concerns http://buff.ly/2c8qU7X #cndpoli

CJFE
Canada's #natsec system undermines #freeexpression & #privacy. The gov't must fix this. http://bit.ly/2c7jkFB

NATIONAL SECURITY / SÉCURITÉ NATIONALE

CBCNews
Anti-money laundering agency Fintrac finds 'very significant' deficiencies in realtor probe cbc.ca/1.3761343 pic.twitter.com/G3KETZIwqg

jkenney
Nobody in Canada knows more about national security than Dick Fadden. Any govt serious about security would heed him https://twitter.com/

Stewart Bell
ISIL 'pushing hard' to radicalize youth: Manitoba teen was pro-ISIL convert. @winnipegnews

BC Civil Liberties
Tune into @CBCMaritimeNoon tomorrow at 8AM PST to hear @bccla's Micheal Vonn talk about IMSI Catchers and compelled passwords!

Rabble.ca
@OpenMediaOrg is taking its fight for free expression all the way to the Supreme Court http://buff.ly/2cuFUf6

David T.S. Fraser
Here's a solution for #LawfulAccess to "basic subscriber information", with judicial oversight and accountability: http://bit.ly/2cCYP7Z

Phil Gurksi
Why an old intel guy can support CVE

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

LeCourrierLaval
Expulsé du pays après avoir purgé sa peine courrierlaval.com/actualites/201...

RCMP Manitoba
#rcmpmb proud to be participating w/@CanBorder in Exercise CRIMSON STEEL at Emerson port of entry

trevortombe
Interesting. On the drywall tariff, CBSA responding to complaint by CertainTeed Canada against, in part, CertainTeed in the US. #cdnecon

NewsTalk770
#Drywall price spike after #CBSA tariff hurts #ymmfire rebuild effort. bit.ly/2cZBbn0

calgaryherald
How are some Canadian cities helping undocumented workers that might face deportation? ow.ly/PFtV304cCQn #workerswithoutborders

TheStarPhoenix
Canada faces big questions about the future of immigration thestarphoenix.com/News/12191358/... #news pic.twitter.com/LF7RKCYEif

CYBER SECURITY / CYBERSÉCURITÉ

IP Osgoode
New post: Public Safety Canada calls for Submissions on New National Cybersecurity Strategy bit.ly/2cayjU4

priorsmart
At iposgoode.ca- "Public Safety Canada calls for Submissions on New National Cybersecurity Strategy" - bit.ly/2cECirn

ReutersLive
LIVE: Rights group says Edward Snowden 'should be thanked and not punished' reut.rs/2cmHnGP

CSE_CST
Electromagnetic Emissions...Should I be Worried? Maybe. Read more here: http://ow.ly/A33U304avbS

LAW ENFORCEMENT / APPLICATION DE LA LOI

KelownaNow
@bcRCMP officers to carry Fentanyl-fighting drug

ChrisDca
RCMP Officers to Be Equipped with Naloxone Kits to Deal with Fentanyl Exposure chrisd.me/2cmRD1Y

CJMENews
RCMP officers to be equipped with kits to deal with fentanyl exposure. ow.ly/tYlp304cC9F

GlobalEdmonton

Some B.C. RCMP officers are speaking out about the dangers of fentanyl exposure after nearly overdosing on the job. glbn.ca/mkaTlj

WLTribune
Williams Lake RCMP issue fentanyl warning to parents: Insp. Pelley releases letter urging parents to talk to ...
bit.ly/2cn57KK

CBC_Aboriginal
Fort Simpson mayor says RCMP used excessive force in detaining her intoxicated brother http://ift.tt/2cXArMl

Alison Crawford
Vigilante child exploitation group's tactics/evidence unlikely to stand...great story here

David Akin
Emergency vehicles at Centre Block. Building cleared but all looks Ok

windspeakernews
RCMP continue investigation into death of Victoria Crow Shoe | Windspeaker fb.me/QduVTnNw

StJohnsTelegram
RCMP seeking public assistance in finding wanted man ow.ly/wKsU304cJde

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

cbcnewsbc
Accused in Kelowna fentanyl bust was former Hells Angels 'middleman'
buff.ly/2cqYdRP pic.twitter.com/R5oNBtYTmG

globalnews
Full parole for Calgary woman in drunk driving crash that killed friend, other driver #yyc glbn.ca/fReyEl

stratapress
"We have found out we have a convicted sex offender living in our townhouse complex..." #strataliving #condolife
timescolonist.com/life/homes/con...

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

VanSunHealth
Councillors in Kamloops unanimously support safe injection clinics ow.ly/iohB504uEuk

VancouverSun
Delta holds fentanyl forums to warn community of the deadly drug ow.ly/9C1S504uvUU

INTERNATIONAL

CBCNews
Calls for Obama to pardon former NSA contractor Edward Snowden likely to be rejected cbc.ca/1.3761582
pic.twitter.com/7SmVet6dPx

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

Today's News / Actualités
September 15, 2016 / le 15 septembre 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

The people of Saskatchewan must decide pipeline regulation future - Liberal MP Goodale
Governments and energy companies "need to go to school" on the effects of oil spills, but it is up to the citizens of the province to determine how pipelines are regulated following the July 20 Husky Energy oil spill, according to **Canada's public safety minister**. ***"That is an issue that the people of Saskatchewan will have to examine, whether the current methodology is appropriate or whether something of a more arms-length nature would be more effective,"*** **Liberal MP Ralph Goodale told**

reporters Thursday in Saskatoon. The roughly 25,000 kilometres of licensed pipelines in Saskatchewan are regulated by the provincial Ministry of Energy and Resources. Its approach has been sharply criticized by the provincial auditor, who concluded in 2012 that it was not in compliance with the law. "There are requirements under this legislation that are not being acted upon. Failure to regulate pipelines effectively could harm people or the environment," Judy Ferguson's 2012 report into the province's pipeline regulatory regime stated. Star-Phoenix

Famille et amis de Michele Torre manifestent
Une soixantaine de personnes ont réclamé la suspension sinon l'abandon de l'avis d'expulsion du Lavallois Michele Torre durant la matinée du 15 septembre devant les bureaux montréalais d'Immigration Canada, rue Saint-Antoine. La manifestation s'est déroulée également devant l'hôtel Ritz-Carlton où le premier ministre Justin Trudeau était de passage. «Notre message a été, j'espère, bien entendu, de confier Nellie Torre. Mon père a purgé sa peine il y a 20 ans. Il a payé sa dette et n'a plus jamais été condamné. Nous demandons aux ministres **Goodale**, McCallum et Trudeau de remédier à cette injustice.» Les nombreuses demandes et lettres acheminées aux ministres libéraux fédéraux sont toujours sans réponse. Seuls eux peuvent suspendre la mesure de renvoi pour des considérations d'ordre humanitaire. Le 9 septembre, Michele Torre a reçu un billet d'avion aller simple pour l'Italie. Il est attendu à l'aéroport Pierre-Elliott-Trudeau ce vendredi 16 septembre à 15h pour être escorté hors du pays. Courrier Laval

Defence minister backs off idea of allowing First Nations to call in military
Defence Minister Harjit Sajjan threw a reality check on the notion he is considering giving direct power to First Nations to call in the military when they feel their rights or communities are being threatened. Sajjan met with indigenous leadership in Winnipeg Wednesday as part of his national defence policy review. At that meeting Ron Swain, vice-chief of the Congress of Aboriginal Peoples, which represents all off-reserve status and non-status First Nations, Métis and Southern Inuit, raised the issue of needing the military to come to the aid of indigenous peoples trying to defend their rights or territories. That could, for example, include protests against pipelines or other development, taking place without First Nations' consent. After the meeting Wednesday, Sajjan's office was non-committal but indicated the request was one of a whole host of things Sajjan would consider as part of the policy review. But Sajjan told the Free Press in an interview Thursday he didn't think the system needs to be changed. "We do have a good system in place and they just need to be reassured the system that is there will serve them as a priority," Sajjan said. The Canadian military is deployed at home almost entirely to help during natural disasters such as the Winnipeg flood in 1997, to help fight wildfires such as last spring's disastrous blaze that razed parts of Fort McMurray, Alta., or the much maligned call for help from Toronto during an extended snow storm in 1998. He said most of the assets and infrastructure to help is kept at the municipal or provincial level. "The military is there as a last resort," he said. Sajjan said the military is there to help First Nations affected as well but he said the process in place is for the province to seek help from Public Safety Canada, which has the lead on emergency preparedness. If the **public safety minister** feels additional resources are needed, he then turns to the defence minister to send in some troops. Winnipeg Free Press

Chris Selley: Shining a light on aboriginal suicides
An opinion piece states “The demand for national strategies to combat every problem under the sun is a signature feature of the Canadian political landscape, and it can be wearisome. Not by accident, Canada is a relatively loose and diverse federation containing multitudes of lifestyles and their associated challenges. Rare is the problem for which there is a single, federally designed solution. Recent demands for a national strategy on suicide prevention, however, have a certain logic — not because we’re “the only developed country without (one),” as the Toronto Star inimitably put it over the weekend, but because the most appalling subset of Canada’s suicide problem exists directly under federal jurisdiction: among the worst-off First Nations… If that holds true today, the rate of suicide on First Nations might well exceed that of any nation state on the planet. Among the Inuit in particular, it certainly does. According to Inuit Tapiriit Kanatami’s (ITK) suicide prevention strategy, in 2009-13 the suicide rate in Nunavut was 117 per 100,000. That’s almost twice the rate in Russia, which leads the world. In 2011, 13.5 per cent of all deaths in Nunavut were suicides. It’s horrifying… On Tuesday, reporters in Ottawa demanded to know what **Public Safety Minister Ralph Goodale** was going to do about the rifle used in the Dawson College

shooting still being legal to buy in Canada, along with a non-restricted longer-barrelled version. Why? Because it was the 10th anniversary of the mass shooting at the school in Montreal, in which some jackass from Lachine killed 18-year-old Anastasia De Sousa. In Canada, banning a specific gun because someone used it to do something awful passes for logical. And everywhere, mass shootings get far too much attention relative to other causes of death — not least suicide." Postmedia Network (National Post)

TOP STORIES / MANCHETTES

Ex-hockey coach and convicted sex offender Graham James granted full parole
A decision to grant convicted sex offender Graham James full parole sparked outrage Thursday from some of the players he abused when he was a junior hockey coach. James, 64, is serving a federal sentence for sexually assaulting players he coached in the late 1980s and early '90s with the Swift Current Broncos of the Western Hockey League. The Parole Board of Canada's decision followed a hearing in Quebec, where James has lived for several years. The move to grant James full parole was swiftly denounced by some of his victims. Canadian Press (CTV News)

Kevin Garratt back home in Canada following release by China
Kevin Garratt, the Canadian who was detained in China in 2014 and indicted on charges of spying and stealing state secrets, is back home in Canada following his release. According to an emailed statement from the Garratt family, a Chinese court ruled on his case on Tuesday and he was deported from the country and "has returned to Canada to be with his family and friends."... In January of this year, a Chinese foreign ministry spokeswoman said authorities there had found evidence that "implicates Garratt in accepting assignments from Canadian espionage agencies to gather intelligence in China." Their family denied accusations the couple had been involved in espionage. The Garratts' initial detention followed closely on accusations by the Canadian government that China had spied on Canadian federal agencies, including the National Research Council. During his China trip and a few days after his meeting with Li, Trudeau was asked how Canada could justify continuing discussions on trade and closer relations while Garratt was being held on charges Canada had said weren't based on evidence. He said Canadian officials had been working "diligently" on Garratt's case and on "other challenging issues." CBC News; Canadian Press (National Post)

Strike averted for Nishnawbe Aski Police Service in northern Ontario
Officers with the Nishnawbe Aski Police Service have reached a tentative agreement with their employer. The union representing officers, the Public Service Alliance of Canada (PSAC), said the deal was reached after two days of meetings with a conciliator. Those meetings were scheduled for Wednesday and Thursday of this week. Without a deal, the union would have been in a legal strike or lock-out position as of Friday morning. "I am very proud of our bargaining team for all their work and to the officers who stood strong and lobbied their provincial and federal political representatives to fund First Nations policing effectively," said Sharon DeSouza, the union's Regional Executive Vice President for Ontario. Nishawbe Aski Police serve 35 First Nations in the most northern parts of Ontario. It's funded through the First Nations Policing Program. An auditor general's report in 2014 found the program is not adequately funded and not working as intended. CBC News

Travis Vader convicted of 2nd-degree murder in McCann deaths
Travis Vader saw two Alberta seniors as "targets of opportunity" the day he murdered them and stole their money, their SUV and their motorhome, a judge ruled Thursday as he convicted the drug dealer and meth addict on two counts of second-degree murder. With a television camera recording the event, Court of Queen's Bench Justice Denny Thomas read a summary of his 131-page ruling, in which he accepted much of the evidence presented by the Crown... At the centre of everything, the outspoken accused man has badmouthed the RCMP, proclaimed himself the victim of a witch hunt, and insisted that he is innocent... Crown prosecutors have argued the McCanns never made it to B.C. According to the prosecution, they were killed near Highway 16, somewhere around Peers, Alta., while Vader was trying to steal from them. Their motorhome was found in flames at the Minnow Lake campground near Edson, Alta., two days after the couple left on their road trip. Their SUV was found several days after that. The McCanns' bodies have never been found. RCMP quickly zeroed in on Vader as a suspect. At the time, he

was a drug addict with no fixed address and a lengthy criminal record for petty crimes. CBC News; Toronto Star; Canadian Press (National Post)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Transport des matières dangereuses à Québec: 161000$ pour des données périmées
«Quand on pense qu'en matière de transport on a pas de données à jour depuis neuf ou dix ans, c'est compliqué», a-t-il lancé. «Mais il n'existe aucune autre donnée. Ils ont fait des évaluations sur des données officielles qui sont vieilles. On s'est posé beaucoup de questions sur la valeur du travail de ceux qui ont fait le rapport, mais à cause de l'absence de données. Honnêtement, c'est anormal», a tranché le maire de Québec. Les données les plus fraîches du rapport qui a couté 161 000$ datent de 2012. Une situation plutôt ironique étant donné que le document de 130 pages a été commandé dans la foulée de la tragédie de Lac-Mégantic qui a fait 47 mors à l'été 2013. «On avait promis de faire l'étude, c'est fait. Mais on n'a pas de garanti», a dit M. Labeaume estimant quand même le travail «utile» et «valable». Le maire de Québec a écrit au ministre québécois des transports, Jacques Daoust et à celui du fédéral, Marc Garneau. Ce dernier lui a déjà accusé réception dans une missive que Régis Labeaume dit avoir trouvé plutôt «insatisfaisante». La Presse

Exercice d'intervention d'urgence à l'aéroport international d'Edmonton
Un exercice d'intervention d'urgence à grande échelle s'est déroulé à l'aéroport international d'Edmonton, avec faux blessés et avion en proie aux flammes. La formation a été mise en place pour permettre aux employés de l'aéroport et au personnel d'intervention d'urgence régionale de preatiquer les procédures en simulant une situation d'urgence. L'exercice a été simulé à l'aide d'une unité mobile ressemblant à un avion utilisée expressément pour des situations de formation. Des flammes et des nuages de fumée s'en sont d'ailleurs dégagés. Des acteurs jouant les victimes d'une explosion se sont prêtés au jeu. Des policiers, des pompiers et des ambulances étaient également présents pour simuler les interventions possibles en cas d'urgence. Radio-Canada

Province doing all it can to help drought-stricken Nova Scotians, says minister
The Nova Scotia government says it was doing everything it can to help the hundreds of families whose wells have run dry this summer. On Thursday, the minister responsible for emergency management office, praised municipal staff and volunteers who have been keeping fire halls and municipal facilities open so those who need water can get it." Ground Search and Rescue, volunteer fire departments have put countless hours in ensuring that people who need water are getting it," Zach Churchill said. "All that can be done is being done." CBC News; Chronicle-Herald; Canadian Press (Cape Breton Post)

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Kevin Garratt back home in Canada following release by China
Kevin Garratt, the Canadian who was detained in China in 2014 and indicted on charges of spying and stealing state secrets, is back home in Canada following his release. According to an emailed statement from the Garratt family, a Chinese court ruled on his case on Tuesday and he was deported from the country and "has returned to Canada to be with his family and friends."... In January of this year, a Chinese foreign ministry spokeswoman said authorities there had found evidence that "implicates Garratt in accepting assignments from Canadian espionage agencies to gather intelligence in China." Their family denied accusations the couple had been involved in espionage. The Garratts' initial detention followed closely on accusations by the Canadian government that China had spied on Canadian federal agencies,

including the National Research Council. During his China trip and a few days after his meeting with Li, Trudeau was asked how Canada could justify continuing discussions on trade and closer relations while Garratt was being held on charges Canada had said weren't based on evidence. He said Canadian officials had been working "diligently" on Garratt's case and on "other challenging issues." CBC News; Canadian Press (National Post); Presse canadienne (Le Soleil)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Aéroports sans douaniers : le point dans l'Est du Québec
Des documents obtenus par Radio-Canada en vertu de la Loi sur l'accès à l'information nous apprennent que les passagers de vols privés qui atterrissent dans les petits aéroports du Canada ne rencontrent pas de douanier. C'est le cas dans l'Est du Québec, où aucun aéroport n'est desservi par l'Agence des services frontaliers du Canada (ASFC). Ce fait explique pourquoi il n'y a pas de vols commerciaux directement en provenance des États-Unis ou d'outre-mer dans l'Est du Québec. Quand un avion commercial revient d'un pays étranger, les passagers doivent passer à la douane dans un plus grand aéroport, comme celui de Montréal, Québec ou Ottawa. Pour ce qui est des vols d'aéronefs privés, comme des jets privés ou des avions nolisés par des entreprises, il est aussi possible de dédouaner les passagers et les membres d'équipage par téléphone ou par télécopieur jusqu'à deux heures avant l'atterrissage. S'il y a un doute sur un passager ou une marchandise, un examen physique peut être demandé. En 2012-2013, cet examen n'a toutefois eu lieu que dans 40 % des cas à travers le pays. Radio-Canada a tenté d'avoir ces données pour l'Est du Québec de la part de l'ASFC, mais nous sommes toujours dans l'attente d'une réponse. Radio-Canada

Transport Canada keeping close eye on bridge following emergency orders
Transport Canada is so far satisfied officials from the Ambassador Bridge company have done enough to act on "safety deficiencies" that have indefinitely closed down a curb lane on the 87-year-old crossing, a spokesman said on Thursday. "The Canadian Transit Company (CTC) is complying with the department's emergency direction, which required CTC to install temporary concrete or steel barriers between traffic on the bridge and the outside curbs as a safety precaution," said Daniel Savoie of Transport Canada. The orders did not include "a timetable for the repairs to be made," he said. "However, the minister of transport, in his statement on this issue, did ask CTC to do everything it can to speed up repair work," Savoie said. Transport Canada and federal Transport Minister Marc Garneau announced Sept. 2 that a section of the bridge will be blocked with concrete barriers near the entrance to Windsor where there is a crumbling sidewalk and rusted-out railings. The orders were issued in the "interest of public safety" after Transport Canada's latest bridge inspection which took place in August and found "issues" with the bridge's outside curbs and railings. Windsor Star

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

Strike averted for Nishnawbe Aski Police Service in northern Ontario
Officers with the Nishnawbe Aski Police Service have reached a tentative agreement with their employer. The union representing officers, the Public Service Alliance of Canada (PSAC), said the deal was reached after two days of meetings with a conciliator. Those meetings were scheduled for Wednesday and Thursday of this week. Without a deal, the union would have been in a legal strike or lock-out position as of Friday morning. "I am very proud of our bargaining team for all their work and to the officers who stood strong and lobbied their provincial and federal political representatives to fund First Nations policing effectively," said Sharon DeSouza, the union's Regional Executive Vice President for Ontario. Nishawbe Aski Police serve 35 First Nations in the most northern parts of Ontario. It's funded through the First

Nations Policing Program. An auditor general's report in 2014 found the program is not adequately funded and not working as intended. CBC News

Travis Vader convicted of 2nd-degree murder in McCann deaths
Travis Vader saw two Alberta seniors as "targets of opportunity" the day he murdered them and stole their money, their SUV and their motorhome, a judge ruled Thursday as he convicted the drug dealer and meth addict on two counts of second-degree murder. With a television camera recording the event, Court of Queen's Bench Justice Denny Thomas read a summary of his 131-page ruling, in which he accepted much of the evidence presented by the Crown... At the centre of everything, the outspoken accused man has badmouthed the RCMP, proclaimed himself the victim of a witch hunt, and insisted that he is innocent... Crown prosecutors have argued the McCanns never made it to B.C. According to the prosecution, they were killed near Highway 16, somewhere around Peers, Alta., while Vader was trying to steal from them. Their motorhome was found in flames at the Minnow Lake campground near Edson, Alta., two days after the couple left on their road trip. Their SUV was found several days after that. The McCanns' bodies have never been found. RCMP quickly zeroed in on Vader as a suspect. At the time, he was a drug addict with no fixed address and a lengthy criminal record for petty crimes. CBC News; Toronto Star; Canadian Press (National Post)

Dawson: la cybersurveillance comme solution?
Le tireur qui a fait un mort et 16 blessés au Collège Dawson le 13 septembre 2006 avait tenu des propos inquiétants sur le site internet VampireFreaks et sur son blogue, en plus d'y afficher des photographies le montrant avec tout son attirail de guerre avant de se rendre lourdement armé au cégep montréalais. Avec les avancées technologiques effectuées depuis 10 ans, une cybersurveillance efficace pourrait-elle empêcher une autre tragédie de se produire ? La question se pose, car Kimveer Gill n'était pas étudiant au Collège Dawson. Son comportement n'aurait pu y être décelé. Mais il avait laissé des traces de son état troublé et de ses pensées violentes sur internet. Selon des experts en cybersurveillance, tenter d'arrêter une personne qui annonce son intention de tuer sur le web, en surveillant les sites internet, est un « défi herculéen » et équivaut « à tendre des filets pour attraper des comètes ». La tâche n'est pas impossible, souligne le professeur Stéphane Leman-Langlois, mais les ressources policières requises seraient alors considérables. La Presse (Le Droit)

La Gendarmerie royale du Canada recherche 4 enfants disparus à Drumheller
La Gendarmerie royale du Canada (GRC) recherche quatre enfants issus de la même famille qui se seraient échappés du domicile familial à Drumheller. Maxim Gruner 15 ans et ses frères et soeurs Olivia 13 ans, Charlie 10 ans et Sofia 8 ans sont portés disparus depuis le 31 août dernier, date de leur fuite. La GRC a expliqué dans un communiqué de presse que les enfants seraient actuellement cachés. Ils seraient aussi toujours ensemble. Radio-Canada

Review flags concerns about money laundering by organized crime in Canada's real estate sector
An in-depth review of Canada's anti-money laundering efforts has uncovered serious concerns that organized crime is using the country's hot real estate sector to illegally funnel cash. The report from the Paris-based Financial Action Task Force makes special note of real estate as an area of the economy with a high risk of illicit activity, one of a few weak spots in what the report calls a comprehensive federal regime to combat money laundering and terrorist financing. The charitable and life insurance industries are also identified in the report as sectors at risk of providing financial help to terrorists and criminals. Of particular concern are real estate schemes in which a foreign or domestic criminal provides cash to a local buyer, or more sophisticated schemes where loans and mortgages are combined with lawyers' trust accounts to move money around quietly. Canadian Press (National Post); Presse canadienne (Le Devoir)

Elsipogtog RCMP seek missing 13-year-old girl - Tia Augustine hasn't been seen since leaving her home around 5 p.m. Wednesday
RCMP in Elsipogtog First Nation are asking for the public's help to find a missing 13-year-old girl. Tia Augustine left her home around 5 p.m. Wednesday and hasn't been seen since. Augustine is Aboriginal and is about five feet, four inches tall with a medium build. RCMP said she has a medium complexion, brown eyes and dark shoulder-length hair with highlights at the ends. Anyone with information about her whereabouts is asked to contact the Elispogtog RCMP. CBC News

Broadcast Media / Médias télédiffusés

CBC News' Power and Politics interviewed RCMP National Drug Program Coordinator Sergeant Luc Chicoine on the RCMP's response to the dramatic increase in fentanyl overdoses. Rough Transcript

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Federal prisons begin stocking fentanyl antidote naloxone after B.C. officers fall ill from suspected opioid exposure
Federal prison officers now have access to the life-saving opioid blocker naloxone, following a complaint that several front-line officers in B.C. were exposed to fentanyl. Jason Godin, president of the Union of Canadian Correctional Officers, says members logged a complaint with the Correctional Service of Canada a few weeks ago after some guards at Mountain Institution in Agassiz fell ill. He said paramedics had to administer naloxone to some of the affected officers, indicating that they had been exposed to fentanyl, an opioid that has led to a surge in overdose deaths in B.C. this year. "Fentanyl is a very dangerous for front-line correctional officers," Godin said, adding he did not have specific numbers on how many overdoses there have been in B.C. prisons. "I know we have issues with fentanyl in the prisons. There certainly has been a huge problem in B.C." Godin said over the past week the union has held several meetings with CSC, which agreed that the spray version of naloxone should be on site so officers have quick access in case of exposure. "We put our concerns on the table to make sure our members are protected," he said. Godin said the two parties agreed to have naloxone on site in a secured area instead of providing it to individual officers. Postmedia Network (Vancouver Sun)

Ex-hockey coach and convicted sex offender Graham James granted full parole
A decision to grant convicted sex offender Graham James full parole sparked outrage Thursday from some of the players he abused when he was a junior hockey coach. James, 64, is serving a federal sentence for sexually assaulting players he coached in the late 1980s and early '90s with the Swift Current Broncos of the Western Hockey League. The Parole Board of Canada's decision followed a hearing in Quebec, where James has lived for several years. The move to grant James full parole was swiftly denounced by some of his victims. Canadian Press (CTV News); CBC News

Sheldon Kennedy convinced sex offender Graham James will reoffend
Former NHL star Theo Fleury called Canada the "Disneyland for pedophiles" following the decision to grant full parole to convicted sex offender and former hockey coach Graham James. The National Parole Board handed down its decision Thursday after a hearing at a federal penitentiary in Laval. Fleury was one of the players James abused while coaching the Swift Current Broncos of the Western Hockey League in the late 1980s and 1990s. Fleury and his cousin, Todd Holt, and former NHLer Sheldon Kennedy are among six former players James has been convicted of sexually assaulting. On his twitter account, Fleury issued a scathing press release which said Graham's former victims are being "re-victimized." "As the news came in today that a repeat offender was granted full parole, we are again asking questions as to how this is possible? I say again, "Canada is the Disneyland for pedophiles," Fleury's statement said. Montreal Gazette; CBC News

No parole for sex offender
Convicted sexual offender Carl Leone will be living at the minimum-security unit of Joyceville Institution for the foreseeable future after the Parole Board of Canada denied his request for day parole Thursday morning. Between 1997 and 2004, the Windsor, Ont., native had sex with multiple women without telling any of them he was HIV-positive. Five known victims contracted the virus from him. Before they met Leone, three of the women he infected were virgins. Two of his victims have attempted suicide. Leone, 40, wearing a light blue golf shirt, jeans and beige running shoes, stared silently at the two parole board members after they rendered their decision in a conference room at the institution just north of Kingston. Leone was sentenced to 18 years in prison after his 2008 conviction on 15 counts of aggravated sexual

assault. He was previously denied day parole on last November. He challenged the decision in a letter sent to the parole board in February, setting up Thursday's hearing. Whig-Standard

Broadcast media / Médias télédiffusés

CBC News interviewed Sheldon Kennedy on the granting of full parole to convicted sex offender Graham James. Rough Transcript

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Eight overdoses in 20 minutes: The night fentanyl-tainted cocaine almost devastated a B.C. town
… Cody was the first of eight overdoses in a frenzied 20 minutes that night across three separate locations in the municipality of Delta. A ninth victim would be discovered about two hours later at a fourth address. They had taken cocaine tainted with fentanyl purchased earlier that evening, likely from the same dealer, police said. "At some point I wondered how many people would live and how many people would die," said Delta Police Staff Sgt. Ryan Hall, the watch commander that night. "How am I going to conduct up to nine next-of-kin notifications?" Postmedia Network (National Post)

Child porn, exploitation numbers jump drastically in Hamilton and across Ontario
In the last decade in Hamilton and across Ontario, child pornography and child exploitation incidents have grown a staggering amount, data obtained by CBC News shows. From police officers to victim services and support workers, the rallying cry is the same: The exploitation of children is a problem that is affecting more victims and demanding increasing attention from police and social agencies every year. "The amount of files coming to our attention is on a massive increase," Ontario Provincial Police Det. Staff Sgt. Frank Goldschmidt told CBC News. It's a loathsome problem that experts say is caused by many things. Chief among them is the continued rise of the internet and social media, which is connecting predators to victims - and to each other - in ways never before possible. While that explosion of technology has also given police a larger arsenal of tools to fight the problem, it's still nearly impossible to keep up with an increasingly interconnected underground culture. Back in 2005, Hamilton police didn't lay any charges for child pornography or child sexual exploitation. But in the last decade, those numbers rose drastically. Statistics Canada data shows local police reported 42 child pornography incidents in 2015. CBC News

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Légalisation de la marijuana : menace ou manne pour l'immobilier?
Les acheteurs de maisons et de condos devront redoubler de vigilance une fois que la marijuana sera légalisée, prévient une entreprise albertaine de remédiation. L'entreprise Western Site Technologies nettoie les résidences qui ont abrité des cultures illégales de cannabis. Selon un de ses employés, Adam Jackson, faire pousser de la marijuana dans une maison crée d'énormes problèmes même s'il s'agit que de quelques plants. La marijuana a besoin de beaucoup de chaleur et d'humidité, ce qui peut générer de la moisissure sans un bon système de ventilation. Ce n'est toutefois pas l'unique problème que pose la culture de la marijuana dans un domicile. « Des produits chimiques et des fertilisants sont évacués dans la plomberie ou suintent dans les tapis et les murs. Les insectes sont un autre problème et les gens devront utiliser des pesticides, » indique M. Jackson. Radio-Canada; CBC News

PUBLIC SERVICE / FONCTION PUBLIQUE

Federal goverment argues pay problems 'an honest administrative error,' as tribunal wraps – Public Service Alliance of Canada filed a complaint in June over payroll mess
The Phoenix pay problems affecting 80,000 workers is an "honest administrative error," the federal government argued as a labour tribunal came to a close on Thursday. The four-day hearing in front of the Public Service Labour Relations Board wrapped up with closing arguments from both sides. During the tribunal, union representatives and senior officials testified, including the associate assistant deputy minister responsible for the roll out of government's new Phoenix pay system. Rosanna Di Paola testified yesterday that the root cause of the problems are insufficient training, not the technology itself. The Public Service Alliance of Canada filed a complaint in June arguing the Treasury Board of Canada broke the law by not paying public servants accurately or on time after the roll out of Phoenix. CBC News

OTHER / AUTRES

NIL

INTERNATIONAL

Snowden's leaks caused 'tremendous' damage to U.S. security: House panel
A U.S. House committee issued a scathing report on Thursday accusing National Security Agency contractor Edward Snowden of lying about his background, feuding with co-workers and leaking secrets that "caused tremendous damage" to U.S. security. The House of Representatives Intelligence Committee report declared that Snowden was "not a whistleblower" as he has claimed in interviews and that most of the material he stole from NSA outposts was about intelligence and defense programs of great interest to U.S. foreign adversaries. The committee only released a four-page summary of what it said was a 36-page investigative report by committee staff that remains highly classified. But the summary contained strong words about Snowden's actions and background. Reuters

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

FrontiereCan
Le ministre Goodale annonce des tables rondes sur le nouveau cadre pour la détention liée à l'immigration http://nouvelles.gc.ca/web/article-fr.do?nid=1124999 …

NATIONAL SECURITY / SÉCURITÉ NATIONALE

cyblesoleil
Un Canadien détenu en Chine pour espionnage est libéré https://t.co/nSQvyAd91W

CanadianPM
Statement by the Prime Minister of Canada on Kevin Garratt's return to Canada: https://t.co/6LLQN00Eq5

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

GgNewsCA
New Brunswick could welcome more Syrian refugees, minister says https://t.co/AgmXfYP8Vj

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Safety_Canada
Have #YourCyberSay! Join us in 1 hour for an English Twitter chat @ 7:30 p.m. EDT, on the evolution of #cyberthreats

Safety_Canada
Welcome to #YourCyberSay Twitter chat on #cybersecurity

Safety_Canada
Before we get going, make sure you read our Twitter Protocol that helps us keep the chat enviro friendly & safe: http://ow.ly/QJ3AX

Safety_Canada
We won't answer questions that attack or discriminate against others, as outlined in our Protocol: http://ow.ly/QJ3AX

Safety_Canada
We've got a great #YourCyberSay chat planned for today!

Safety_Canada
To "set the stage", we want to tell you abt something important underway in Canada on the subject of cyber security #YourCyberSay

Safety_Canada
4 those unfamiliar w/ us, we recently launched a public #cybersecurity consultation. We refer to it as #YourCyberSay

Safety_Canada
The digital environment & technology are always evolving & have a central role in our lives #YourCyberSay

Safety_Canada
They also have far-reaching security, economic & social impacts on Canada #YourCyberSay

Safety_Canada
The #cybersecurity consultation (#YourCyberSay) is the way to share views on this very important subject http://ow.ly/MqxE304fa2q

Safety_Canada
#cybersecurity is not the responsibility of Gov't alone; we all have a role to play #YourCyberSay

LAW ENFORCEMENT / APPLICATION DE LA LOI

660 News
RCMP Statement on Travis #Vader verdict #yeg

Breanna Karstens Smith
In a statement, the RCMP say it fulfilled the role of investigating and gathering evidence and providing it to the Crown #yeg #Vader

TheTorontoSun
Travis Vader guilty of second-degree murder of Alberta seniors Lyle and Marie McCann. http://ow.ly/hHvp304fNAd

Karissa Donkin
Great Q&A here from @AngMacIvorCBC with BC officer training Nova Scotia RCMP on how to deal with fentanyl:

910 CFCW
Drumheller RCMP are asking for the public's assistance in locating four missing children. -- RCMP are searching... http://fb.me/5rts0HmeQ

TorontoStar
Toronto police urging body cameras for officers despite estimated $85M price tag https://t.co/CUirjqkoWG

PnPCBC
Now on #pnpcbc: Nat'l drug program coordinator Sgt. Luc Chicoine on why @rcmpgrcpolice is arming officers with naxolone against #fentanyl

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

VancouverSun
Fentanyl crisis: Prisons stock naloxone after guards exposed to opioid https://t.co/E6l3JE3jO3

GgNewsCA
Swift Current, Sask., mayor shocked Graham James granted full parole https://t.co/ArWrU0t0bs

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

nationalpost
8 overdoses in 20 minutes: The night fentanyl-tainted cocaine almost devastated a B.C. town http://natpo.st/2cuqTcj

vicecanada
How Ontario's opioid overdose strategy is failing drug users: http://bit.ly/2cRNQVu

CBCNews
A walk on the front line of B.C.'s fentanyl crisis reveals dangers first-hand http://www.cbc.ca/1.3762446

PUBLIC SERVICE / FONCTION PUBLIQUE

Kyle Duggan
Minister appearing for Phoenix committee meeting next week. https://t.co/YZFdRkTpgM

OTHER / AUTRES

GgNewsCA
Kevin Garratt back home in Canada following release by China - CBC.ca https://t.co/0D1FNX8J0J

INTERNATIONAL

Reuters
Snowden's leaks caused 'tremendous' damage to U.S. security: House panel https://t.co/RhdEbXwtlZ

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

Today's News / Actualités
September 16, 2016 / le 16 septembre 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Michele Torre, ex-convict, spared deportation at last minute
A convicted felon who once had ties to the Mafia was not deported on Friday, even though a Federal Court judge had ordered Michele Torre out of the country earlier in the day. Torre's family said the last-minute temporary reprieve come following an order from a federal minister's office. His daughter Nellie said her member of parliament, Angelo Iacono, called her right after the deportation order was cancelled. "He advised me that he got a call from the [public security] minister's office saying that they are granting a

stay of a few weeks and they will be reviewing the file," she told CBC News. **No one from Public Security Minister Ralph Goodale's officer would comment, citing privacy reasons.** CBC News; Montreal Gazette; Canadian Press (Winnipeg Free Press)

TOP STORIES / MANCHETTES

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Search boats scour Rivière des Prairies for missing persons
Three search boats are scouring Rivière des Prairies for an unknown number of missing people, possibly kayakers. So far, two have been found safe. Montreal Fire department spokesperson Mélanie Drouin said officials are "looking for people," but did not have more information. Officers from the Montreal and Laval police forces are aiding in the search. Global News

'Praying for tropical storms': Hope for respite in N.S.
An Environment Canada climatologist says it will take the tail end of a tropical storm to end the weeks-long dry spell in Nova Scotia, where some communities experienced their driest summer in more than a century. Bottled water is being delivered to residents of several towns in southwestern Nova Scotia, where close to 1,000 homes are without running water. "It really is a real head-shaker," Environment Canada senior climatologist David Phillips told CTV News Channel on Friday. "When you think about this summer, Calgary had one of its wettest summers on record and parts of Nova Scotia have had their driest in 150 years. We've got records in Dartmouth going back to 1870." CTV News

Water OK: Oil-spill cities can open intakes on North Saskatchewan River
Communities affected by an oil spill into the North Saskatchewan River are being told it's OK to start using the water again. Saskatchewan's Water Security Agency says the cities of North Battleford, Prince Albert and Melfort can resume taking water from the river. The cities had to shut off their intakes and find alternate water sources after the oil plume from a Husky Energy (TSE:HSE) pipeline spill moved downstream. Up to 250,000 litres of oil mixed with a lighter hydrocarbon leaked into the river near Maidstone, Sask., in July. The water agency says about 88 per cent of the oil has been recovered and there is no significant health risk once the water is treated. The City of Prince Albert, which had built a pipe to pump water from another source, said Friday that it will spend the next several days preparing its water treatment plant to return to full operations from the North Saskatchewan on Monday. Canadian Press (CTV News)

Summer storms push Saskatchewan insurance price tag over $30 million
According to new figures released by the Insurance Bureau of Canada (IBC), more than $30 million in insurance claims were issued after several storms passed through the province in June and July. The figures, provided by the IBC, lists the July 10 storm that caused severe flooding in Estevan as the costliest storm in the province this year, incurring more than $24 million in damages. The storm dumped 130 millimetres of rain on Estevan in a very short amount of time, resulting in flooded basements throughout the community. The storm system did a total of $48 million in damages through the Prairies. A storm that passed through Saskatchewan from June 24-25 caused $1.4 million in damage from heavy rain and hail, primarily in the Saskatoon area. On July 16, another storm did $1.5 million in damage, dropping baseball-sized hail in Stewart Valley, and 60 mm of rain in Swift Current in just one hour. One week later, a storm did $5.8 million in damage in the Stewart Valley and Outlook area. The storm did an overall $66 million in damage across Alberta, Saskatchewan and Manitoba. There were also reports of a tornado touching down in the Davidson area during the storm, lasting for four minutes and destroying a few farm buildings. "In recent years we have seen a number of instances of severe weather that go through a region and have heavy rains and winds. It can cause considerable damage," said Steve Kee, director of media and digital communications for IBC. Leader-Post

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Trouver refuge au Canada après avoir caché Snowden?
L'avocat montréalais Robert Tibbo espère que les réfugiés qui ont caché Edward Snowden à Hong Kong pour l'aider à échapper aux autorités américaines pourront refaire leur vie dans un nouveau pays. Et il pense que le Canada pourrait très bien jouer ce rôle. « J'espère que ces gens extraordinaires vont pouvoir quitter Hong Kong et être réinstallés dans un pays qui estime et soutient les droits de la personne », a-t-il déclaré hier lors d'un long entretien accordé à sa résidence de Westmount. « Absolument ! », a-t-il répondu lorsque La Presse lui a demandé si le Canada pouvait constituer une destination intéressante pour les réfugiés en question. Quelques médias, incluant le New York Times et le National Post, ont révélé hier, avec l'assentiment de Me Tibbo, que certains demandeurs d'asile qu'il représente à Hong Kong avaient accepté d'héberger le célèbre lanceur d'alerte en juin 2013. Edward Snowden, qui était arrivé dans l'ex-colonie britannique en mai avec des documents confidentiels en poche pour rencontrer un groupe de journalistes, venait alors de s'identifier dans une vidéo du quotidien The Guardian comme l'auteur de fuites traitant des pratiques de surveillance de la National Security Agency. Et l'aveu venait de déclencher une traque à laquelle il n'était pas bien préparé. La Presse

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Feds stop man's deportation
The federal government has stepped in at the last minute to temporarily stop the deportation of a Quebec man to Italy based on a 20-year-old conviction. Michele Torre was at Montreal's Pierre Elliott Trudeau airport awaiting an early evening flight when word of a ministerial reprieve came down late today. His daughter, Nellie Torre, says she received word from her local MP that a ministerial reprieve had been granted for three weeks to review the case. Canadian Press (Castanet); Radio-Canada; Courrier Laval

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

RCMP officer allegedly caught in Surrey Creep Catchers sting facing charges
A video shot by a controversial group allegedly showing an RCMP officer meeting an underage girl is making the rounds online and being investigated by Surrey Mounties. The Surrey Creep Catchers, who shot and streamed the encounter live on Facebook Wednesday night, claim the man in the video is an RCMP officer. Creep Catchers is a network of people who bait people arranging to meet juveniles and confront them in person, all with the cameras rolling. The RCMP have confirmed they are investigating the filmmakers and the alleged suspect. The man in the video has not been identified. Surrey RCMP said in a statement to CKNW they are "mindful of allegations that the matter involves a police officer. While a number of people have been identified, this remains a fluid investigation and no one is in custody and currently no charges have been laid." Global News; AM 730; Vancouver Sun

New RCMP commander imitates inimitable predecessor

The Upper Columbia Valley has a new commander for its RCMP detachment. Last week, Sergeant Bob Vatamaniuk stepped into the role vacated by former Columbia Valley Staff Sergeant Marko Shehovac in March, and although Mr. Shehovac (or Marko, as he was affectionately called up and down the valley) was an inimitable presence here, Mr. Vatamaniuk is doing is utmost to fill the large shoes left by his predecessor. Sgt. Vatamaniuk made clear last week, during a visit to The Pioneer, just how seriously (and how literally) he takes this quest — donning a faux bushy silver moustache and caterpillar eyebrows to demonstrate that he can not only look like Marko, but that he also has a similar sense of humour to the former commander. Columbia Valley Pioneer

Travis Vader verdict: lawyer files appeal notice less than 24 hours after convictions
The lawyer for Travis Vader, found guilty of second-degree murder in the deaths of an Alberta couple Thursday, says he has filed notice he will appeal his client's conviction. Brian Beresh says the appeal focuses on what he calls a major error in the ruling and is seeking to have Vader acquitted or a new trial ordered. The appeal also asks that if granted, a new trial be by judge and jury. Beresh says Justice Denny Thomas relied on a section of the Criminal Code that has been declared unconstitutional and made other errors involving the interpretation of evidence. Canadian Press (Global News)

Cops and cameras: What are your rights? - 'Caribou Legs' was stopped from filming a police officer outside Montreal
Two incidents in the past week involving cops, cameras and Northerners have raised the question: when are people allowed to film police at work? Inuvik's Brad Firth, known as Caribou Legs, was around 10 kilometres outside of Montreal when a police officer stopped him on the side of the highway. A video, posted on Facebook by the marathoner — who's running across the country to raise awareness around the issue of missing and murdered Indigenous women — shows a Sûreté du Québec officer approaching him on the side of the highway, asking a series of questions. After a brief interaction, the officer reaches towards the camera and blocks the lens. The video cuts out… A similar incident allegedly occurred last Friday in Fort Simpson during the public arrest of Darrell Sibbeston. "When I was at the scene... The RCMP officer was pointing his finger at me and telling me now is not the time, and he was asking me to leave," says the town's mayor Darlene Sibbeston, who's the sister of the man arrested. "I was calling out to the crowd: 'Is there somebody with a camera or phone?' And one of the community members came up with their cell phone and started taking pictures, and [the RCMP officer is]… blocking her and telling her she was not to take any pictures and leave. "She didn't put the camera away, she continued to take pictures close up and away, and I don't believe that she said anything, she refused to leave the situation," adds Sibbeston. An RCMP spokesperson declined to comment on the Fort Simpson incident, saying it was currently under internal review. CBC News

St. Albert RCMP issue warning after three fentanyl overdoses in the last week
A warning to parents, children and residents about fentanyl after three overdoses in St. Albert in the last week alone. According to the RCMP, in each case the individual was non-responsive and given naloxone, which immediately reverses the effects of the drug. All were transported to hospital and later released. "In all three cases, the individuals involved were extremely fortunate that they were located and received treatment so quickly as the outcome could have been drastically different," said Cst. M.J. Burroughs. They're reaching out to the public in hopes of, once again, informing them about the risks of this dangerous drug. 660 News

Êtes-vous préoccupés par les drones de la GRC?
La GRC utilise des drones dans des activités de surveillance sans l'encadrement voulu par le Commissariat à la protection de la vie privée. Les engins sont utilisés plusieurs fois par jour et le nombre de missions augmente. Radio-Canada a enquêté et a publié un article sur ce sujet. Des documents internes de la GRC, obtenus par Radio-Canada, montrent que la surveillance de personnes fait partie des tâches pour lesquelles ses drones peuvent être utilisés. Mais cela nécessite l'obtention d'une autorisation judiciaire. Radio-Canada

Conduct hearing postponed again for Osoyoos Mountie in fourth year of paid suspension
The lawyer for a Mountie in his fourth year of paid suspension told a disciplinary hearing Tuesday that proceeding with the matter could prove to be "an embarrassment for the RCMP". John Benkendorf,

representing Const. Amit Goyal of the Osoyoos detachment, said that after reviewing new evidence in the case, "it got to the point where I felt this hearing would be an embarrassment for the RCMP were it to proceed." The material, which Benkendorf described as "incontrovertible evidence of (Goyal's) innocence," led him to do something he had never done in five years of representing officers in misconduct allegations. Ahead of the scheduled hearing, he presented his defence case to his opposing counsel, the lawyer representing the RCMP. After the opposing lawyer reviewed Benkendorf's evidence, he agreed the four-year-old matter should not go ahead on Tuesday's scheduled hearing and instead he requested it be adjourned for a fifth time. The lawyers for both sides told Postmedia News it was a particularly unusual turn of events. Postmedia News (Osoyoos Times)

La centralisation de la lutte contre le crime organisé suscite des inquiétudes en région
Des craintes circulent dans les milieux policiers et judiciaires selon lesquelles les plus récents changements de structure dans la lutte contre le crime organisé faciliteront le retour en force des Hells Angels et autres groupes de motards dans les régions du Québec. Comme l'a démontré le reportage d'Enquête diffusé jeudi soir, les défis sont grands pour les policiers et les procureurs, maintenant que le crime organisé intègre l'économie légale - grâce à des commerces de vapotage ou de vêtements, par exemple - et qu'il recommence à mettre sur pied de nombreux clubs-écoles. Or, plusieurs sources consultées par Radio-Canada sont d'avis que l'abolition du Bureau de lutte au crime organisé (BLACO), en 2015, a dilué l'expertise de la Couronne. Elles jugent en outre que cette réorganisation, qui a fait en sorte de centraliser les activités de lutte contre le crime organisé à Montréal, a nui à des régions comme l'Outaouais, l'Estrie, la Mauricie, Québec et le Saguenay, qui disposaient jusqu'à l'an dernier d'antennes régionales du BLACO. Radio-Canada

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Parole denied for multiple offender who took part in 1995 Toope murders
A man serving time for having killed a passenger in his car while driving impaired in LaSalle and for strangling his ex-girlfriend has been denied parole because his violent behaviour has continued while behind bars. Ryan Patrick McPhee, 36, has served time in the past for his role in the April 2, 1995, deaths of Jocelyn and Frank Toope, an elderly couple who were murdered in their home in Beaconsfield. McPhee, who was 14 at the time, and two other youths broke into the home because they believed the Toopes were on vacation. McPhee testified about his role in the murders in adult court, in 2012, and admitted he struck Frank Toope, a 75-year-old Anglican minister, with a baseball bat during the attack on the couple. Jocelyn Toope was 70 at the time of the murders. McPhee received three-year sentence, as a youth, after being convicted of second-degree murder. The murders are mentioned in a recent decision by the Parole Board of Canada denying McPhee any form of release on the 39-month sentence he received in 2014 for his latest crimes. Montreal Gazette

OPP seek public's help to locate federal offender known to frequent Ottawa
The Ontario Provincial Police is seeking the public's help to locate a federal offender known to frequent the Ottawa and Toronto areas. Mohamed Hersi, 29, is wanted on a Canada-wide warrant for being unlawfully at large, said the OPP's Repeat Offender Parole Enforcement unit in a release Friday. Hersi is serving a 27-month sentence for break and enter, assault with a weapon, robbery and forcible confinement. Ottawa Citizen

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NIL

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

B.C. First Nation offers 20K reward in case of Immaculate Basil, missing since 2013 - Immaculate Basil, 26, last seen June 14, 2013 near Fort St. James, B.C.
A $20,000 reward is being offered for information that could help locate an Indigenous woman who disappeared from northern British Columbia three years ago. Immaculate "Mackie" Basil was 26 when she was last seen on June 14, 2013, around the Kuzche Reserve near Fort St. James, British Columbia. At the time, an extensive search by the RCMP and search rescue teams failed to find her. Large community searches were also conducted. The Tl'azt'en First Nation posted the reward after Immaculate's older brother, Peter Basil, approached the band to ask for help. "I asked our chief for $20,000, and he said he was going to put it through chief and council, and they did approve it for me," said Peter." The family is trying to open up any avenue that will get Mackie back," said Ron Wisner, the community's economic development officer, who also helped coordinate community searches when Immaculate first went missing. CBC News

'Loving' tribute to missing and murdered Indigenous women part of Edmonton art installation
An Edmonton artist has created a personal tribute to missing and murdered Indigenous women that, for a few hours Friday, people can actually walk through. The work by Dawn Marie Marchand is based on one of her paintings called "Prayers for my Sisters," and is open to everyone until around 6 p.m. Friday, at 101A Avenue and 96th Street "I've had my own personal life touched by violence. I could very easily have been one of these women," said Marchand, who is a Cree-Metis mixed-media artist and the first ever Indigenous artist in residence for the City of Edmonton. Marchand said the issue of the nearly 1,200 cases of missing and murdered women the RCMP have documented between 1980 and 2012 is one that's close to her heart and one that has affected many friends and family. She hopes when people walk through the installation they stop to remember all of the women. CBC News

Violence against aboriginal women ignored
An opinion piece states "At the centre of a circle of remembrance in London's Ivey Park last Sunday morning stood a staff decorated with colourful ribbons and two eagle feathers. The staff, said Dennis Whiteye, men's co-ordinator at AtLohsa Native Family Healing Services, is a sign of the 'life-giving force that women represent' in native culture. At its tip were two eagle feathers: one in memory of Therssa Wilson, a Londoner who went missing in November 2010 and was found dead near Chatham four months later; the other to commemorate Sonya Cywink, a London resident found murdered in August 1994. Nearby, Ken Oliver, who co-ordinates the Kizhaay Anishinaabe Niin ('I am a kind man') initiative to help aboriginal men understand the effects of violence against aboriginal women, smoked a ceremonial pipe, its stem representing the male spirit entity and its bowl symbolic of the female entity... The National Inquiry into Missing and Murdered Aboriginal Women and Girls, which formally began its work Sept. 1, aims to 'look at all underlying causes of violence against indigenous women and girls, including systemic issues, and make concrete recommendations to end the unacceptably high rates of violence, as well as the authority to examine institutional policies and practices such as policing or child welfare.' The panel's five commissioners, led by B.C. provincial court judge Marion Buller, are still trying to figure out how they'll tackle that mammoth task. But at least one thing should be clear: the inquiry must be more than a venue for the retelling of Canada's record of injustice against native people. It must be more than an inquiry that traces the many scourges that afflict First Nations people to the residential schools system. Those things have been established. And while the inquiry's hearings will serve as an opportunity for cathartic storytelling and attempts at some degree of closure by the families and loved ones of missing and murdered women, the exercise will be a failure if it does not adequately fulfil the 'concrete recommendations' aspect of its mandate and then see measures adopted by the government. Postmedia Network (London Free Press)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

NIL

PUBLIC SERVICE / FONCTION PUBLIQUE

Public service union frustrated, disappointed with bargaining - PSAC president says the Liberals are negotiating like the former Conservative government
After a week at the bargaining table, the head of the Public Service Alliance of Canada says union negotiators are frustrated and disappointed with the Liberal government. "They told our teams they don't have a mandate," said Robyn Benson, PSAC president. "Well, if you don't have a Liberal mandate, then you still have a Conservative mandate." Benson said the government's agenda has changed very little since the Liberals were elected almost a year ago. PSAC, which represents a majority of federal government workers, has been trying to negotiate a new collective agreement for 26 months. Benson said no future bargaining dates are planned at this time, giving the union time to prepare its next steps. Benson said the PSAC remains open to negotiations, but only if government will make substantive changes to its offers. Among the top issues for the union are a negotiated sick leave program and a wage increase. So far the government has offered a wage increase of 0.5 per cent. CBC News

OTHER / AUTRES

Federal copyright lawsuit involving Blacklock's Reporter puts content paywalls at stake
One of two radically different things will be taking place in an Ottawa court starting Monday. If you believe one side, a forum is being given to a "troll" website that hoodwinks government agencies into accessing content and then unfairly sues them for copyright infringement in order to make money. If you believe the other, an upstart media outlet is making an unprecedented defence of Canadian intellectual property rights in the digital era against federal bureaucrats who would rather steal than pay for content. What's not at issue is that the potential implications for Canadian copyright law are tremendous. Blacklock's Reporter, a four-year-old Ottawa-based subscription news site that caters to policy wonks, is suing the Government of Canada, claiming that staffers at Finance Canada used the subscriber account of a third party to access two articles from its website. Blacklock's does not disclose its number of subscribers, although says it has bulk subscriptions in all 10 provinces. An individual annual membership to its website currently costs $314. Financial Post

INTERNATIONAL

House Intelligence Committee Urges No Pardon for Edward Snowden
Lawmakers on the House Intelligence Committee unanimously signed a letter to President Obama on Thursday asking him not to pardon Edward J. Snowden, the former intelligence contractor who leaked troves of information about National Security Agency surveillance and data collection in 2013. "We urge you not to pardon Edward Snowden, who perpetrated the largest and most damaging public disclosure of classified information in our nation's history," the bipartisan letter said. "If Mr. Snowden returns from Russia, where he fled in 2013, the U.S. government must hold him accountable for his actions." New York Times

Study Confirms That Zika Virus Causes Brain Damage In Newborns
Early results from a crucial case-control study in Brazil have confirmed a direct causal link between Zika virus infection in pregnant women and the brain damaging birth defect microcephaly in their babies, scientists said on Thursday. But while preliminary findings from the first 32 cases involved in the study confirm causality, the researchers said, the true size of the effect will become clear only after full analysis of all 200 cases and 400 controls. The study, published in The Lancet Infectious Diseases journal, was requested by the Brazilian health ministry to investigate the causes of the microcephaly epidemic that the World Health Organization (WHO) declared an international public health emergency earlier this year. Reuters (Huffington Post)

Typhoon Kills at Least 11 in China and Taiwan; Another on the Way
The world's strongest storm this year killed at last 10 people in China when it hit the southeast coast, the government said on Friday, as rescuers scoured flooded streets and work crews struggled to restore power to more than a million homes. Typhoon Meranti had largely dissipated by Friday afternoon, a day after it swept in from the Pacific Ocean, clipping the southern tip of Taiwan, and making landfall near the Chinese port city of Xiamen, in Fujian province. The storm killed seven people in Fujian and three in neighboring Zhejiang province, state media and the government said. Eleven people were missing. Reuters (NBC News)

Suicide bomber kills at least 25 in Pakistan mosque
A suicide bomber has killed at least 25 people and wounded more than 28 others during Friday prayers at a Pakistan mosque in a tribal area bordering Afghanistan, local officials said. The attacker shouted "God is Great" as he entered the mosque in the village of Ambar in Pakistan's Mohmand tribal region, government administrator Naveed Akbar told The Associated Press. He said rescuers had transported the dead and wounded to nearby hospitals, where some of the wounded were listed in critical condition. Akbar said about 200 worshippers were inside the mosque at the time of attack. Al-Arabiya

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

RalphGoodale
Happy to join w/ @SUMA_amplify Malcolm Eaton at announcement of $236million for new infrastructure investment in SK

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Global_Montreal
Search boats scour #RivieredesPrairies for missing persons https://t.co/YXw06nRsG5

DRDC_RDDC
#CSSP funded project helps Canadian firefighters make more informed decisions #NatlPrep http://www.drdc-rddc.gc.ca/en/dynamic-article.page?doc=information-that-saves-lives-the-value-of-a-national-fire-information-database/ijzbnh4d ...

CTVNews
'Praying for tropical storms': Hope for respite from Nova Scotia dry spell http://ow.ly/Nk8g304i8lV

CTVNews
Communities affected by North Sask. River oil spill told it's OK to use the water again http://ow.ly/w4zw304i9gR

CBCAlerts
USGS reporting 4.3-magnitude earthquake 189 km west-southwest of Bella Bella, B.C. No reports of damage, and none are expected.

NATIONAL SECURITY / SÉCURITÉ NATIONALE

rabbleca
B.C. Supreme Court finds RCMP planned, funded and facilitated terrorist offence http://buff.ly/2d0vS7J #cdnpoli

LAW ENFORCEMENT / APPLICATION DE LA LOI

globalnews

BC RCMP officer allegedly caught in Creep Catchers 'sting' operation now facing two charges. https://t.co/M6Ocwh05WM

globalnews
"This is an exceptional error in an exceptional case": Criminal law prof on conviction & Travis Vader appeal #yeg https://t.co/4mgYouxXGU

rcmpgrcpolice
Wanna influence choices? Let us hear your voices! Youth aged 13-18 can now apply to join the #RCMPYouth Committee. http://rcmp.ca/-ruO

motherboard
Body cameras won't end police brutality in Toronto http://bit.ly/2cPg2tz

BurnabyRCMP
Join us tomorrow at our Open House from 11am to 3pm at Burnaby Det/City Hall. Bring your best moustache! @bcRCMP

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

CBC_Aboriginal
B.C. First Nation offers 20K reward in case of Immaculate Basil, missing since 2013 http://ift.tt/2d6L7uN

PUBLIC SERVICE / FONCTION PUBLIQUE

CBC News Alerts
Canada's chief statistician stepping down with a bang. Wayne Smith sends letter to staff blaming Shared Services Canada difficulties. 1/2

CBC News Alerts
Smith: Government handed crucial StatsCan informatics infrastructure to SSC, damaging StatsCan's independence and efficiency. 2/2 #cdnpoli

GgNewsCA
Public service union frustrated, disappointed with bargaining https://t.co/ZQSpx2zCtl

OTHER / AUTRES

nationalpost
Federal copyright lawsuit involving Blacklock's Reporter puts content paywalls at stake http://natpo.st/2cwUgej

INTERNATIONAL

Independent
Leaked email reveals Israel has '200 nukes' https://t.co/UTo9T8yeWY

HuffPostCanada
Study confirms that Zika virus causes brain damage in newborns http://huff.to/2cUrXoN

NBCNews
Typhoon kills at least 11 in China and Taiwan as another storm looms http://nbcnews.to/2cdk3oM

AlArabiya_Eng
Suicide bomber kills at least 25 in #Pakistan mosque

Blogs

Our best chance to repeal Bill C-51 is officially here

Here we go, everyone: the government has just released its official consultation on Bill C-51, privacy, and national security. This consultation represents our last, best chance to get this reckless legislation repealed, and to deliver the strong privacy rights Canadians deserve. Your OpenMedia team is working hard to ensure your voices won't be ignored. Today we're sharing a new action for you to tell the government to repeal Bill C-51 and strengthen our privacy laws to keep us safe. By taking action, we'll send a full letter on your behalf to Public Safety Canada's Consultation on National Security. Check it out right now. and let's tell **Public Safety Minister Ralph Goodal**e: "Repeal Bill C-51 and create strong, transparent, and enforceable privacy laws as outlined in Canada's Privacy Plan." rabble.ca blogs

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

Today's News / Actualités
October 3, 2016 / le 3 octobre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

TOP STORIES / MANCHETTES

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Northwestel phone, internet services back up after Telesat satellite issue in Northern Canada
Northwestel phone and internet services have been restored in all satellite-served northern communities after problems with a Telesat satellite disrupted communications in a wide swath of northern Quebec and Nunavut on Sunday afternoon. After more than 12 hours, debit and credit services in much of Nunavut are finally back online (...)The Telesat Anik F2 satellite cut out around 5 p.m. ET Sunday. In a statement, the company said the satellite, which helps provide cellphone and internet service to communities across the North, experienced a "technical anomaly" that resulted in loss of services. The outage would also have impacted ATMs and aircraft in some communities, said John Flaherty, vice-president of marketing for Telesat, early Monday morning. CBC News

Disaster Assistance Granted To Flooded Homeowners
Windsor-Essex residents dealing with flood damage can now apply to get financial assistance from the province. Minister of Municipal Affairs Bill Mauro met with a team assessing damage in Tecumseh, Lakeshore and Windsor, and has determined that the region needs access to disaster relief programming. Half of the programming is for citizens, although Mauro's quick to point out that the funding is not a replacement for insurance (...)The other half of the disaster relief programming is for municipal infrastructure that may need repair. Blackburn News; CTV News

Search for missing boater resumes in Lac Saint-Louis
The search for a 38-year-old Laval man who fell from a boat in Lac Saint-Louis over the weekend resumed Monday morning. Authorities believe the missing man and three other men left Pointe-Claire Marina to go fishing around 10 p.m. Friday night. Police, firefighters and the Canadian Coast Guard spent Saturday looking for him. CBC News

Missing teenager found in Red Deer
Marissa Greenwood, 15-year old female from Drayton Valley, has been found. The Drayton Valley RCMP said Greenwood was located on Sept. 29 in Red Deer. Greenwood was reported last seen by family members on Sept. 22 in Red Deer but no contact was made. The Drayton Valley RCMP and the Red Deer City RCMP worked together in investigating this case and in locating Greenwood. Drayton Valley Western Review

103 Squadron takes SAREX trophy
A Royal Canadian Airforce (RCAF) search and rescue squadron has emerged as the best overall crew at a recent national SAR exercise (SAREX). The event, held in Yellowknife, Northwest Territories, Canada from 18 to 24 September, brought together over 230 participants from rescue organisations such as the Civil Air Search and Rescue Association (CASARA), the Royal Canadian Mounted Police (RCMP) and various RCAF squadrons in the week-long exercise (...)The exercise also saw the department of Fisheries and Oceans, Environment and Climate Change Canada, Public Safety Canada and Transport Canada help and observe proceedings. A variety of RCAF aircraft were used during the exercise, including CH-149 Cormorant helicopters, CH-146 Griffon helicopters, and CC-130H Hercules and CC-138 Twin Otter planes. AirMed & Rescue Magazine

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Quebec men among 'first wave' of Canadians to join jihadist groups
In 2012, a handful of young men from Quebec left the country for Turkey after having prepared as if they were heading to war. Four years later, police are still trying to establish what really happened during their trip. Some are suspected of having taken part in a kidnapping in Syria. Others were suspected of having fought alongside Islamists. They are the subject of a La Presse investigation into what appears to be the first wave of Canadian foreign fighters... For months, the Quebec group prepared their departure, according to sources. They trained with weapons, they frequented the same mosques - including two Montreal Islamic centres, Badr and Assahaba - and met up regularly at each other's house... Another man, who was 18 at the time of his departure, told his family that he left to do humanitarian work in Turkey. He had recently converted to Islam and practised an extremely rigorous version, refusing to shake hands with women. His speech became more and more alarming. In his luggage, he had night-vision goggles. Several months after leaving, he returned, completely disillusioned, said the imam who counselled him upon his return to Canada. What happened during his trip? He told investigators that he went to Antakya, a Turkish city well known as a passage for jihadists going to Syria. He swears that he never crossed the border. But that's not the view of police. According to court documents obtained by La Presse, the RCMP's Integrated National Security Enforcement Team believes that he and at least five other members of the group were involved in the kidnapping of two American journalists in Syria in 2013, which was orchestrated by a group linked to Al Qaeda. Toronto Star

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Irish-accented contractors in alleged paving scam arrested, ordered deported
Four people have been arrested and ordered removed from Canada after police warned the public about an alleged paving scam involving suspects with Irish accents. Four foreign nationals were arrested and $70,000 in cash was seized after investigators from the Canada Border Services Agency and Ottawa police's fraud unit teamed up to arrest the quartet on Sept. 24. The arrests came four days after Ottawa police warned the public to beware of door-to-door paving contractors with Irish accents who would quote an inexpensive price to repave a driveway or lane, only to do the work and then demand more money. The CBSA said Monday that the four foreign nationals who are suspected of being involved in the fraudulent contract work were working without a permit in Canada. According to the CBSA, an admissibility hearing took place in front of the Immigration and Refugee Board on Sept. 27 and all four were ordered removed from the country. The four were ordered to remain in custody pending their removal. All four are accused of two offences under the Immigration and Refugee Protection Act. Their names were not released. Ottawa Citizen

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Over 70 Per Cent Terrorists Using Cyber Space: PMO Cyber Coordinator
Over 70 per cent of terrorists and terror groups across the globe are using various cyber medium tools to spread the evil of terrorism and further their goals, Gulshan Rai, the National Cyber Security Coordinator in the Prime Ministers Office (PMO) has said. Speaking at the India Conference on Cyber Security & Internet Governance organised by Observer Research Foundation in New Delhi, Mr Rai said 70-75 per cent of terrorists are using tools like voice over internet telecom, social media and even encryption to spread the menace of terrorism and further their goals. He said that post the controversy surrounding whistle-blower Edward Snowden, users and nations have become worried about the security of their data and are now using various encryption techniques and policies that has led to interruptions in seamless flow of data and information. NDTV; One India

Google diverts would-be jihadists away from radical websites

Hundreds of thousands of people seeking information about Islamic State on Google have been diverted to anti-extremism search results, as part of a drive to stop Muslims becoming radicalised online. The pioneering project directed people searching for particular Isis-related terms to YouTube videos that confront jihadist propaganda. The under-the-radar scheme, which has been praised by government ministers, made use of Google's AdWords service, which allows organisations to pay to have their results at the top of searches. The Times

Space Wars Will Be Fought With Hacks, Not Missiles
On Monday morning, a number of professionals in the aerospace industry received a rather mundane email containing a PDF ostensibly about the future of Russian aerospace programs, but which actually contained a 'Komplex' trojan. The Komplex trojan works by connecting the user's computer to a remote command and control server, a centralized computer that issues commands to a botnet. Although nothing malicious has happened in connection with the Komplex virus yet, this could change should the hackers responsible for the virus (believed to be the Sofacy Group, an infamous cyberespionage collective) choose to send commands through this server to be executed on the infected computers. The Sofacy Group's chosen target—the aerospace industry—is instructive, insofar as it speaks to the growing vulnerability of space systems in the information age. To address this issue, a panel of security experts convened at the International Astronautical Congress on Friday morning to discuss cyber-vulnerabilities particular to the space sector and how to protect it against hacking. Motherboard

UK National Cyber Security Centre comes online to protect nation from threats
The UK's National Cyber Security Centre (NCSC) has now opened, acting as a central command post to coordinate the nation's response to the growing threat of cyber attacks.The centre is based in London, near Victoria, and is headed by Ciaran Martin, formerly director general for cyber at GCHQ. Dr Ian Levy, currently technical director for cyber security at GCHQ, will join as technical director. They will oversee 700 staff at the facility. Speaking ahead of the launch of the centre last month Martin revealed that the government logs over 200 "national security-level cyber incidents" a month, and that it is only a matter of time before one does serious damage. The creation of a new centre to coordinate the response to cyber threats, including working with the private sector to have the right protection in place, was seen as vital for the future of the country. V3; SC Magazine; IT Pro Portal

Report a Grim Reminder of State of Critical Infrastructure Security
U.S. critical infrastructure got another reminder this week that it needs to do more to protect itself from cyber attacks with the release of an annual government report. The NCCIC/ICS-CERT FY 2015 Annual Vulnerability Coordination Report points out that nagging issues continue to plague industrial control systems (ICS) and SCADA systems, notably a dearth of access controls limiting unauthorized access, poor software code quality, and the weakening, or absence of, crypotographic security when it comes to the protection of data and network communications. The report, released by the U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), represents trend data culled by private and public industrial control firms for 2015. Topping the list of industries with the most reported vulnerabilities are energy, critical manufacturing, water and wastewater systems, and food and agriculture. Threat Post

HITRUST Begins Sharing Cyber Threats With Homeland Security
HITRUST, a consortium of stakeholders collaborating to better secure protected health information, is the first healthcare cyber threat-sharing information organization to connect with the federal government's cyber threat sharing program. The federal program, launched earlier this year, is the Automated Indicator Sharing Program of the Department of Homeland Security, designed to collect and disseminate cyber threat information. The DHS program enables electronic exchange of cyber threat indicators across private sector industries, and HITRUST is the first healthcare organization to link with the feds to receive and submit threat information, says CEO Daniel Nutkis Information Management

A top-level look at the cyber criminal underworld
Last month at CloudSec 2016, Robert McArdle - EMEA manager for forward looking threat research at Trend Micro – held a talk about the differences between the various underground marketplaces around the world. Undergrounds tend to be separated by language rather than geographical location and "the big three," as McArdle called them, are the Russian, Chinese and English speaking marketplaces. "You

need to be able to know your enemy in order to be able to defend against them," McArdle said, so understanding the differences between these secretive hangouts could be the difference between staying secure or being the next victim of a cyber attack. IT Pro Portal

LAW ENFORCEMENT / APPLICATION DE LA LOI

Man found bleeding on steps of RCMP detachment in Burnaby
A man is in hospital this morning after being found on the front steps of the Burnaby RCMP detachment, stabbed in the lower back. Just before 2 a.m. Monday the man was reportedly at an apartment nearby when he got into an altercation and jumped off the balcony. Witnesses say he then ran to the police station on Hastings Street near GilmoreAvenue for help. It appears his injuries are not life-threatening. Global News

Ex-Mountie charged with drug dealing expected to enter plea
A former high-profile Kamloops police officer accused of trafficking cocaine while still employed by the RCMP last summer is expected to enter a plea later this week. Randi Love did not appear in person on Monday for a brief hearing in Kamloops provincial court, at which her arraignment was set for Thursday. Her lawyer, Brad Smith, appeared on her behalf. The 40-year-old is facing three counts of trafficking cocaine stemming from a trio of alleged incidents on separate dates in June 2015. At the time, Love was on injury leave from her job as an RCMP constable. Police launched an investigation into Love in the weeks that followed. She submitted her resignation papers to the national police force in October 2015. Love made headlines in 2013 when she testified at the fraud trial of her former boyfriend, then-RCMP Const. Trent Wessner, who was convicted of bilking Costco out of $400 based largely on Love's testimony. Wessner left policing following the conviction. Kamloops This Week

Large meth lab bust in Abbotsford nets police two suspects
Two men are in custody after a methamphetamine lab bust in a residential Abbotsford neighbourhood. The RCMP clandestine lab unit, Abbotsford police and Abbotsford fire and rescue swooped in on the house at 35045 Marshall Road Sunday around noon. "It was a large scale operation," said Abbotsford Police Const. Ian MacDonald, describing the size of the lab that was discovered. "A 20-year-old and a 30-year-old are in custody." MacDonald said he expects the men to be named, and charges to be laid, either today or tomorrow. He estimated it will take a little longer to complete a full inventory and analysis of the chemicals seized, some some which are considered hazardous. CBC News; CTV News

RCMP officers rescue man from Peace River
A pair of RCMP officers in Peace River are being hailed as heroes after a harrowing water rescue on the Peace River over the weekend. At approximately 9:00 on Saturday morning, members of Peace Regional RCMP were called to a report of a man in distress in the waters of the Peace, near downtown Peace River. Police arrived at the shoreline along with other EMS and called for the male to swim to shore as rescue boats were dispatched. As emergency personnel watched, the man was seen to be unable to manoeuver himself to shore and appeared to be going under. Two officers on shore jumped into action, grabbing the foam backseat of their police cruiser to use as a flotation device before jumping into the water. The officers were able to reach the man and eventually got him to shore where fire crews provided the man with first aid treatment. Energetic City

Three charged after stolen truck located
Two adults and one youth are facing charges following a Battlefords RCMP investigation into multiple complaints about a dark-coloured pickup truck. Reports indicated the occupants of the vehicle were in poseession of a firearm and stolen property. (…) A 17-year-old male youth is charged with two counts of failing to comply with an undertaking, resisting arrest and two counts of possession of property obtained by crime. Battlefords News-Optimist

RCMP warn Fort McMurray residents of CRA telephone scam

Fort McMurray residents are being warned to be aware of a phone scam where people are claiming to be from the Canada Revenue Agency (CRA). Wood Buffalo RCMP said they've received a few reports of residents in the region being targets of the "CRA scam," where the scammer tells the person they owe the CRA money and to pay in iTune gift cards or face arrest. Global News

Drayton Valley RCMP welcomes new sergeant
There is a new RCMP sergeant in town. In July, Erin Matthews replaced former Drayton Valley RCMP Sgt. Chris Delisle. Matthews, who has been working for the RCMP for 17 years, spent most of her time in Saskatchewan. "I spent the first 15 years in Saskatchewan and then I moved to Edson in 2014 and then just recently to Drayton Valley," she said. According to her, Drayton Valley is a "nice" place to live and work. "I am excited to be here. I really like it. It is clean and it's got lots to offer," she said. "With this line of work, we don't deal with everybody in the community, but I am getting involved in other aspects in the community and I am enjoying the work. The people I have dealt with so far are great." Drayton Valley Western Review

Purple to shed light on a dark topic in Chilliwack
That distinctive purple glow you'll be seeing this month is a declaration that domestic violence has no place in Chilliwack. The annual Purple Light Nights 2016 campaign kicks off Monday, Oct. 3 at the Chilliwack RCMP community policing office on Airport Road with a tree lighting ceremony at 6:30 p.m. "Domestic violence is a crime that often goes unreported," said Cpl. Mike Rail. "RCMP urges anyone who has knowledge of or suspects someone of being a victim of domestic violence, to report this crime to the police." (…) "Our goal is to increase awareness of domestic violence and the effect it has on children, families, and our community. Through the Purple Light Nights campaign we provide education to promote healthy relationships to youths and adults," said Darlene Wahlstrom, Victim Services coordinator for Chilliwack RCMP. Chilliwack Progress

Ontario review puts police oversight groups under scrutiny
Ontario's police oversight groups are themselves under scrutiny, as a provincially-appointed group travels to Sudbury to solicit input from citizens. Ontario's Special Investigations Unit, the Office of the Independent Police Review Director and the Ontario Civilian Police Commission are suffering from "inefficiencies due to overlap" said Danielle Robitaille, speaking for the Ontario Police Oversight Review, and these consultations hope to identify and recommend changes to the system. "We hear from community to community that there is a problem with these agencies in terms of overlap which creates confusion from members of the public in terms of where do they turn to," Robitaille said. "If they have a police complaint where do they go?" All three oversight agencies look into cases where there has been a complaint against police. They also investigate if police are involved in a death or serious injury involving a citizen. CBC News

Teen dies during police intervention in Cree community
A 19-year-old died Sunday night during an intervention with Chisasibi First Nations police in a Cree community in northern Quebec. Police responded to a call around 9:45 p.m. that claimed a person was outside a home with a gun. Police attempted to negotiate with the man. The Bureau des enquêtes indépendantes has called on the Sûreté du Québec to investigate. Investigators are expected to arrive mid-afternoon Monday. Chisasibi is a village on James Bay, about 1,400 kilometres north of Montreal. Montreal Gazette

Broadcast media / Médias télédiffusés

Les spécialistes ne savent pas encore quelle région sera choisies pour établir ce nouveau chapitre Hells Angels. Cet espace sera probablement dans le nord de la province parce que c'est un territoire qui a déjà été géré par des sympathisants des Hell's Angels s'inquiète la GRC du nouveau Brunswick qui dit qu'elle surveille de très près la situation. (Le Canal Nouvelles, 8h00)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Les drogues de synthèse augmentent en popularité
Le portrait du crime lié à la drogue change au pays : si le taux d'infractions visant le cannabis et la cocaïne a baissé ces dernières années, celui des drogues de synthèse, dont le dangereux «crystal meth», a augmenté, selon les plus récents chiffres de Statistique Canada. En ce qui concerne le cannabis, le taux d'infractions rapportées par la police mettant en cause cette drogue a fléchi de 15 % entre 2014 et 2015. Il s'agit d'une quatrième baisse annuelle consécutive. Le taux d'infractions rapportées liées à la cocaïne a aussi chuté de 7 % depuis 2014. En revanche, les taux d'infractions de possession, de trafic ou de production de «crystal meth» étaient en hausse de 25 %. Statistique Canada a également observé une croissance du taux lié à l'ecstasy (7 %) et aux autres drogues, telles que les médicaments d'ordonnance, le LSD et les «drogues du viol» (6 %). L'expression «drogues de synthèse» désigne des molécules chimiques concoctées en laboratoire, comme l'ecstasy et le fentanyl, par opposition aux substances qui proviennent de la nature, comme le cannabis. Le professeur Jean-Sébastien Fallu, professeur à l'École de psychoéducation de l'Université de Montréal, spécialisé en toxicomanie, a toutefois exprimé un doute sur le taux d'infractions calculé par Statistique Canada sur le «crystal meth» - une hausse de 25 %. Il est d'avis que la consommation du crystal meth est quand même limitée et croit que la statistique vise vraisemblablement plus la catégorie globale des métamphétamines, qui inclut le «crystal meth». Contactée de nouveau à ce sujet, Statistique Canada a toutefois confirmé sa donnée initiale. Presse Canadienne (Le Droit, 15, Quotidien)

Islamophobic 'feminism' doesn't help Muslim women
Time and tired time again, we have seen how the claim of standing up for Muslim women has served as a pretext for singling out Islam and Muslims for excoriation. This was the case in the recent furor over Toronto's Valley Park Middle School providing space for Muslim students to pray (in which girls and boys sat separately), and in the previous federal government's efforts to prohibit women in niqabs from becoming Canadian citizens. The castigation of Prime Minister Justin Trudeau for attending an Ottawa mosque on Eid ul-Adha is the latest in this string of manufactured controversies. Trudeau's recent visit to the mosque, where men and women pray in separate areas (but are mixed during other events), has been condemned as a betrayal of "feminism" and collusion with patriarchy. (…) According to Statistics Canada, "from 2010 to 2013, Muslim populations had the highest percentage of hate crime victims who were female (47 per cent)." Women wearing the hijab and the niqab have been physically attacked in cities across Canada and the United States. A few weeks ago, two Muslim women were assaulted while strolling their babies in Brooklyn; their assailant punched one of the women in the face, tried to rip off their headscarves, and yelled "Get the f— out of America, b——s." In June, a Muslim woman was punched, spat on and had her hijab pulled while shopping with her four-month-old son in London, Ont. Ottawa Citizen

Government must act to end racism in children's aid system: Editorial
A new report has found a children's aid system that is riddled with racism. The Ontario government must implement changes needed to keep families from being unnecessarily ripped apart. The Ontario government now has even more evidence, if it needed it, that Ontario's children's aid system is plagued by problems of race. It's high time for it to act. The evidence is detailed in a two-volume report from the Ontario Association of Children's Aid Societies that backs up what the Star reported as long as two years ago: four in 10 children in the care of the Children's Aid Society of Toronto are black in a city where only 8 per cent of children are. Worse, the problem is not just in Toronto, but throughout the province. (…)But it will take government funding to support the recommendations that are aimed at ending racism, ignorance about poverty and cultural misunderstandings. And it will take more financial support to provide parents with the services they need, whether it's to get back on their feet financially or to learn about what disciplinary measures are acceptable in Canada. The Star

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Drogue au volant: un sénateur en faveur du dépistage chez les automobilistes
Avant de légaliser la marijuana, le gouvernement Trudeau devrait donner de meilleurs outils aux policiers pour combattre un fléau qui prend de l'ampleur au pays : la conduite avec les facultés affaiblies par la drogue. C'est du moins ce que soutient le sénateur conservateur Claude Carignan, qui entend déposer un projet de loi au Sénat demain afin de modifier le Code criminel de manière à ce que les policiers aient le pouvoir d'exiger un test de dépistage aux automobilistes dont la conduite est erratique en utilisant un appareil qui analyse un échantillon de salive. Cette méthode non invasive pour déceler la présence de drogue chez un conducteur est déjà utilisée dans certains pays, comme l'Australie, l'Allemagne, la France, la Belgique, l'Espagne, l'Italie et le Royaume-Uni, de même que dans certains États américains. Selon l'organisation MADD (Mothers Against Drunk Driving), la drogue était présente dans l'organisme du conducteur lors de 614 morts sur la route au pays, selon des données de 2012, tandis qu'on détectait de l'alcool chez le conducteur pour 476 morts de la route. « Le projet de loi du sénateur Carignan modifierait le Code criminel afin de donner aux policiers les outils dont ils ont besoin pour repérer sur la route les conducteurs aux facultés affaiblies par la drogue à l'aide d'un appareil de détection utilisant une méthode non invasive qui analyse la salive. Cet appareil décèlerait rapidement la présence de certaines drogues illicites », a indiqué une source conservatrice. La Presse

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

'It's not over' for U of T student released on bail in Bangladesh, brother says
A University of Toronto student detained in Bangladesh for weeks in connection with a terrorist attack has been released on bail, his family confirmed. Tahmid Hasib Khan, 22, is healthy, safe and living under the supervision of his parents in the capital city of Dhaka, said his brother Talha Khan. Tahmid Khan, a permanent resident of Canada, was arrested without charge on August 4. Bangladeshi police allege Khan was involved in a July 1 terrorist attack on the Holey Artisan Bakery in Dhaka, in which gunmen killed 20 people and took several others hostage. "He's the furthest thing away from all that," said Talha Khan of his younger brother. "He's the kind of person who has enough faith in the power structures of the world that are already there. (He's) not trying to resurrect the caliphate or something." But the ordeal "is not over," for Tahmid, Talha said. At the time of the attack, Tahmid was in Dhaka visiting his parents for the Muslim holiday of Eid al-Fitr, Talha said. Tahmid was then scheduled to fly to Nepal, where he an internship lined up with UNICEF. Khan is confirmed to have been in the restaurant at the time of the terrorist attack, but his family has maintained that he was merely a customer, a survivor of the attack, not a perpetrator. Toronto Star

U.S.-Led NATO in Spotlight as Europe Pushes Joint Army, Defenses
European nations are pressing ahead with plans for joint defenses and military cooperation, raising fears that U.S.-led NATO could be undermined. With Britain poised to quit the European Union and Donald Trump raising doubts over NATO, France and Germany have been spearheading moves to boost Europe's capacity to run its own security operations. oint development of assets such as helicopters and drones, stronger defenses against state-sponsored computer hackers and the expansion of peace-

keeping abroad were among the proposals unveiled last week at a conference of European ministers. The plans, which could be green-lighted as early as December, come after EU President Jean-Claude Juncker called for the construction of a new EU military headquarters that would eventually control a joint EU army comprised of troops from member states. A common military force would be "in complement to NATO," he insisted in a speech last month, adding: "More defense in Europe doesn't mean less transatlantic solidarity." NBC News

INTERNATIONAL

At least 2 killed as Hurricane Matthew starts lashing Haiti, Jamaica
Heavy rains from the outer bands of Hurricane Matthew drenched Jamaica and Haiti on Monday, flooding streets and sending many people to emergency shelters as the Category 4 storm approached the two countries. Two deaths were reported in Haiti, bringing the total for the storm to at least four. Matthew had sustained winds of 140 mph as it moved north, up from 130 mph earlier in the day. The center was expected to pass just east of Jamaica and near or over the southwestern tip of Haiti early Tuesday before heading to eastern Cuba, the U.S. National Hurricane Center in Miami said. "We are looking at a dangerous hurricane that is heading into the vicinity of western Haiti and eastern Cuba," said Richard Pasch, a senior hurricane specialist with the center. "People who are impacted by things like flooding and mudslides hopefully would get out and relocate because that's where we have seen loss of life in the past." Many were taking that advice. In Jamaica, more than 700 people packed shelters in the eastern parish of St. Thomas and the Salvation Army said there were about 200 people at its shelters in Kingston as it put out a call for mattresses and cots. Many streets flooded throughout the country's southeast. Associated Press (Fox News)

Morocco says arrests 10 suspected female ISIS militants
Morocco has dismantled a suspected ISIS militant cell and arrested 10 women believed to be planning attacks in the North African kingdom, the Interior Ministry said on Monday. It was the latest in a series of militant cells Morocco says it has broken up, but it is the first time authorities have arrested a group of female suspects. An Interior Ministry statement said the cell was operating in several regions including the cities of Kenitra and Tangier. It said the cell members reflected an ISIS effort to integrate female militants for attacks in the kingdom and they were inspired by the brother of one of them who was involved in bombings in Iraq earlier this year. Al Arabiya

Inside the mind of an honour killer in Pakistan: 'It was all I could think about. I had to kill her'
For two months, over the thunder of machines at the steel mill, the men taunted Mubeen Rajhu about his sister. Even now, they laugh at how easy it was to make him lose his temper. Some people had seen Tasleem in their Lahore slum with a Christian man. She was 18, a good Muslim girl, out in public with a man. Even though the man had converted to Islam out of love for her, this couldn't be allowed. K.M. Chaudary / Associated Press Mubeen Rajhu couldn't stand the teasing, accusations and whispers from co-workers and neighbors that his sister was having an affair and with a Christian "Some guys got to know that his sister was having a relationship," says Ali Raza, a co-worker at the mill. "They would say: 'Can't you do anything? What is the matter with you? You are not a man.'" Raza can barely contain a smile as he talks about the hours spent needling Rajhu. "He used to tell us, 'If you don't stop, I will kill myself. Stop!"' Raza says. He raises his voice to compete with the sounds of the coal-powered mill, and workers blackened by its dust gather to listen. They too smile. A few laugh at the memory of Rajhu's outbursts. (…) On the seventh day, he retrieved the pistol from where he had hidden it and walked up to his sister and with one bullet to the head, he killed her. Associated Press (National Post)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

RalphGoodale
Mon article @nationalpost sur C22: loi qui protègera nos droits&sécurité-renforçant la reddition de comptes http://ow.ly/eMhF304Ny0f

fullcomment
Ralph Goodale: Bill C-22 is designed to protect Canadians' rights, and defend their security http://ow.ly/ABL55054k10

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

CBCPEI
Canada plays catchup as wireless providers create emergency alerts for cellphones http://buff.ly/2dDEywV #pei

HealthCanada
First responders and health service partners sharpen their skills during emergency disaster training in Hodgson, Manitoba September 27.

okrescue
Search & Rescue Kept Busy COSAR called to two concurrent searches on Sunday Kelowna, BC – Oct 2, 2016 – Sunday... http://fb.me/WV9fBnzA

northwestel
Update: Services in all satellite-served Northern communities have now been restored. http://www.nwtel.ca/about-us/corporate-and-media/service-and-maintenance-updates ...

NATIONAL SECURITY / SÉCURITÉ NATIONALE

JimBronskill
Spies use C-51 to gather intelligence from Canadians detained overseas, says newly declassified memo http://ctv.news/WVjazPh #cdnpoli #hw

ArarMaher
RT @AndrewMitrovica: The constitutional lawyer who probed the horror that @ArarMaher endured says #C51 should be repealed. My latest: https://t.co/yUxYFakoXm

althiaraj
CSIS using C-51 powers to spy on Canadians in foreign prisons #cdnpoli http://www.huffingtonpost.ca/2016/10/03/spies-use-c-51-to-gather-intelligence-from-canadians-detained-overseas_n_12309254.html?ncid=engmodushpmg00000004 ... via @HuffPostCanada

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

fullcomment
Spencer McKay: The illusion of participatory democracy - A summer of seemingly endless town-hall meetings on va... https://t.co/EPZnRZ3fqT

StephanieCarvin
This Thursday! @uOttawaCIPS event with @cforcese, myself 3 MPs talking about Parliamentary Intelligence C

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

CyberExaminer
#cybersecurity Over 400 instances of Dresscode malware found on Google Play store, say researchers http://dfi.io/MNXWSy #infosec

GetCyberSafe

October is Cyber Security Awareness Month! Help promote **#CSAM** by using our toolkit: http://www.getcybersafe.gc.ca/cnt/rsrcs/csam-tlkt-en.aspx ...

LAW ENFORCEMENT / APPLICATION DE LA LOI

RadioCanadaInfo
Les Hells Angels de retour dans les Maritimes http://bit.ly/2doFJBf

nationalpost
Missing Japanese woman found dead in Vancouver heritage mansion weeks after she disappeared http://natpo.st/2dpZKXU

CGCanBoston
Voyez Le Carrousel de la @grcrcmppolice au Topsfield Fair au Massachusetts! http://ow.ly/W0kn304NPKh

RoyalCdnLegion
The Legion honours Canada's military & RCMP families & recognizes the contributions they bring to our military heritage. #NationalFamilyWeek

CochraneEagle
New #Cochrane #RCMP inspector up for Order of Merit http://ow.ly/q3B2304GQf6

OFOVC_BOFVAC
Visit @rcmpgrcpolice to learn about stopping child abuse http://bit.ly/1TSMXZA

sdpuddicombe
#Cbcns Halifax gun amnesty

cgrcmp
You'll be this happy too when you're #CyberAware

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

CSC_SCC_en
View the latest Independent Review Committee report and action plan on deaths in custody #CorrectionsCanada http://ow.ly/f5vF304NfK3

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

OPP_Aboriginal
PLT, CBSA, & SSMPS assisted organizers Donna Pangowish and Alison Recollet in their walk to bring awareness to Human Trafficking #Awareness

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

davidakin
#NewsNOW on Parliament Hill — Aboriginal leaders hold vigil for murdered and missing aboriginal women.

AmnestyNow
Attend a vigil to honour missing and murdered Indigenous women tomorrow #NoMoreStolenSisters #MMIW >> http://amn.st/6019BhVtV

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

MichelleLamarch

Le sénateur Carignan veut modifier le code criminel pour aider les policiers a détecter les fac. affaiblies par la drogue. #tvanouvelles

CBCPolitics
Canada faces choice on international drug treaties over legalized pot http://www.cbc.ca/news/politics/marijuana-legalization-pot-anti-drug-treaties-1.3780661?cmp=rss&utm_source=twitterfeed&utm_medium=twitter … #cdnpoli #hw

CBCToronto
High drivers in Ontario now will temporarily lose their licenses as new legislation takes … http://ift.tt/2dDz6dh

OTHER / AUTRE

NBCNewsWorld
Europe wants its own joint army, so what happens to NATO? https://t.co/EWWmtcr4uL

INTERNATIONAL

AP_Politics
BREAKING: State Department: US suspends bilateral contacts with Russia over Syria.

Independent
Colombia off the list of Nobel Peace Prize contenders after Farc conflict deal defeated in referendum https://t.co/RuiZc1AJl5

ReutersUS
Shootings at U.S. colleges deadlier and more frequent, report finds https://t.co/XwxQmBQH5X

MaxAbrahms
Seven of the terrorists involved in the Paris attacks had slipped through Hungary's borders while posing as migrants https://t.co/QfxjhYx2s1

AlArabiya_Eng
#Morocco says arrests 10 suspected female ISIS militants https://t.co/D1hlPHRkpo

globeandmail
Hurricane Matthew's threat to Haiti grows; some resist evacuation http://trib.al/cv9Qu79

AJENews
Super Typhoon Chaba heads towards Japan with damaging winds and flooding rains http://aje.io/7px9

ReutersUK
Taliban fighters enter northern Afghan city of Kunduz: http://reut.rs/2doWQ6g

abcnews
#Russia's Vladimir Putin orders suspension of weapons-grade plutonium disposal program with 'unfriendly' #US https://t.co/8x1iGmv6Dy

cnni
At least 52 are dead in Ethiopia after a stampede at a holy festival: http://cnn.it/2dBZbZv

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

Today's News / Actualités
October 5, 2016 / le 5 octobre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

TOP STORIES / MANCHETTES

Canada's National Security Consultation I: Digital Anonymity & Subscriber Identification Revisited… Yet Again
An opinion piece states, "Last month, Public Safety Canada followed through on commitments to review and consult on Canada's national security framework. The process reviews powers that were passed into

law following the passage of Bill C-51, Canada's recent controversial anti-terrorism overhaul, as well as invite a broader debate about Canada's security apparatus. While many consultation processes have explored expansions of Canada's national security framework, the current consultation constitutes the first modern day attempt to explore Canada's national security excesses and deficiencies. Unfortunately, the framing of the consultation demonstrates minimal direct regard for privacy and civil liberties because it is primarily preoccupied with defending the existing security framework while introducing a range of additional intrusive powers..." CIPPIC

The Canadian Government's Plan to Sell New Spying Powers to Citizens
Canada's government is taking a forum for citizens to sound off about its spying powers and flipping it into an opportunity to sell Canadians on new and overbroad police capabilities, according to a new watchdog report. In September, Trudeau's Liberals made good on a promise to open a public consultation on national security and released two documents, a green paper and a background document, explaining the issues at stake to Canadians at a time when the government is ramping up its efforts to thwart domestic terrorists. These included hot topics such as the difficulties police face when dealing with encrypted devices and issues surrounding data retention. However, according to the watchdog report, the government's framing of the issues is selling Canadians on a police power that has been shot down again and again by the courts and the public: warrantless access to subscriber information from telecom companies. "Successive federal governments have sought to legislatively enshrine a state power to access subscriber identification data from telecommunications companies," Citizen Lab researcher Christopher Parsons and Canadian Internet Policy and Public Interest Clinic staff lawyer Tamir Israel write in their report. "Such legislative initiatives would have facilitated access to such data on an indiscriminate basis and without any judicial authorization or control." "All of these attempts have proven controversial and each has fallen in the face of public resistance," they continue. In 2014, the Supreme Court of Canada ruled that accessing subscriber information without a warrant constitutes an illegal search. In its green paper, the government describes subscriber information as being akin to a phone book. However, subscriber information includes IP addresses, name, home address, phone number, email address, and mobile devices' IMSI number—much more information than is contained in your average phone book. "Our laws on how information can be properly collected and then used in court as evidence were mostly written before the rapid pace of new technology became a consideration," the government's green paper states. Now, police worry about "slow and inconsistent access to basic subscriber information to help identify who was using a particular communications service at a particular time," the report states. Motherboard; Boing Boing

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

UPDATE: Hurricane Matthew could miss New Brunswick entirely
The latest weather prediction models suggest New Brunswick will be spared from Hurricane Matthew, but people should still prepare for the worst, says a forecaster with the Canadian Hurricane Centre. "Late last night, the models started to produce solutions that push the trajectory more eastward on a track south of the Maritimes," Jim Murtha said on Wednesday morning. But trends change, he said. "There is still a scenario where this storm could move towards the Maritimes, so we're not completely rejecting that consideration at this point," said Murtha. "We're still advising the public to pay attention to the forecast to see how this thing unfolds as Matthew moves northwards." CBC News

Tragédie de Lac-Mégantic : les accusés de retour en cour aujourd'hui
Les accusés impliqués dans la tragédie ferroviaire de Lac-Mégantic survenu le 6 juillet 2013 sont de retour en Cour, mercredi. La poursuite déposera son cahier de procès, rassemblant les preuves et souhaite fixer les dates de procès. Des accusations fédérales ont été portées contre l'entreprise Montreal, Maine & Atlantic (MMA) Canada, MMA Railways, et sept personnes en vertu de la Loi sur la sécurité ferroviaire et de la Loi sur les pêches. L'enquête menée par Transports Canada a conclu que le nombre de freins à main serrés pour immobiliser le train était insuffisant et que la résistance des freins à main au déplacement du train n'avait pas été vérifiée convenablement. L'audition est prévue à 9 h 30. Radio Canada

City of Saskatoon reporting multiple power outages; Environment Canada says storm will continue until Thursday
Saskatoon's first winter storm of the season has knocked out power in several Saskatoon neighbourhoods and Environment Canada says there is more snow is store. "Gusty northerly winds will also continue today and visibilities may be reduced at times in snow and blowing snow," says a snowfall warning issued by Environment Canada Wednesday morning. The warning, which predicts 10 to 15 centimetres of snow before the storm tapers off Thursday, is in place for a swath of Saskatchewan stretching from Southwest to East-Central. The City of Saskatoon's online service alerts page lists outages Wednesday morning in Sutherland, Sutherland Industrial, Forest Grove, Grosvesnor Park, Varsity View, Caswell Hill, Riversdale, Pleasant Hill, Westmount and City Park. Other neighbourhoods lost power overnight but have since had it restored. Star Phoenix; CBC News

Fort McMurray's Waterways subdivision given green light to rebuild
The Alberta government has assured the residents of a fire-ravaged community in Fort McMurray they can rebuild even though the subdivision sits on a floodplain. "This clears the path in some respects of people looking for some answers," Mayor Melissa Blake said Tuesday. The permission from the province was required because it will soon pass legislation preventing any community from building in zones prone to flooding. The Alberta government told the municipality it will provide disaster recovery funding in case of a future flood. CBC News

Province, emergency personnel to host mock disaster Wednesday
A major train disaster is being simulated in Truro on Wednesday. The mock disaster will test the health system response at the former Colchester Regional Hospital on Willow Street from 10 a.m. until noon. The simulation, hosted by the Department of Health and Wellness, will involve emergency personnel, including police, firefighters and paramedics. Truro Daily

Enterovirus is back: Cases of EV-D68 reported across Canada, U.S.
Exactly two years ago, kids turned up in hospital with cold-like symptoms and struggling to breathe across Canada and the U.S. as enterovirus swept the continent. Now, in 2016, the rare respiratory illness has resurfaced after disappearing last year. So far, cases have been reported in British Columbia, Alberta and Ontario, with experts anticipating escalating numbers. "The numbers are low so far but we can expect more infections to occur through the fall and early winter period," Dr. Danuta Skowronki, an epidemiologist with the B.C. Centre for Disease Control, said in a statement (…) It has also reappeared in the U.S. The Centers for Disease Control and Prevention said it's seen a rise in cases, too. Global News

RCMP officer from Yarmouth assists in resourceful rescue
Peace River RCMP officers use backseat of cruiser as flotation tool to rescue drowning man. Quick-thinking action by officers with the Peace River, Alberta, detachment of the RCMP helped save the life of a drowning man on Oct. 1. Yarmouth-born Constable Brandon Goudey was patrolling downtown Peace River with Cst. Tim Stevens and Cst. Stephanie Gratton when they saw EMS and the Peace River Fire Department (PRFD) driving with their emergency lights flashing near the dyke that runs alongside the river. The Mounties had not yet been dispatched to any calls so they decided to follow in case they could provide assistance. As they approached the River Front Park downtown, detachment dispatch notified them that EMS and PRFD were requesting assistance with a man in distress in the river. Constables Goudey and Gratton followed the PRFD rapid response truck to a boat launch that provides access to the Peace River, in hopes of sighting the man. Yarmouth County Vanguard

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Canada's National Security Consultation I: Digital Anonymity & Subscriber Identification Revisited… Yet Again
An opinion piece states, "Last month, Public Safety Canada followed through on commitments to review and consult on Canada's national security framework. The process reviews powers that were passed into law following the passage of Bill C-51, Canada's recent controversial anti-terrorism overhaul, as well as invite a broader debate about Canada's security apparatus. While many consultation processes have

explored expansions of Canada's national security framework, the current consultation constitutes the first modern day attempt to explore Canada's national security excesses and deficiencies. Unfortunately, the framing of the consultation demonstrates minimal direct regard for privacy and civil liberties because it is primarily preoccupied with defending the existing security framework while introducing a range of additional intrusive powers…" CIPPIC

The Canadian Government's Plan to Sell New Spying Powers to Citizens
Canada's government is taking a forum for citizens to sound off about its spying powers and flipping it into an opportunity to sell Canadians on new and overbroad police capabilities, according to a new watchdog report. In September, Trudeau's Liberals made good on a promise to open a public consultation on national security and released two documents, a green paper and a background document, explaining the issues at stake to Canadians at a time when the government is ramping up its efforts to thwart domestic terrorists. These included hot topics such as the difficulties police face when dealing with encrypted devices and issues surrounding data retention. However, according to the watchdog report, the government's framing of the issues is selling Canadians on a police power that has been shot down again and again by the courts and the public: warrantless access to subscriber information from telecom companies. "Successive federal governments have sought to legislatively enshrine a state power to access subscriber identification data from telecommunications companies," Citizen Lab researcher Christopher Parsons and Canadian Internet Policy and Public Interest Clinic staff lawyer Tamir Israel write in their report. "Such legislative initiatives would have facilitated access to such data on an indiscriminate basis and without any judicial authorization or control." "All of these attempts have proven controversial and each has fallen in the face of public resistance," they continue. In 2014, the Supreme Court of Canada ruled that accessing subscriber information without a warrant constitutes an illegal search. In its green paper, the government describes subscriber information as being akin to a phone book. However, subscriber information includes IP addresses, name, home address, phone number, email address, and mobile devices' IMSI number—much more information than is contained in your average phone book. "Our laws on how information can be properly collected and then used in court as evidence were mostly written before the rapid pace of new technology became a consideration," the government's green paper states. Now, police worry about "slow and inconsistent access to basic subscriber information to help identify who was using a particular communications service at a particular time," the report states. Motherboard; Boing Boing

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

NIL

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

After Yahoo Revelations, Microsoft Swears It Didn't Spy on Users for the NSA
Microsoft was one of the first tech companies to deny involvement in spying programs secretly launched by the NSA and the US government and carried by Yahoo, according to recent revelations. The Redmond-based tech giant provided a very short statement to explain that the firm has never been involved in spying programs like the ones that Yahoo might have been part of, but the company refused to provide any other details on this. Softpedia

NSA contractor arrested over 'stolen secret code used to hack Russia'
The FBI has secretly arrested a National Security Agency (NSA) contractor suspected of stealing highly classified computer codes used to hack the computer systems of foreign governments including Russia and China, raising fears of another embarrassing intelligence leak to rival the Edward Snowden affair, the New York Times reported on Wednesday (…)The contractor in this case, who was reportedly arrested "in recent weeks", is suspected of stealing the NSA's "source code", used to break into the computer networks of rival powers such as Russia, China, Iran and North Korea. Independent (UK); New York Times

Feds subpoena, gag encrypted chat firm Open Whisper Systems
Open Whisper Systems, the brainchild of cryptographer Moxie Marlinspike, has published the results of an unsealed subpoena set against the company -- and how little US law enforcement received for their trouble. The company is the developer of encrypted messaging application Signal, recommended by NSA whistleblower Edward Snowden, of which the technology is also used in other services including WhatsApp, Facebook Messenger and Google Allo. According to court documents unsealed last week, OWS was forced to hand over user data as part of a federal investigation, but the firm's ethos gave law enforcement very little to work with. ZDNet; Threat Post; New York Times

Facebook rolls out opt-in encryption for 'secret' Messenger chats
As of today, all of Facebook's 900 million Messenger users should be able to choose to have specific chat threads end-to-end encrypted, protecting a message from all eyes except the sender and recipient. Called Secret Conversations, the feature also allows users to set messages to self-destruct anywhere between five seconds to one day. Once a Secret Conversation is initiated, Facebook's app says that the conversation has been "encrypted from one device to the other". Encrypted conversations can be started from the home page by tapping a new message and then tapping the Secret button on the top right corner of the page, followed by the contact you want to start a secret chat with. The new privacy feature follows the completion of Facebook's end-to-end encryption rollout for the billion users of its other chat app, WhatsApp, earlier this year. ZDNet

Three-quarters of Firms Hit by DDoS
Nearly three-quarters of global firms have suffered a DDoS attack over the past 12 months with half losing $100,000 or more each hour during peak periods, according to the latest study from Neustar. The global DDoS mitigation provider polled just over 1,000 C-suite execs to compile its October 2016 Worldwide DDoS Attacks & Protection Report. Of those who had experienced an attack, 85% said they were subject to multiple blasts, with the largest number (29%) suffering attacks between 2-5 times. Although 49% claimed they lost $100,000 per hour during peak periods as a result of an attack, the figure went as high as $250,000 or more for a third of respondents. Time is money, but unfortunately 71% of respondents said they took an hour or more to detect attacks and 72% an additional hour to respond. More worrying still for organizations is the fact that DDoS attacks appear to be increasingly used in conjunction with efforts to steal information, infect systems with ransomware or other cyberattacks – possibly as a smokescreen to distract IT teams. Infosecurity Magazine

Facebook Marketplace launches, selling guns, drugs and baby hedgehogs
Facebook's Marketplace has immediately been flooded with people selling guns, drugs and baby hedgehogs. The company has been forced to apologise after its brand new feature – intended to let people sell things in the same way as they would through Ebay or Craiglist – has already been flooded with illegal items, those that break rules, and others that are just odd. As well as offering illegal items like drugs, some users appeared to be selling things that are banned by Facebook's own terms, like snakes and hedgehogs. Independent (UK)

LAW ENFORCEMENT / APPLICATION DE LA LOI

Female youth behind Instagram kidnapping threats in Fort McMurray, RCMP say
A female youth from Fort McMurray has been identified as the person responsible for sending kidnapping threats via Instagram to students at two local high schools. No charges have been laid but the investigation is continuing, Wood Buffalo RCMP said in a news release Wednesday. Police said they have concluded interviewing four people who were arrested early Tuesday at a home in Fort McMurray. All four have been released from custody. Police started their investigation after receiving a complaint at 10:15 p.m. Monday that kidnapping threats had been uttered using Instagram's messaging feature. Investigators tracked down an I.P. (Internet Protocol) address which led them to a home in Fort McMurray. Police went to the home at 5 a.m. Tuesday and arrested four people from one family. CBC News

Outlaws Motorcycle Club gone from Gander, says RCMP

Police in Gander are praising the community's approach for helping discourage a chapter of the Outlaws Motorcycle Club to the point it has left town altogether. The bikers set up shop in a clubhouse on Gander's main drag in 2013, but they now "cease to exist" in the community, according to RCMP Staff Sgt. Roger Flynn. "I think it was a good example of how not just the police, but the community, can work together," said Flynn. "We had a lot of co-operation from the town of Gander to be able to manage that issue." Watch this Here & Now report from 2013 on the Outlaws Motorcycle Club. When the club's lease on the Airport Boulevard space ran out around May of 2015, they went door-to-door in search of a new location but no one would rent to the club. Flynn said it's an example of community policing at work. "People have to learn it's a community concern. Gone are the days when... it's just a policing issue," said Flynn. "It's a community issue." Last week raids in St. John's under Project Bombard made headlines across the province, as police laid a slew of charges against members of the Vikings Motorcycle Club, an affiliate of the Hells Angels. CBC News

'Overdose epidemic killing two per day'

An overdose death can hit any family. That will be the message Dr. Ingrid Tyler brings to tonight's community forum on fentanyl, taking place at Westview secondary. Tyler is a medical health officer with Fraser Health, and will talk about the epidemiology of overdose deaths in B.C. – the epidemic that has been caused by fentanyl. "Overdoses can affect everyone," said Tyler, whether it be young people experimenting with drugs, or adults who use drugs socially. Every drug bought in the street could be contaminated with fentanyl, she said. "There have been some high-profile cases that have not involved street-entrenched individuals." There have been 488 overdose deaths from the start of the year until the end of August, and that is a 60-per-cent increase over last year. There have been 20 in that period in Maple Ridge. "You can think of this as two deaths per day," she said. More than 60 per cent of the drug deaths involved fentanyl (…) The forum will run from 7-8:30 p.m. in the multipurpose room at Westview. It is being organized by Fraser Health, School District No. 42, Alouette Addictions, Ridge Meadows RCMP and the city. Maple Ridge News

What is up with this 'creepy clown' thing coming to Nova Scotia?

Alleged "creepy clown" sightings and hoaxes have been reported on social media across North America since August. Most have turned out to be pranks. According to the New York Times, as of Sept. 28, there were 12 arrests across the U.S. connected to clown hoaxes, including for alleged threats to individuals and schools. In the NYT piece, psychology cited "mass hysteria" and a desire to be part of a news event as possible fuel for the hoax. (…) Nova Scotia RCMP spokeswoman Cpl. Jennifer Clarke said Oct. 5 the force "is aware of the group posing as clowns and making threats on social media." "We have received complaints from concerned citizens regarding these people. We are taking these complaints seriously. Based on an evaluation of information provided, the RCMP may initiate an investigation." Annapolis County Spectator

Bomb threat cancels classes today for Baddeck Academy

It was a bomb threat that led to the cancellation of classes today at Baddeck Academy. The Cape Breton-Victoria Regional School Board announced the cancellation early this morning on social media through its Twitter account. An RCMP spokesperson confirmed a bomb threat as the reason for the cancellation. Officers were on scene this morning but have since left the scene. Cape Breton Post

Government will 'act swiftly' on e-gaming report

The P.E.I. government will take Wednesday's auditor general report as a reminder that transparency and accountability must be at the core of its decisions and actions, says Premier Wade MacLauchlan. Auditor General Jane MacAdam's report on the province's failed effort to establish P.E.I. as an e-gaming centre found "numerous examples of non-compliance with legislation, policies and controls."(…) Provincial NDP Leader Mike Redmond said he sent a copy of the report to the commercial crime division of the RCMP. "This is no longer an internal review of government affairs, this requires a thorough police investigation and with a view to charges being laid," said Redmond in a news release. Redmond said every government member that was in cabinet at the time needs to be held responsible. That would include several current members of cabinet. CBC News

Teens terrorize with pistols

A Kelowna mother is sounding the alarm after her 11-year-old son was chased home, terrorized and pelted with airsoft pistols. According to RCMP, a youth was confronted and allegedly assaulted by several other teens armed with apparent airsoft pistols in the area of Verna Court and Southview Avenue in Glenmore Monday evening at about 6 p.m. "The 11-year-old youth sustained minor injuries as a result of being shot at with the airsoft pistols," said Const. Jesse O'Donaghey. "The youth later reported the incident to his guardians, who in turn reported the incident to the RCMP." The mom, who asked to stay anonymous for her son's sake, is concerned about the safety of children and small pets in the area. She said the group of about five to seven teens, approximately 15 years old, terrorized her son. "There are several kids that hang out in that area, there are small pets. If they are targeting kids, they could be targeting pets," she said. Castanet

At large high-risk sex offenders back in custody: police
Two high-risk sex offenders, at large since July, are back in police custody, RCMP said Wednesday. The Manitoba High Risk Sex Offender Unit put out a public call for help in finding the two men in early August. Police said Martin Patrick didn't return to his approved residence on July 6, and was unlawfully at large. Patrick turned himself into police on Sept. 24, officials said. Meanwhile, Walter Francis didn't return to his approved residence on June 22 and was unlawfully at large. Police said Francis was found on Long Plain First Nation on Sept. 13. He was arrested without incident. CTV News

Broadcast Media / Médias télédiffusés:

Radio-Canada a fait une entrevue avec Éric Grandbois, un policier de la GRC. Grandbois a été déployé sur une mission des Nations unies pour la stabilisation en Haïti. Il a expliqué l'état de la situation actuelle en Haïti. (RDI, 2h30)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Collins Bay pen medium security unit locked down
October 05, 2016 11:42 am - Another lock down is in place at Collins Bay Institution in Kingston. Correctional Services locked down the medium security unit of the prison at about 7 p.m. Tuesday. The move was necessary for staff to conduct an exceptional search of the cells. Correctional Services has not said what prompted the lock down or what guards are searching for. Regularly scheduled visits to Collins Bay could be affected. Anyone who has planned a visit should contact the prison directly. CKWS (Big 963)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Failure to protect indigenous children in care perpetuates cycle of abuse
"Groomed for a lifetime of victimization," says Mary Ellen Turpel-Lafond. Too often, that is the tragic fate of kids in a child-welfare system that is supposed to protect them. Those who are victimized – abused sexually and otherwise – are most likely to be indigenous girls. But children with disabilities, mental illnesses and substance-abuse issues are also at higher risk. (…) The raw numbers are shocking – 145 reports of sexual violence against 121 children over a four-year period just in British Columbia – but the circumstances even more so, with foster children abused by foster fathers, foster children preying on younger ones and sexual abuse in group homes, not to mention by family members, casual acquaintances and strangers. Two in every three of the victims of sexual abuse disclosed between 2011 and 2014 were indigenous girls, even though they represented only one in four children in care in British Columbia. The fact that indigenous girls are four times as likely to be victims of abuse as non-indigenous girls – even when they are supposed to be in a safe space – is as shameful as it is unsurprising. Globe and Mail

'Gun culture' sounds like an excuse to us

An editorial piece states, "After three years of record-level shootings, Ottawa must ask itself, what kind of city do we want to be? How safe a city can we reasonably expect to be? Maybe the answer is that gun violence in any growing city is inevitable and we'll just have to be OK with guns going off. Maybe we have to accept the inevitable spillover from the U.S. Maybe we can blame some sort of nebulous "gun culture" that isn't ever defined. Or ... maybe we can ask hard questions about why the police don't seem to be making inroads on gun crime. Maybe we need to stop making excuses and resolve to get guns off the street." Postmedia Network (Ottawa Sun)

'You all have stories': Panel laments drugged drinks at UPEI
Students at the University of Prince Edward Island are having their drinks drugged, and everyone has to work together to deal with that reality, a panel told a meeting of students and staff Tuesday evening. "We always are optimistic. We hope we're not going to be dealing with this, but we do realize the reality that this can and does happen," said Shannon Fenelon, residence life coordinator at UPEI. One of the themes of the evening was the lack of official reports. That could be due to shame, or just uncertainty about what happened due to memory loss. CBC News

Case adjourned for teens accused of sharing intimate images without consent
The case of a group of Nova Scotia teens charged with sharing intimate images of more than 20 underage women has been adjourned until later this month. Judge Timothy Landry put the unusual matter over to Oct. 19 to allow lawyers time to receive more of the disclosure, which includes thousands of pages of evidence from several electronic devices that were seized following a year-long investigation. Two 18-year-olds and four 15-year-olds are facing charges of distributing intimate images without consent and possessing and distributing child pornography (…)The case is one of the first in Canada that involves federal anti-cyberbullying legislation introduced in late 2013 after the high-profile death of Nova Scotia teen Rehtaeh Parsons. Canadian Press (CTV News)

'Think about the future': Kids face up to the dangers of sexting
In a world where sexting — digital flirting — can create devastating personal and and legal problems, Grade 4 students in Nova Scotia are learning how to stay safe online. Like many teachers and school boards across Canada, educators at Bluenose Academy in Lunenburg are making online safety a priority (…)Concern about the dangers young people can encounter while sexting is growing. Some of it focuses on the nearby community of Bridgewater, where six teenage boys are scheduled to appear in court Wednesday on child pornography charges as well as charges of sharing intimate images without consent. They were arrested after pictures of more than 20 teenage girls were allegedly shared in a Dropbox account without the girls' knowledge (…) Canadian studies say kids as young as nine have sent explicit images of themselves. And half of older high school students say they've sent or received an intimate image. CBC News

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Canada Slammed for 'Lack of Progress' on Inquiry into Missing and Murdered Indigenous Women
A Indigenous women's advocacy group is demanding more transparency and calling out the government for what they see as a "lack of progress" in Canada's national inquiry into missing and murdered indigenous women. The condemnation comes a day after Prime Minister Justin Trudeau stood on the steps of Parliament and denounced Canada for repaying Indigenous people with "neglect" and "indifference" during a vigil honouring Inuit artist Annie Pootoogook, whose body was found in an Ottawa river two weeks ago. In a press release Wednesday, the Native Women's Association of Canada slammed the government for a lack of communication and called for easily accessible information on office locations, how to reach commissioners and their staff, how members of the public can get involved, as well as a straightforward website. "We are very disappointed to see that over two months into the two-year Inquiry mandate, no visible progress has been made," said President Francyne Joe in a press release. "Family members, loved ones have been waiting for decades to be heard. We recognize that it is a big task to start a National Inquiry but the lack of communication has been disappointing and worrying."

A 2014 RCMP report found 1,181 Aboriginal women have gone missing or been murdered in Canada between 1980 to 2012, although Carolyn Bennett, the minister of Indigenous affairs, has said the true figure is "way bigger." VICE News; Globe and Mail

Confronting the crisis of violence against Indigenous women and girls in Canada
In late September, Inuit artist Annie Pootoogook died tragically in Ottawa. Pootoogook was an award-winning illustrator from Cape Dorset, Nunavut. Her ink-and-crayon depictions of everyday life in the north -- families sitting to eat a meal of seal meat or shopping at the Arctic co-op -- received international acclaim. In contrast to the idealized vision many Canadians have of the north, of majestic rock and ice landscapes or charismatic wildlife like polar bears, Pootoogook's drawings often reflected the crushing poverty northern families face and its devastating impacts on their health and well-being. (…) Although the national inquiry into murdered and missing Indigenous women won't investigate cases police previously examined, it will look at broader factors that put Indigenous women and girls at such great risk. According to the UN Committee on the Elimination of Discrimination Against Women, this includes institutional racism, social and economic marginalization and inadequate access to affordable housing so women can escape abusive relationships. Police forces have often failed to deal with violence against Indigenous peoples, and officers themselves have been implicated or charged with assaults and sexual abuse. Rabble

100 march for missing and murdered aboriginal females
Yellowknife resident James Jenka was like many of the other 100 or so people who marched in the annual Sisters in Spirit Walk yesterday. He too has lost a loved one - possibly due to violence. The march, from Ndilo to Northern United Place, was held on a blustery, chilly, grey day to honour and remember the roughly 1,500 missing aboriginal women and girls in Canada. The weather did not dampen the spirits of the marchers. Yellowknifer

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

What happens when you're caught driving stoned? Canada's Supreme Court may soon tell us
It seemed straightforward at first. In 2009, a number of people reported seeing an Ottawa driver cutting off another car, crossing over the centre line and barely missing oncoming traffic, forcing other drivers out of his way, and running into a car driven by an 87-year-old woman. Two separate people called 911 to report him as a drunk driver. To the police officer who showed up to investigate, Carson Bingley certainly seemed impaired: "swaying from side-to-side, slurred speech, slow and deliberate movements, and (staring) off into the distance during questioning." He stumbled, his fly was undone, and he had trouble zipping it up again, according to court documents. (…)If all of this sounds more complicated than a traditional drunk driving case, that's because it is. It's also why the courts have been chewing slowly on *Carson Bingley v. Her Majesty the Queen*, acquitting him twice because of an issue related to whether the police drug expert's evidence was admissible, ever since the original incident (the Supreme Court will hear the case in mid-October). Though stoned driving creates many of the same problems as drunk driving, it's not as easy to define. Without the ability to set a limit, measure it objectively and enforce it, the justice system is forced to fall back on the subjective judgment of police experts who have to determine whether someone was impaired in any given case. The result is an expensive, cumbersome system that has none of the clarity of our approach to drunk driving. Depending on what the Supreme Court does in the Bingley case, Canada's approach to drug-impaired driving may turn out to be broken in a way Parliament will have to fix. Stoned driving has attracted new attention lately because of the federal government's plan to legalize marijuana next spring. Global News

New Brunswick community colleges to offer pot-growing program
A new community college program is being developed in New Brunswick to train people to work in the growing medical marijuana field. Michel Doucet, executive director of contract training and customized learning for Collège communautaire du Nouveau-Brunswick, said he hopes the course will be offered at francophone community colleges in 2017. "We know there's a need for qualified workers. It's a brand new industry," Doucet said. CBC News

PUBLIC SERVICE / FONCTION PUBLIQUE

Update on Phoenix pay system problems expected this afternoon
An update on the federal government's efforts to fix problems arising from the Phoenix pay system is expected this afternoon. Senior officials from Public Services and Procurement Canada are expected to deliver remarks and answer questions from reporters. CBC News

OTHER / AUTRES

NIL

INTERNATIONAL

Matthew storms toward East Coast as evacuations begin
Authorities in Florida and South Carolina prepared to evacuate hundreds of thousands of people Wednesday as Hurricane Matthew roared closer to the U.S. after leaving a path of destruction across Haiti. Tropical storm conditions are expected to reach parts of the Florida coast by early Thursday, with hurricane conditions in some areas later that day, the National Hurricane Center warned. Matthew had top sustained winds of 120 mph, a Category 3 hurricane, Wednesday morning and could strengthen in coming days, the center said. "People have less than 24 hours to prepare," Scott warned Wednesday morning. "Having a plan could be the difference between life and death." At least 11 deaths have been attributed to the powerful storm as it has marched across the Caribbean this week, five of them in Haiti. But with a key bridge washed out there, roads impassable and phone communications down, there was no further word on the dead or injured. At 11 a.m. ET Wednesday the storm was about 105 miles south of the Bahamas, heading northwest at 12 mph. Florida and South Carolina prepared to evacuate more than 1 million people as the U.S. braced for the most powerful storm to smash through the region in almost a decade. USA Today; CBS/Associated Press; Sky News; ABC News; NBC News

Hurricane Matthew likely to miss D.C. and Delmarva
The track forecast for Hurricane Matthew has shifted dramatically since Tuesday, and the storm no longer appears to be a significant threat for the Mid-Atlantic coast north of the North Carolina Outer Banks. The computer model consensus is that Matthew will hug the Southeast coast between Thursday night and Saturday before retreating to the east. It poses a serious threat from the east coast of Florida to near the South Carolina-North Carolina border. Washington Post

Hurricane Matthew: UN says 350,000 Haitians in need of assistance
The destruction wrought by Hurricane Matthew has affected 350,000 Haitians and left the country facing its “largest humanitarian event” since the devastating earthquake six years ago, the UN has said. Ten thousand Haitians have been forced into shelters, while hospitals are under severe strain and water is in short supply, according to Mourad Wahba, the UN secretary general’s deputy special representative for Haiti. A situation report from the UN’s Office for the Co-ordination of Humanitarian Affairs (Ocha), citing information from the Haitian government’s Directorate of Civil Protection, says that 350,000 men, women and children in Haiti are in need of assistance. Ocha said that flooding had been reported in 11 towns on Haiti’s southern coast, while the International Organisation for Migration issued alerts over the plight of the 55,000 internally displaced people who are still living in temporary shelters in and around the capital, Port-au-Prince, following the 2010 quake. The Guardian; CNN; Reuters

2 Belgian police officers stabbed near Brussels in possible militant attack
Belgian counter terror prosecutors stepped in to investigate the stabbing of two police officers in Brussels on Wednesday, an indication the case was being treated as a possible militant attack. Brussels prosecutors said in a brief statement that the file had been taken on by their federal counterparts, who normally intervene in cases of organized crime or terrorism. According to public broadcaster VRT, one officer was stabbed in the neck and another in the stomach. The attacker then broke the nose of a third

policeman who had arrived at the scene. The attacker was shot in the leg and taken away by ambulance, VRT said, adding that the police officers' wounds were not life-threatening. Federal prosecutors were not immediately available to comment on why they were handling the case. Reuters (Global News); The Guardian; Sky News; Wall Street Journal; CBC News

France makes new push for Aleppo ceasefire
France is to launch a new push for United Nations backing for a ceasefire in Syria that would allow aid into the city of Aleppo after some of the heaviest bombing of the war. As diplomatic efforts resumed, a Syrian military source said army commanders had decided to scale back air strikes and shelling in Aleppo to alleviate the humanitarian situation there. The Syrian army command said civilians in rebel-held eastern Aleppo were being used as human shields and a reduced level of bombardment would allow people to leave for safer areas. France said Foreign Minister Jean-Marc Ayrault would travel to Russia and the United States on Thursday and Friday to try to persuade both sides to adopt a Security Council resolution to impose a new truce. Globe and Mail

Pakistan: trading fire with India after 'unprovoked' attack
Pakistan's military has accused India of another "unprovoked" attack in the disputed Himalayan region of Kashmir and says it is returning fire. In a statement, the military said Wednesday Pakistani and Indian troops continue to trade fire in various parts of Kashmir. It is unclear if either side has suffered casualties. The exchange of fire started shortly after Pakistani Prime Minister Nawaz Sharif arrived in parliament to discuss a Sept. 28 attack that killed two Pakistani soldiers, which India described as a "surgical strike" against militants. Associated Press (CTV News)

Morocco arrests ten female Isil suicide bombers who 'planned to strike on election day'
"It was a suicide attack and we found bomb-making materials," he added, but did not give further details. An interior ministry spokesman said the arrests, which followed a police raid in the capital of Rabat, could indicate that Isil was stepping up its efforts to recruit women to carry out attacks. "It was a suicide attack and we found bomb-making materials," he added, but did not give further details. An interior ministry spokesman said the arrests, which followed a police raid in the capital of Rabat, could indicate that Isil was stepping up its efforts to recruit women to carry out attacks. Telegraph (UK)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

Colinfreeze
Nub of @parsons @tamir_i critique is PSmin says cops face telco warrant hurdles s (l). Their data says not so (r). https://cippic.ca/news/national_security_consultation_revisiting_online_anonymity_yet_again …

CBCWindsor
Windsor-Tecumseh politicians demand more disaster relief from senior levels of government http://www.cbc.ca/1.3791382

TheHillTimes
(SUB) Security watchdog legislation passes first stage in Commons, opposed by Conservative party http://bit.ly/2cSpgr9 #cdnpoli

CBCCanada
MPs urge Ottawa to help first responders with PTSD http://ift.tt/2dpKEpu

globeandmail
How Ottawa revived Canada's most controversial privacy issue http://trib.al/AzxRDx2 from @GlobeBusiness

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

CBCManitoba
Province issues flood watch after west, north hit hard with rain http://ift.tt/2dcLrEL

Brett_CBC
Scene right now at the simulated train crash (training exercise) in Truro, with 100+ mock victims.

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Justin_Ling
Trudeau's C-51 consultations might expand, not limit, the spying bill. http://motherboard.vice.com/read/canadian-governments-plan-new-spying-powers-national-security-consultation-warrantless-access

CYBER SECURITY / CYBERSÉCURITÉ

Gizmodo
Yahoo secretly scanned users' emails for the NSA and FBI: report http://gizmo.do/WnRK0Fv

SCMagazine
Facebook Messenger caught up to WhatApp security with opt-in encryption https://t.co/RR9l1YZd5h

IndyUSA
NSA contractor arrested over 'stolen secret code used to hack Russia' http://ind.pn/2dKXVsw

LAW ENFORCEMENT / APPLICATION DE LA LOI

VOCMNEWS
RCMP Officers Armed With Fentanyl Antidote http://vocm.com/news/rcmp-officers-armed-with-fentanyl-antidote/ ...

CBCNorth
Inuvik celebrates new RCMP detachment https://t.co/1kXoyr9rF1

wlLakenews
Youth the focus of trafficking prevention project - Williams Lake Tribune http://fb.me/1emdRAzgJ

ctvwinnipeg
At large high-risk sex offenders back in custody: police #ctvwpg http://bit.ly/2dRVbcr

globalnews
3 @CalgaryPolice officers facing assault charges after man suffers broken ribs during arrest #yyc

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

CBCOttawa
Corrections Canada's $266K toilet solution was pooh-poohed by prison watchdog: http://cbc.ca/1.3790860 #ottnews #cdnpoli via @DavidBurkeCBC

CBCSask
Convicted murderer Roger Gillet found after 4 days on the loose https://t.co/2G9GdurSZl

963bigfm
Another lockdown at Collins Bay Pen #ygk http://www.963bigfm.com/syn/145/130048/collins-bay-pen-medium-security- ... unit-locked-down

CKWS_TV
Another lock down in place at Collins Bay pen http://bit.ly/2drYNCh

BigDogTruro
Lockdown ends at the Springhill Institution. http://bit.ly/2e2nUdz

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

globeandmail
Failure to protect indigenous children in care perpetuates cycle of abuse http://trib.al/QkPZloe From @picardonnhealth

rp_browne
Another e.g. of #naloxone barriers here: Toronto Pub Health wouldn't give guy a kit cuz he didn't ID as opioid user https://t.co/rHZWKiFv88

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

KBlazeBaum
Native Women's Association of Canada frustrated by #MMIW inquiry's "lack of progress," takes issue w transparency. http://www.theglobeandmail.com

AngelaSterritt
Please join us in Prince George for a public forum on #MMIW that will be aired on @TheCurrentCBC . I will be there! https://t.co/WUHXvEKFGW

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

trinafraser
RCMP continue to investigate marijuana dispensary - Merritt Herald -

PUBLIC SERVICE / FONCTION PUBLIQUE

TheHillTimes
Liberals do decent media relations, but departments still 'terribly unresponsive,' say Hill reporters http://bit.ly/2dJqvoH #cdnpoli

MichelleLamarch
Problèmes système de paye Phénix: 38000 cas sont réglés, il en reste plus de 40000. Échéancier 31 oct... #TVANouvelles

CBCKatie
Deputy Minister says 38,000 cases have been cleared in total. #hw

CBCKatie
Deputy Minister says technical challenges have slowed down progress. Says it is not Phoenix system related. #hw

CBCKatie
Another Phoenix data breach: happened on Friday. Employee data accessible to compensation advisors, risk considered low. #hw

CBCKatie
Deputy Minister says clearing the backlog will not mean an end to pay problems. #hw #phoenix

INTERNATIONAL

BBCBreaking
Two police officers stabbed in Brussels in possible terrorist incident, Belgian prosecutors say https://t.co/toalYolQla

TelegraphNews
Morocco arrests ten female Isil suicide bombers who 'planned to strike on election day' https://t.co/U5PIKO4DDT

BBCBreaking
Former Portuguese PM Antonio Guterres poised to become next UN secretary general, diplomats say https://t.co/dk9Kj5haNv

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

Sent to: !INTERNAL; !INTERNAL 2; CBSA Today's News; CSC & PBC Today's News; PS Today's News; RCMP Today's News; RCMP Today's News 2

Today's News / Actualités
October 7, 2016 / le 7 octobre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Canadian business leadership critical to reducing climate and other natural disaster risks, PwC Canada says

Canadian business leadership is crucial to reducing the risks from climate and other natural disasters, PwC Canada said on Friday. That day, PwC convened a group of private and public sector leaders to discuss the case for Canadian businesses to take action on reducing and managing the risks of climate and other natural disasters, the assurance, advisory and tax services firm noted in a statement. The event marks the first step in exploring the establishment of a country-level private sector leadership

alliance aligned with the global United Nations International Strategy for Disaster Reduction (UNISDR)-led ARISE partnership, PwC reported. Over the next year, PwC will engage Canadian businesses that are "willing and able" to take action on reducing the risks of climate, earthquake and other natural hazards, along with government partners and other parties interested in disaster risk reduction. Federal **Minister of Public Safety and Emergency Preparedness, Ralph Goodale**, **said** that the ministry is participating in the "***first step towards the launch of ARISE Canada. We are committed to working with all levels of government and partners from the private sector to strengthen public-private partnerships and to embrace a whole-of-society approach to emergency management***." **Goodale** pointed out that the upcoming National Roundtable on Disaster Risk Reduction in Montreal in November will provide further opportunities to engage across sectors on this important issue. "***We look forward to working with the private sector both domestically and as part of our international commitments with the UNISDR to meet Sendai commitments for disaster risk reduction and build a more resilient Canada***," **he said**. Canadian Underwriter

TOP STORIES / MANCHETTES

Un agent correctionnel de Donnacona tire sur un détenu
Un agent correctionnel du pénitencier de Donnacona a ouvert le feu sur un détenu, jeudi matin, le blessant sérieusement. La Sûreté du Québec a ouvert une enquête sur l'incident qui serait survenu suite à une bataille entre deux détenus. Une violente bagarre aurait éclaté entre deux détenus, vers 10h30, jeudi matin, au pénitencier à «sécurité maximale» de Donnacona. Craignant pour la vie d'un des détenus impliqués, des agents correctionnels auraient tenté de maîtriser l'agresseur avec des gaz irritants, avant d'ouvrir le feu sur lui. Selon Ann Mathieu, porte-parole de la Sûreté du Québec (SQ), «au moins un coup de feu» aurait été tiré par un agent correctionnel. Les deux détenus ont été transportés dans un Centre hospitalier. Le détenu touché par balle aurait subi des blessures sévères, mais l'on ne craindrait pas pour sa vie. L'unité des crimes majeurs de la SQ a été mandatée pour enquêter sur l'évènement. Rappelons que la sécurité à l'intérieur des pénitenciers fédéraux relève du Service correctionnel du Canada. La Presse; CBC News

ISIS just identified a dead leader by name — and that's unusual
The Islamic State has for the first time identified Canadian citizen Tamim Chowdhury as its former head of military and covert operations in Bangladesh — using his real name in print, in an unusual move — six weeks after he died in a hail of bullets during a shootout with Bangladeshi police. Chowdhury, a relative unknown until this year, gained worldwide notoriety in July as the alleged mastermind of a terrorist attack on a popular Dhaka cafe that left 22 people, mostly foreigners, dead. ISIS immediately claimed responsibility for the attack, but until Tuesday the extremist group had never acknowledged any association with Chowdhury. "I think it's the first time that ISIS has ever used anyone's real name in an official publication," said Amarnath Amarasingam, a fellow at the Center for Cyber and Homeland Security at George Washington University who has written extensively on extremism. Chowdhury was killed in August in one of a series of raids on suspected militant dens in Bangladesh, which has seen dozens of deadly attacks on atheists, secular writers, and religious minorities in the last two years. The latest issue of Rumiyah magazine, a newer publication hawked by the militants, includes a fresh account of the Dhaka attack, under Chowdhury's byline. The author profiles each of the six attackers who died in the clash and describes the bloodshed as "just a glimpse, and what is yet to come by the permission of Allah will be worse and far more bitter." (…) Since his death, other ties between Canada and extremist outfits in Bangladesh have emerged: One of Chowdhury's accomplices, a now-dead former army officer named Mohammed Jahidul Islam, once received training from the Canadian military. (Canada's Department of National Defence confirmed to VICE News that someone of a "similar name" participated in an academic course on warfare.) VICE News (2016-10-06)

RCMP too big to fix, says former spokesperson Catherine Galliford
The RCMP offered a national apology Thursday to female officers and employees who were subjected to harassment, discrimination and sexual abuse while on the job. Compensation could total up to $100 million. Catherine Galliford, a former high-pofile RCMP spokeswoman, filed an individual lawsuit in 2012 and settled in May. Hundreds of other women came forward afterwards, resulting in two class action

lawsuits. Galliford spoke with On The Coast host, Gloria Macarenko, to share her reaction to the apology and settlement. Q: What goes through your mind when you hear the emotional responses to the apology from other women? I am so proud of them. This is like a revolution because people are talking about it now. I don't want the members of the RCMP to stop talking about this because now they have a voice. Q: The settlement covers all women in the RCMP since 1974. What do you think about those terms? I think those terms are amazing. But what struck me today was the national apology For these women to have a national apology from the Commissioner of the RCMP, to have him say we owe these women an apology, that is worth more to them than anything. Q: Do you think this settlement goes far enough? I think they are talking about changing a culture and I don't know if that can be changed. I think the RCMP has gotten too big to be managed. There are a lot of women and men who have been harassed to the point where they are still trying to do their jobs but are walking zombies. People are afraid to complain and are still being harassed. I don't believe the RCMP in its current state can be fixed. I think it should be a federal police board only and provincial governments can set up their own police forces. CBC News

Canada's Police Force Pledges $75 Million in Compensation for Women Abused in Its Ranks
At a press conference Thursday announcing upward of $75 million in compensation for hundreds of harassed female employees with the Royal Canadian Mounted Police, Officer Linda Davidson embraced Commissioner Bob Paulson. "It takes a great person to acknowledge what went wrong," Davidson, who was diagnosed with PTSD as a result of alleged harassment by her co-workers and bosses, told reporters Thursday. "This is a new step, it's a new beginning. We are headed in the right direction." Davidson mounted a class action lawsuit against Canada's national police force in March 2015, alleging that she and other female officers were victims of systemic sexual harassment and discrimination within the force. It's the second class action of its kind after another such action by former RCMP constable Janet Merlo five years ago. The Merlo class action snowballed into about 500 women who joined on with their own allegations of harassment. The RCMP said Thursday they expect 1,000 women to come forward, which is how they decided on the "ballpark estimate" of $75 million in compensation. It was an emotional moment for Paulson, too, who choked up as he read his statement. "For many of our women, this discrimination and harassment has hurt them mentally and physically," he said. Adding: "Their very lives have been affected." VICE News

Harcèlement à la GRC : la députée Ginette Petitpas Taylor satisfaite du règlement
La députée fédérale de Moncton-Riverview-Dieppe, Ginette Petitpas Taylor, est contente que le commissaire de la Gendarmerie royale du Canada (GRC), Bob Paulson, ait présenté ses excuses aux centaines d'employées de la police fédérale qui disent avoir été victimes de harcèlement sexuel et de discrimination. La députée libérale a travaillé 23 ans au sein du détachement Codiac de la GRC, en tant qu'employée civile. Elle espère que l'annonce de jeudi va permettre de fermer un chapitre regrettable pour le service de police. Ginette Petitpas Taylor reconnaît qu'à certaines époques, il régnait une culture de discrimination au sein de la GRC. Cette attitude se manifestait notamment par des commentaires sexistes et des abus de pouvoir. Elle précise qu'au détachement de Codiac, elle n'a jamais eu l'impression que les femmes étaient désavantagées pour des promotions. Radio-Canada

Justice served by RCMP apology, $100M settlement of harassment claims says former Mountie
Justice has been served through Thursday's settlement of class action lawsuits over harassment of female RCMP members, says Heli Kijanen, the former Mountie who spearheaded legal action against the national force in 2011. RCMP commissioner Bob Paulson apologized to female RCMP officers who had been harassed, and announced $100-million has been allotted to settle claims. Kijanen, who was born in Thunder Bay, Ont., had been working as an RCMP officer in Saskatchewan, but resigned due to bullying from male members of the force. "I feel like people have been given back pieces of their lives to complete the puzzle of closure," she said of the settlement. CBC News (2016-10-07); Thunder Bay News Watch (2016-10-06)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

UPDATED : Hurricane Matthew unlikely to reach Canada: weather expert

A Canadian hurricane preparedness expert says Hurricane Matthew is unlikely to reach Canada on its path up the East Coast. The massive Category 3 storm is far more likely to loop back on itself and pound Florida a second time in the days ahead, according to Bob Robichaud, a warning preparedness meteorologist with the Canadian Hurricane Centre... Hurricane Matthew is projected to slowly push north through Florida, Georgia and South Carolina, before eventually curving east out to sea and turning south again. CTV News

Stranded Yukon hunters survived on rosehips and lake water for 4 days
RCMP say three hunters followed "all the right steps" when they found themselves stranded for days on a remote Yukon lakeshore, with almost no survival gear. The three were successfully rescued on Wednesday, in good health, despite living only on rosehips and lake water for four days. Police say the hunters left Whitehorse Sunday morning on a hunting trip. They took their aluminum boat out on a lake about 90 kilometres west of Whitehorse.They beached their boat to look for some prey on shore. That's when the wind carried the boat away, and with it, all their supplies. The three men were left only with the clothes they were wearing, a few lighters, a knife and binoculars... Police say the men - all very experienced hunters - then hunkered down to wait for a rescue. They had told their families they'd be back on Tuesday night, so they knew it would likely be a few days before a search began... About midday on Wednesday, relatives reported them missing to police. RCMP search and rescue managers checked two possible locations the relatives had told them about, and soon found the men's vehicle. A helicopter was then used to search for the men, and they were found at about 6 p.m. on Wednesday. They were hungry, but otherwise in good health, according to RCMP. CBC News

Fort McMurray evacuees rebuild life in Elliott's Cove
Ivy and Bruce Berkshire sit for a photo on their newly constructed patio at their house in Elliott's Cove. The couple returned to the province after losing their home in the Fort McMurray wildfires on May 3... A week later, on May 11, they flew to Newfoundland. That's when Bruce began showing signs of illness. Inhalation of the smoke and live amber caused him to have a lung infection. "Naturally, I had to consume some of it, because I was in it," he said. "I was in that for two hours. Had no choice, we had to keep moving to get out of the city." He spent about a week recovering in hospital. Today, Bruce says he's feeling much improved, other than some minor issues... They say they harbour anger towards the powers-that-be for not accepting help that was offered by other countries and provinces, to help battle the blaze. The property owners for their complex, and their insurance company have also been silent, leaving them with some uncertainties. Besides what they lost in fire, flooding consumed belongings they had stored at the hotel where Ivy worked. All they can do now, is focus on the present. Telegram

Top squad
A national search and rescue (SAR) exercise — SAREX — conducted in Yellowknife, Northwest Territories, from Sept. 18-24 highlighted the importance of conducting real-world SAR missions and training to ensure crews are ready to respond when Canadians are in distress. The value of the Royal Canadian Air Force exercise was further underlined when exercise participants unexpectedly provided real-time assistance to a canoeist in distress on Great Slave Lake, N.W.T. and, in a separate incident, rescued four individuals from a remote area near Ulukhaktok, N.W.T. In the spirit of traditional, friendly competition during National SAREX 2016, 103 Search and Rescue Squadron from 9 Wing Gander, Newfoundland and Labrador, won the Diamond Trophy by emerging as the best overall SAR squadron after five intense exercise days. Gander Beacon

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Tackling the Government Green Paper on National Security: Part 2
This is our second in a series of responses to the federal government's Green Paper on Canada's current national security framework. While the paper generally favours the current national security framework, CCLA will seek to add additional context, and to show why there is no incompatibility between a strong commitment to national security and a strong commitment to our Charter rights and freedoms. This week, we discuss the amendments made by Bill C-51 to the Canadian Security Intelligence Act ("CSIS Act")

drastically expanding the Canadian Security Intelligence Service's (CSIS) powers. These provisions are among those highlighted in our constitutional challenge to the Anti-Terrorism Act, 2015 (the "ATA, 2015"). Canadian Civil Liberties Association (2016-10-05)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

ISIS just identified a dead leader by name — and that's unusual
The Islamic State has for the first time identified Canadian citizen Tamim Chowdhury as its former head of military and covert operations in Bangladesh — using his real name in print, in an unusual move — six weeks after he died in a hail of bullets during a shootout with Bangladeshi police. Chowdhury, a relative unknown until this year, gained worldwide notoriety in July as the alleged mastermind of a terrorist attack on a popular Dhaka cafe that left 22 people, mostly foreigners, dead. ISIS immediately claimed responsibility for the attack, but until Tuesday the extremist group had never acknowledged any association with Chowdhury. "I think it's the first time that ISIS has ever used anyone's real name in an official publication," said Amarnath Amarasingam, a fellow at the Center for Cyber and Homeland Security at George Washington University who has written extensively on extremism. Chowdhury was killed in August in one of a series of raids on suspected militant dens in Bangladesh, which has seen dozens of deadly attacks on atheists, secular writers, and religious minorities in the last two years. The latest issue of Rumiyah magazine, a newer publication hawked by the militants, includes a fresh account of the Dhaka attack, under Chowdhury's byline. The author profiles each of the six attackers who died in the clash and describes the bloodshed as "just a glimpse, and what is yet to come by the permission of Allah will be worse and far more bitter." (…) Since his death, other ties between Canada and extremist outfits in Bangladesh have emerged: One of Chowdhury's accomplices, a now-dead former army officer named Mohammed Jahidul Islam, once received training from the Canadian military. (Canada's Department of National Defence confirmed to VICE News that someone of a "similar name" participated in an academic course on warfare.) VICE News (2016-10-06)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Improve mental health services for Edmonton deportee, urges Black Lives Matter
Black Lives Matter Edmonton is urging authorities to provide better mental health supports to a man awaiting deportation and has been detained without charge for months. "We really need to find help for him," said Ufuoma Odebala-Fregene, immigration consultant and executive member of Black Lives Matter Edmonton. "We need to engage the mental health system to find out why they are not taking him because that's clearly an issue." For at least eight months, authorities have held convicted criminal 31-year old Abdikarim Gelle in the Edmonton Remand Centre as they try to deport him, even though he has served his time. Somalia won't accept Gelle because he suffers from mental illness. Transcripts from Gelle's detention reviews show Canadian authorities hope that decision will change. In the meantime, the tribunal has ruled that Gelle is too dangerous to release. Gelle, who arrived in Canada as a 13-year-old refugee originally from Somalia, has racked up 57 convictions as an adult for crimes including sexual assault, assault of a peace officer and trafficking cocaine. Gellw failed to appear in court and breached his probation account for about a third of his convictions. Documents show Somali authorities have told Canadian officials they will not accept deportees suffering from mental illness. Gelle suffers from a long list of conditions which began showing up as a youth including schizoaffective disorder, chronic psychosis and cognitive delay that results in delusions, deficient judgement, hearing voices and other consequences. Officials have looked into transferring Gelle to Alberta Hospital, according to detention review transcripts. However, a forensic psychiatrist with Alberta Health Services has indicated the psychiatric hospital in Edmonton won't take Gelle because he can't be easily transitioned into the community, and won't comply with his treatment plan. Despite repeated requests from CBC News, neither Alberta Health Services or the Canadian Border Services Agency has provided comment. CBC News

Traffic backed up heading to Ambassador Bridge

Windsor police are reporting serious backups on Huron Church Road heading to the Ambassador Bridge. Police report traffic is backed up to Tecumseh Road West. Officers are in the area directing traffic. CBC News

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Yahoo's Government Email Scanner Was Actually a Secret Hacking Tool
The spy tool that the US government ordered Yahoo to install on its systems last year at the behest of the NSA or the FBI was a "poorly designed" and "buggy" piece of malware, according to two sources closely familiar with the matter... Anonymous sources told The Times that the tool was nothing more than a modified version of Yahoo's existing scanning system, which searches all email for malware, spam and images of child pornography. But two sources familiar with the matter told Motherboard that this description is wrong, and that the tool was actually more like a "rootkit," a powerful type of malware that lives deep inside an infected system and gives hackers essentially unfettered access. The rootkit-like tool was found by Yahoo's internal security testing team during one of their checkups, according to a source. "They assumed it was a rootkit installed by hackers," an ex-Yahoo employee, who requested anonymity to discuss sensitive issues, told Motherboard. "If it was just a slight modification to the spam and child pornography filters, the security team wouldn't have noticed and freaked out." "It definitely contained something that did not look like anything Yahoo mail would have installed," the source added. "This backdoor was installed in a way that endangered all of Yahoo users." Motherboard;

Web-Based Keylogger Used to Steal Credit Card Data from Popular Sites
Popular ecommerce sites have been infected with web-based keyloggers that are being used to steal credit card data as it's entered into online checkout forms. More than 100 compromised sites have been identified, but the number could be in the thousands, researchers said. RiskIQ, in collaboration with ClearSky, published their findings (PDF) Thursday, and said some of the ecommerce sites impacted include Everlast Worldwide, the Australian ecommerce site for apparel giant Guess and Fidelity Investments' FidelityStore, a site maintained by a third-party firm SwervePoint. Threat Post; Security Week

US NIST Warns Security 'Fatigue' is Putting Users at Risk
A reluctance to deal with computer security is putting users in danger online as they take unnecessary risks due to general fatigue with things like passwords, according to a new NIST study. The US standards body uncovered feelings of resignation, loss of control, fatalism, risk minimization, and decision voidance in its interviews with a range of ordinary computer users aged between 20 and 60-years-old. The research team found respondents have grown tired of being on constant alert for online threats and of trying to understand the nuances of online security issues. Infosecurity Magazine; SC Magazine; BBC News

EFF: NSA's Support of Encryption 'Disingenuous'
The National Security Agency came out in support of encryption again Wednesday, but privacy advocates were quick to contest the agency's stance, criticizing it for having a different definition of the term than others. Glenn Gerstell, general counsel for the NSA, stressed that the agency believes in strong encryption multiple times during a panel, "Privacy vs. Security: Beyond the Zero-Sum Game," at Cambridge Cyber Summit here at MIT, on Wednesday. Another panelist, Cindy Cohn, executive director of the Electronic Frontier Foundation, took offense and said that when the NSA uses the word encryption, it should really place an asterisk at the end. "I think there should be an asterisk most of the time. I've been in meetings with people from the NSA and FBI and when they say we support strong encryption... what they really mean is strong encryption that only they have access to," Cohn said. Threat Post

We're not going to beat cybercrime in our lifetime says ex-FBI cyber chief
A former director of the FBI's crime and cybercrime response unit has warned that the problems of hacking and cybercrime will not be solved in our lifetimes, but we that we owe it to future generations to avoid completely mismanaging the issue to make it worse to deal with in years to come. Shawn Henry spent 24 years at the FBI where he rose through the ranks to oversee all of the Bureau's criminal and

cyber investigations across the globe before retiring from the organisation in 2012. "We're not going to solve it, folks, not in our lifetime, but we have to constantly manage it," he said, speaking at IP EXPO 2016 in his post-FBI role as president of cybersecurity firm Crowdstrike… Rather than an organisation sitting back and waiting to see if it's attacked, Henry argues that cybersecurity professionals should be constantly examining their own network looking for indicators of attack because "If we're not out constantly hunting for the adversaries they're hunting us". ZDNet

Exclusive: The Aspen Institute's Walter Isaacson Interviews Admiral Michael S. Rogers from the Cambridge Cyber Summit Today
Following is the unofficial transcript of an EXCLUSIVE interview with Admiral Michael S. Rogers, Commander, U.S. Cyber Command; Director, National Security Agency; Chief, Central Security Service, live from the Cambridge Cyber Summit hosted by The Aspen Institute, CNBC and MIT on Wednesday, October 5th. CNBC

Arrested NSA Contractor 'Doesn't Fit the Profile'
The FBI has arrested NSA contractor Harold Martin, who is suspected of stealing highly classified source code developed by the agency to hack the computer networks of adversaries like Russia, China, Iran and North Korea. Apparently though, the suspect did not fit any of the usual profiles of an "insider threat."… One administration official told the *New York Times* that he didn't fit the assumed profile, and that he was "not like a Snowden or someone who believes that what we were doing was illegal and wanted to publicize that." A Navy veteran working on a Ph.D. in computer science, Martin may have simply been collecting files for his own edification—much like other senior officials across Washington take classified documents home with them. It's a known shadow practice, but not a malicious one. Infosecurity Magazine; Daily Beast

Radio hacker 'caused havoc at Edinburgh airport and hospital'
Jamie Corrigan was 17 when he started tapping into the signals "as a prank". Edinburgh Sheriff Court heard calls on the Air Traffic Control frequency at Edinburgh Airport interfered with aircraft and emergency vehicles. Network Rail also reported attempts to redirect moving trains. Corrigan, now 20, has now been banned from leaving his home between 22:00 and 06:00 for the next six months. He was also ordered to forfeit radio equipment. Corrigan, of Niddrie House Square, Edinburgh, had previously pleaded guilty to charges of culpable and reckless conduct by making repeated radio transmissions which caused fear and alarm, potential endangerment and making abusive and offensive remarks. His targets also included Edinburgh Castle, the Royal Infirmary of Edinburgh, NSL Services Group, and Westside and Cameron Toll Shopping Centres. BBC News

LAW ENFORCEMENT / APPLICATION DE LA LOI

RCMP too big to fix, says former spokesperson Catherine Galliford
The RCMP offered a national apology Thursday to female officers and employees who were subjected to harassment, discrimination and sexual abuse while on the job. Compensation could total up to $100 million. Catherine Galliford, a former high-pofile RCMP spokeswoman, filed an individual lawsuit in 2012 and settled in May. Hundreds of other women came forward afterwards, resulting in two class action lawsuits. Galliford spoke with On The Coast host, Gloria Macarenko, to share her reaction to the apology and settlement. Q: What goes through your mind when you hear the emotional responses to the apology from other women? I am so proud of them. This is like a revolution because people are talking about it now. I don't want the members of the RCMP to stop talking about this because now they have a voice. Q: The settlement covers all women in the RCMP since 1974. What do you think about those terms? I think those terms are amazing. But what struck me today was the national apology For these women to have a national apology from the Commissioner of the RCMP, to have him say we owe these women an apology, that is worth more to them than anything. Q: Do you think this settlement goes far enough? I think they are talking about changing a culture and I don't know if that can be changed. I think the RCMP has gotten too big to be managed. There are a lot of women and men who have been harassed to the point where they are still trying to do their jobs but are walking zombies. People are afraid to complain

and are still being harassed. I don't believe the RCMP in its current state can be fixed. I think it should be a federal police board only and provincial governments can set up their own police forces. CBC News

Canada's Police Force Pledges $75 Million in Compensation for Women Abused in Its Ranks
At a press conference Thursday announcing upward of $75 million in compensation for hundreds of harassed female employees with the Royal Canadian Mounted Police, Officer Linda Davidson embraced Commissioner Bob Paulson. "It takes a great person to acknowledge what went wrong," Davidson, who was diagnosed with PTSD as a result of alleged harassment by her co-workers and bosses, told reporters Thursday. "This is a new step, it's a new beginning. We are headed in the right direction." Davidson mounted a class action lawsuit against Canada's national police force in March 2015, alleging that she and other female officers were victims of systemic sexual harassment and discrimination within the force. It's the second class action of its kind after another such action by former RCMP constable Janet Merlo five years ago. The Merlo class action snowballed into about 500 women who joined on with their own allegations of harassment. The RCMP said Thursday they expect 1,000 women to come forward, which is how they decided on the "ballpark estimate" of $75 million in compensation. It was an emotional moment for Paulson, too, who choked up as he read his statement. "For many of our women, this discrimination and harassment has hurt them mentally and physically," he said. Adding: "Their very lives have been affected." VICE News

Harcèlement à la GRC : la députée Ginette Petitpas Taylor satisfaite du règlement
La députée fédérale de Moncton-Riverview-Dieppe, Ginette Petitpas Taylor, est contente que le commissaire de la Gendarmerie royale du Canada (GRC), Bob Paulson, ait présenté ses excuses aux centaines d'employées de la police fédérale qui disent avoir été victimes de harcèlement sexuel et de discrimination. La députée libérale a travaillé 23 ans au sein du détachement Codiac de la GRC, en tant qu'employée civile. Elle espère que l'annonce de jeudi va permettre de fermer un chapitre regrettable pour le service de police. Ginette Petitpas Taylor reconnaît qu'à certaines époques, il régnait une culture de discrimination au sein de la GRC. Cette attitude se manifestait notamment par des commentaires sexistes et des abus de pouvoir. Elle précise qu'au détachement de Codiac, elle n'a jamais eu l'impression que les femmes étaient désavantagées pour des promotions. Radio-Canada

Canadian Mounties apologise for rampant sexual harassment after multi-million dollar lawsuit settlement
The Royal Canadian Mounted Police have reached a multi-million dollar settlement with female members of the force after decades of gender and sexual discrimination and harassment. Once approved in federal court, the settlement agreement is expected to reach C$100m ($76m). The settlement comes as a result of two class action lawsuits filed by two former Mounties: Linda Gillis Davidson, who joined the RCMP in 1985, and Janet Merlo, who joined in 1991. “Some of these women left the RCMP heartbroken, disillusioned, and angry,” said RCMP Commissioner Bob Paulson, apologising for "shameful conduct". “Others stayed and were forced to find ways to cope with this inexcusable condition since they did not see an organisation that was willing to change.” Ms Merlo called Mr Paulson’s apology a “turning point” for the iconic Canadian organisation. “I have total faith that this is the beginning of a new era, hopefully a better era,” she said. She added that the hundreds allegations were not directed at the entire organisation, but rather at a few members of the Mounties. “Within the RCMP itself,” she said, “it seems that it was a minority, but a potent minority, that behaves this way.” Independent UK

Justice served by RCMP apology, $100M settlement of harassment claims says former Mountie
Justice has been served through Thursday's settlement of class action lawsuits over harassment of female RCMP members, says Heli Kijanen, the former Mountie who spearheaded legal action against the national force in 2011. RCMP commissioner Bob Paulson apologized to female RCMP officers who had been harassed, and announced $100-million has been allotted to settle claims. Kijanen, who was born in Thunder Bay, Ont., had been working as an RCMP officer in Saskatchewan, but resigned due to bullying from male members of the force. "I feel like people have been given back pieces of their lives to complete the puzzle of closure," she said of the settlement. CBC News (2016-10-07); Thunder Bay News Watch (2016-10-06)

Editorial: A welcome apology from the RCMP

An editorial states, "... Now RCMP Commissioner Bob Paulson has offered a heartfelt apology and committed to transformational change as part of the settlement of two class-action lawsuits. The mea culpa from the top brass is a historic public acknowledgement of the RCMP's failure to stand by its female members. The settlement represents justice for 500 complainants who have denounced demeaning treatment. About $100 million has been set aside for compensation. The process is to be administered by retired Supreme Court Justice Michel Bastarache and it is estimated as many as 1,000 women could make claims. The most important part of the settlement, though, is its reinforcement of efforts to bring the RCMP "into modernity," as Paulson put it... Paulson seems sincere in his commitment to banishing sexism from the RCMP and his leadership sends a strong message. But it is essential that the old boys' club get the memo that disrespect toward women is not acceptable." Montreal Gazette

IIO investigating death

The Independent Investigations Office of B.C. is investigating a fatality in Kelowna near the Bennett clock tower Wednesday afternoon. Spokesman Marten Youssef confirmed the IIO was called on to look into the incident after a man reportedly was in medical distress at the clock tower and later died after involvement with police. The organization investigates police-involved deaths across the province. Youssef said the IIO was notified of the incident by Kelowna RCMP and is assessing the situation. "The primary focus of our investigation is to first establish if there is a connection between the male's death and the actions or inactions of police," he told Castanet. "If there is, then we will continue with our investigation. If there is no connection, we will release jurisdiction back to the RCMP." At this time, the IIO is releasing no additional details "as we want to ensure that we independently verify the information," Youssef said in an email. Castanet

Police documents reveal how law enforcement keep Stingray use secret

Police records obtained by the Daily Dot reveal in unprecedented detail how the Obama administration enables law enforcement to suppress information about controversial phone-surveillance technology used by police throughout the United States. The documents, which link the purchase of so-called Stingray devices to various North Carolina state and local police agencies, include a fill-in-the-blank warrant drafted by the U.S. Justice Department (DOJ) and intended for use by state and local police that extends the veil of secrecy over law enforcement's Stingray use. (...) We know from sworn testimony from Toronto police that Stingrays can disrupt all cell activity up to and including 911 calls. Even though the devices are programmed to disengage when citizens in the area attempt to reach emergency services, they often fail to do so, according to an internal Royal Mounted Canadian Police (RCMP) memo, published this April by the *Globe and Mail*. Due to frequent malfunction with Stingrays, Canadian authorities admit the contraption is run at a "calculated risk to public safety," *Globe and Mail* reports. According to RCMP, police are now only allowed to use the device for three minutes at a time. And while the U.S. Justice Department's warrant is meant to reassure judges that any service disruption will be "brief" and "minimized," at least one documented case shows the continuous use of a Stingray in Oakland, California, for over nine hours. Daily Dot

Extortion scam circulating online in Leduc

RCMP are issuing a warning after a number of people in the Leduc area were blackmailed for money, after sharing "compromising" photographs of themselves online. In a statement issued Friday, police said they have recently received a number of reports from people who have been targeted in the social media scam. Police said victims are contacted through various social media platforms, with a friend request from a stranger. When the person accepts the friend request, the scammer then works to "bait" them into providing "compromising images" of themselves, which are then used to blackmail the victim, police said. The scammers demand money, and threaten to release the private images to the victim's friends, family and the public, if they fail to comply. RCMP are encouraging all users on social media to exercise caution when accepting new friend requests, especially when private or compromising images are requested. CBC News

25 000 $ pour aider à retrouver une adolescente de Yorkton

La générosité du public a permis à la famille de Mekayla Bali de récolter 25 000 $ qui serviront de récompense à quiconque partage des informations menant à l'adolescente de 17 ans, annonce la Gendarmerie royale du Canada (GRC). Mekayla Bali a été vue pour la dernière fois le 12 avril dans une

station d'autobus de Yorkton, sa ville de résidence, selon la GRC. Ce matin-là, l'adolescente de 17 ans a été déposée à l'école par sa mère. C'est à ce moment que Paula Bali a vu sa fille pour la dernière fois. La mère de l'adolescente disparue enjoint les personnes qui auraient vu sa fille de communiquer avec la GRC. Paula Bali tient également à remercier les gens qui ont donné à la cause pour aider à retrouver Mekayla. « Ça prend un village pour élever un enfant. Ça pourrait prendre un pays pour en retrouver un, » a-t-elle affirmé jeudi après-midi lors d'un point de presse de la GRC à Regina. Les autorités policières disent avoir reçu 130 indications du public depuis le début de l'enquête. Des pistes de recherche venant d'aussi loin que de la Colombie-Britannique font partie de ce nombre. Cependant, les indications reçues jusqu'à maintenant n'ont pas permis de confirmer quels sont les déplacements précis de Mekayla Bali depuis le 12 avril, précise Jennifer Ebert de la GRC. « Les informations reçues nous font croire qu'il n'y a pas d'acte criminel associé à sa disparition, mais c'est troublant de voir qu'une adolescente de cet âge peut disparaître sans laisser de traces alors qu'on vit dans l'ère du numérique. » - Jennifer Ebert, inspectrice de la GRC. Radio-Canada; Canadian Press (Castanet)

County RCMP seek missing teen
Strathcona County RCMP are asking for the public's assistance in locating a missing 15-year-old girl from Sherwood Park. Rachael Margaret McNeilly was last seen at approximately 6:15 a.m. on Monday, Oct. 3. "Although there is nothing at this time to lead police to believe that McNeilly's disappearance is suspicious, the RCMP are concerned for her well-being and need to locate McNeilly to ensure her safety," said Const. Chantelle Kelly, media liaison with the Strathcona County RCMP. McNeilly is described as Caucasian, five-feet tall, with a slim build and long red hair. Sherwood Park News

Queens District RCMP say there are no menacing clowns in Liverpool.
In a release sent out this morning, police say they want to allay public concerns about the issue, which they say was generated in large part by false social media reports that people disguised as clowns have been menacing local citizens. This week, several Facebook posts indicated that three people dressed as Clowns were in Liverpool. RCMP say this is not true. "While social media can be a useful tool in distributing information quickly, it can also be a detriment as witnessed by false reports of menacing clowns circulating in Queens County," says the release. Police say people should carefully assess unsubstantiated social media posts before forwarding them, and if they appear to be gossip or rumour, do not report them as fact. "Police do not wish to discourage anyone from contacting police if they are witness to an actual incident involving a clown appearing threating or assaultive however, and residents are encouraged to report any genuine wrongdoing." Queens County Advance

Helping out Shamattawa
Bobbi Montean and members of the Thompson RCMP were in the Giant Tiger parking lot Oct. 1 to collect food and goods donations to contribute to the Shamattawa relief effort, after the community lost several local services due to arson, including its sole grocery store. Thompson Citizen

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Un agent correctionnel de Donnacona tire sur un détenu
Un agent correctionnel du pénitencier de Donnacona a ouvert le feu sur un détenu, jeudi matin, le blessant sérieusement. La Sûreté du Québec a ouvert une enquête sur l'incident qui serait survenu suite à une bataille entre deux détenus. Une violente bagarre aurait éclaté entre deux détenus, vers 10h30, jeudi matin, au pénitencier à «sécurité maximale» de Donnacona. Craignant pour la vie d'un des détenus impliqués, des agents correctionnels auraient tenté de maîtriser l'agresseur avec des gaz irritants, avant d'ouvrir le feu sur lui. Selon Ann Mathieu, porte-parole de la Sûreté du Québec (SQ), «au moins un coup de feu» aurait été tiré par un agent correctionnel. Les deux détenus ont été transportés dans un Centre hospitalier. Le détenu touché par balle aurait subi des blessures sévères, mais l'on ne craindrait pas pour sa vie. L'unité des crimes majeurs de la SQ a été mandatée pour enquêter sur l'évènement. Rappelons que la sécurité à l'intérieur des pénitenciers fédéraux relève du Service correctionnel du Canada. La Presse; CBC News

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Fentanyl overdose: 131 people in northern Ontario killed since 2010
Fentanyl overdose has killed 131 people in northern Ontario since 2010, according to new data from the Chief Coroner's Office obtained by CBC.Fentanyl — a powerful narcotic that can be 50 to 80 times more powerful than morphine— is now the number one cause of opioid-related death in Ontario and killed nearly 200 people in 2015. In northern Ontario, an additional 134 people have died of methadone overdose and another 122 overdoses on oxycodone in the last six years. CBC News (2016-10-06)

Why would anyone use a chemical weapon to make drugs? Money
This summer, carfentanil — one of the most potent opioids on the planet — hit the streets of North America. Many users who thought they were taking heroin actually injected or snorted a substance that has until recently been viewed as a chemical weapon . First responders pumped hundreds of dying, bluish people full of the antidote naloxone to try to make them breathe again. Legally used as a tranquilizer for large animals like bears and elephants, carfentanil is so potent that an amount smaller than a poppy seed can kill a person. How such a toxic substance made its way into global narcotics supply chains is a matter of economics, and desperation. Carfentanil is 100 times more potent than fentanyl, a related drug that increasingly has been mixed into narcotics such as heroin. But carfentanil is only slightly more expensive than fentanyl, and it can be cut into much larger volumes, creating stronger, cheaper highs. Associated Press

Governments researched fentanyls as weapons for decades
Before appearing in global narcotics supply chains, fentanyl and substances like it were viewed as potential chemical weapons. Scientists struggled to figure out how to package the chemicals so that they would incapacitate but not kill targets. Here are some highlights of those efforts: Associated Press

Chinese companies willing to export deadly opioid carfentanil to Canada and U.S.
For a few thousand dollars, Chinese companies offer to export a powerful chemical that has been killing unsuspecting drug users and is so lethal that it presents a potential terrorism threat, an Associated Press investigation has found. The AP identified 12 Chinese businesses that said they would export the chemical — a synthetic opioid known as carfentanil — to the United States, Canada, the United Kingdom, France, Germany, Belgium and Australia for as little as $2,750 a kilogram (2.2 pounds), no questions asked. Carfentanil burst into view this summer, the latest scourge in an epidemic of opioid abuse that has killed tens of thousands of people in the United States alone. Dealers have been cutting carfentanil and its weaker cousin, fentanyl, into heroin and other illicit drugs to boost profit margins. Global News; Radio Canada International; Chicago Tribune

Naloxone nasal spray too pricey for those who need it, frontline workers say
Some front line overdose prevention workers in Montreal say a nasal spray version of the potentially life-saving drug naloxone is too expensive to purchase for their clients and should be covered by Quebec's public health insurance. This week, Health Canada approved naloxone for over-the-counter, non-prescription use in Canada, but its price – $145 for two single-use doses of the spray version – is too high for some clinics in Montreal to purchase the drug. Jeremy Wexler, a social worker at a Montreal opiate-replacement clinic, was hoping his clinic would begin training families and friends of users on administering naloxone in case of an overdose. But he was shocked when he found out about the price of the nasal spray version. "We felt like the nasal spray is a big advantage, but we had to back away," Wexler told CBC Montreal's Daybreak. CBC News

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Nunavut plans territorial inquiry into missing and murdered women

People in Nunavut will get to weigh in on the national inquiry into missing and murdered Indigenous women and girls. That news was delivered in person by Keith Peterson, Nunavut's justice minister and Cambridge Bay MLA this week, in his hometown, at the Kitikmeot Inuit Association's annual general meeting. The plan, not yet formally announced, is to hold a special inquiry into missing and murdered Indigenous women and girls [MMIWG] for Nunavut, using the same terms of reference as for the larger national inquiry, announced this past August, said Peterson, speaking Oct. 5 to the AGM. For its inquiry, Nunavut has asked for the additional consideration of domestic violence, due to the high level of domestic violence in the territory, Peterson said. This expanded orientation was confirmed Oct. 6 by Nunavut Premier Peter Taptuna, who also came to the KIA meeting. Taptuna had already brought up that need last February, saying the inquiry should look "at the root causes around systematic domestic violence against women in Nunavut." While there are few missing Inuit women in Nunavut, Taptuna told *Nunatsiaq News* that he hopes the inquiry's look at domestic violence—which has led to the murder of many Nunavut women—will raise awareness nationally about that issue. Nunatsiaq Online

Missing, but never gone: KTC hosts walk for missing and murdered indigenous men and women
Keewatin Tribal Council (KTC) organized a march in honour of missing and murdered aboriginal men and women in Thompson Oct. 4, marching from the KTC offices to the southern bank of the Burntwood River. Family members of the missing and murdered stood in the October cold to share their grief and memories. Laura Wood-Labonte attended to speak for her cousin, Christine Wood, whose recent disappearance is currently the subject of an active police investigation (supplemented by a private detective, as well as searches by Winnipeg's Bear Clan). Wood-Labonte noted that the reality of a missing person is difficult to grasp, until it happens to someone close to you. "It's hard seeing my aunt and uncle every week, seeing the heartache in their eyes." She said that the RCMP have been investigating thoroughly and have kept the family informed; however, she notes that the tips investigators have been receiving are often weeks old. Wood-Labonte noted that individuals with information should report it immediately. "Even if you're unsure, time is precious." Not everyone was satisfied with the RCMP's performance, however. Marylin Flett of Tataskweyak Cree Nation, whose husband Raymond went missing in July 2015, had marched at a separate event earlier this year, near the anniversary of his disappearance. A year later, she and her family are still investigating the disappearance themselves, and continue to express frustration with local RCMP, who she states will not re-open the investigation. Nonetheless, she and her family continue to search for him to this day. "I was married to this man for 35 years. I didn't give up on him, and I won't give up now." Thompson Citizen

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

NIL

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

NIL

INTERNATIONAL

Hurricane Matthew battering Florida's northeast coast as governor warns: 'This is not over'
Hurricane Matthew churned along Florida's Atlantic coast Friday, looking increasingly like its center would remain just offshore as the storm battered the state with punishing rain, beach-swallowing sea surges and destructive wind gusts topping 100 mph. Even if Matthew avoids making landfall and Florida dodges

some of the worst-case scenarios laid out by forecasters and public officials in recent days, the storm still poses a considerable threat to residents from Florida to North Carolina. The strongest hurricane to menace the United States in a decade is continuing its trek north as it rumbles near the coastline, and forecasts warn that a dangerous storm surge of up to 11 feet could cause life-threatening flooding in as many as four states. Early Friday, the storm weakened to a Category 3 storm, but still packed dangerous winds of 120 mph that could threaten land if the storm drifts only slightly closer to shore. The National Hurricane Center reported that the hurricane's center was "hugging the coast" as the storm moved along the northern part of Florida, battering the northeastern coastal areas, and headed toward Georgia and South Carolina. "The storm has only passed half our state, so this is not over," Florida Gov. Rick Scott (R) said during a briefing Friday morning. Washington Post; NY Times

Haiti likely to be 'critical' for 18 months after Hurricane Matthew
The situation in Haiti has been described as 'critical' after it was battered by Hurricane Matthew. Christian Aid told Sky News it was likely to remain that way for 18 months. Prospery Raymond from the charity said: "The south part of Haiti is really affected by Hurricane Matthew. "The population are really in need of water, shelter, materials and in the coming days there will be a resurgence of cholera. "Compared to the earthquake this emergency is very, very critical." Local officials said late on Friday afternoon that the number of dead had risen to 842. Thousands of homes have been destroyed, while more than 60,000 people have entered shelters. The US Navy is sending the USS Mesa Verde to help with the relief effort. The amphibious transport dock ship is carrying food, medicines, baby formula, nappies and first aid supplies. It can also produce 72,000 gallons of fresh portable water each day. There is a surgical team on board and two operating theatres. Across the country, the International Red Cross said tens of thousands of people needed help as it launched a $6.9m appeal. Sky News; Reuters (Global News); NBC News; Global News

Hurricane Matthew could cause US$25-30B in insurance losses
A hurricane threatening the first direct hit on the United States in more than a decade could cause insurance losses of $25-30 billion and be the second costliest U.S. hurricane on record for insurers, according to initial industry estimates. Hurricane Matthew is just off the east coast of Florida near Cape Canaveral, the National Hurricane Center said in an advisory on Friday, after killing at least 339 people in Haiti on its move north through the Caribbean. Data modelling firm RMS has told clients its initial estimates were a 42 per cent chance of a US$20 billion insurance loss and a 26 per cent chance of a $30 billion loss from the hurricane, a source familiar with the research said. BNN

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE
t_dtm
.@Safety_Canada rétablit le financement en #USAR/#HUSAR; 2 nouvelles Canada Task Force seront créées: #Mtl, #Halifax http://nouvelles.gc.ca/web/article-fr.do?nid=1134389 ...

JClimAdapt
Public Safety Canada wants to engage with the private sector on disaster risk reduction and resilience #pwcclimaterisk #pwcdrr https://twitter.com/dgreenall123/status/784393633722146816

maintenant_mtl
Securite_Canada: Bénévoles sont le cœur de #RechercheSauvetage au Canada. Ns voulons votre opinion sur son avenir. Inscrivez-vs …

maintenant_mtl
Securite_Canada: Retour du financement Recherche & sauvetage milieu urbain aide forces opérationnelles pour équipe… http://nouvelles.gc.ca/web/article-fr.do?nid=1134389 …

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

PwC_Canada_LLP
"The Fort McMurray wildfire is the costliest insured disaster in Canadian history" Stephanie Durand of @Safety_Canada

LucyCasacia
Fantastic eye opener speech by Stephanie Durand @PwC_Canada_LLP @govt_of_canada @SiemensCanada #ResilientCities

PwC_Canada_LLP
We're engaging Canadian businesses to talk about reducing, managing climate, disaster #risk http://pwc.to/2dRLj2A #pwcclimaterisk #pwcdrr

HarjitSajjan
#BravoZulu to 9 Wing's 103 SAR Squadron, named 2016's best SAR squadron at National SAREX '16 #squadgoals http://www.ganderbeacon.ca/News/Local/2016-10-07/article-4658828/Top-squad/1 …

TheWindsorStar
'Zero' risk for local Zika transmission, says medical officer https://t.co/E9b2OjnyLM

timescolonist
Thousands without power as wind storm wallops Southern Vancouver Island and the Lower Mainland @environmentca http://www.timescolonist.com/news/local/thousands-without-power-as-storm-hits-vancouver-island-1.2360350 …

ChopperNews
Fishermen rescued near Scots Bay by #helicopter, waterproof phone - from @CBC : https://t.co/KBuBmXUODU

PEIGuardian
Summerside-based Cap Nord answers distress call from fishing boat: No one was injured and the four crewmember... https://t.co/yesrgWU6mJ

maintenant_mtl
environmentca: See how we're doing at warning Canadians when #SevereWeather is coming. #CdnEnv #Indicators …

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

canadianmv
Do you care about national security? Complete @Safety_Canada online consultation & have your voice heard: https://goo.gl/sy07ye #cdnpoli

NATIONAL SECURITY / SÉCURITÉ NATIONALE

cforcese
Tackling the Government Green Paper on National Security: Part 2 - Canadian Civil Liberties Association https://t.co/dmE896Jg5p

MichelleZilio
Kevin Garratt makes first public appearance after release from Chinese prison http://bit.ly/2dEtDDQ (via @globeandmail) #cdnpoli #cdnfp

globeandmail
In search of the triggers to Muslim radicalization http://trib.al/4381UfY @GlobeDebate

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

rp_browne
And Canada Border Services only started separating fentanyl from a broader category of drug seizures this May.

rp_browne

Canada Border Services told us they've seized only 8.46kg worth of fentanyl from May until late September: https://t.co/dqmlELl4M1

rp_browne
US Customs & Border Protection data shows 134 kg of fentanyl seized this year through mid-July, AP reports.

LAW ENFORCEMENT / APPLICATION DE LA LOI

rp_browne
AP on RCMP officers gearing up to deal w/ massive carfentanil seizure in June: "it looked as if they were preparing for a trip to the moon"

RCMPPEI
Police Joint Forces Operations make a number of arrests related to recent thefts - http://www.rcmp.gc.ca/en/news/2016/7/police-joint-forces-operations-make-a-number-arrests-related-recent-thefts …

GlobeBC
RCMP's apology for harassment is merely a first step toward a solution, writes @garymasonglobe http://www.theglobeandmail.com/news/national/rcmps-apology-for-harassment-is-merely-a-first-step-towards-a-solution/article32275335/ …

GlobalEdmonton
15-year-old boy turns himself in - with his mom - in what RCMP call an "error in judgement" #yeg #Fortsask http://glbn.ca/iEHUkP

GaryCunliffeCBC
Extortion scam circulating online in Leduc http://www.cbc.ca/news/canada/edmonton/extortion-scam-circulating-online-in-leduc-1.3795615 … #CBC #yeg #Leduc

cbcnewsbc
RCMP too big to fix, says former spokesperson Catherine Galliford http://ift.tt/2e9jbgy

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

quebectualite
☰ SRC ► Coup tiré lors d'une altercation au pénitencier de Donnacona http://ici.radio-canada.ca/regions/quebec/2016/10/07/002-donnacona-altercation-agent-correctionnel-detenu-blesse.shtml?utm_source=dlvr.it&utm_medium=twitter …

cyblesoleil
Un agent correctionnel de Donnacona tire sur un détenu https://t.co/lSpRJjeXTv

RadioCanadaInfo
Coup tiré lors d'une altercation au pénitencier de Donnacona http://rc.ca/MPyDPJ

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

HeatherWellsCBC
Fentanyl suspected in 3 overdose deaths in Winnipeg this week say @wpgpolice . Officers plan to begin carrying antidote, naloxone. @bkives

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

NunatsiaqNews
Nunavut plans territorial inquiry into missing and murdered women http://ow.ly/CMWY304XkOI

rcmpgrcpolice

#RCMP asks for your help in bringing our missing Indigenous women home #canadasmissing #MMIW http://rcmp.ca/-iNX

PUBLIC SERVICE / FONCTION PUBLIQUE

CBCKatie
Full story: Unions owed up to $2m in Phoenix fiasco, PSAC will pursue government for unpaid funds: https://t.co/7NuelXwic8

CBCKatie
Just reminded by PSAC - that although it is owed dues, the union says its top priority is getting members paid. #hw #Phoenix

OTHER / AUTRE

politicsca
Ottawa posts narrow $1 billion deficit for 2015-16 https://t.co/8lCLbVRNNX

CBCWorldReport
#Unemployment rate is unchanged at 7 per cent. In September, some 67-thousand jobs were created.More people 55 and older found jobs

INTERNATIONAL

NatObserver
As Haiti death toll rises to 842, Matthew slams into Florida, reports @cadamscadams http://tinyurl.com/hdu4h55 via @NatObserver

Reuters
MORE: U.S. National Guard expects flooding, rather than wind damage, as #HurricaneMatthew moves further north. http://reut.rs/2dyCevK

estNATO
BREAKING #Russian SU-27 violates #Estonia's airspace. Ambassador summoned to #MFA . #Russian air activity in region increased over past 48h

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

Sent to: !INTERNAL; !INTERNAL 2; CBSA Today's News; CSC & PBC Today's News; PS Today's News; RCMP Today's News; RCMP Today's News 2

Today's News / Actualités
October 10, 2016 / le 10 octobre 2016
9:00 - 18:00 ET

This collection contains news items that appeared online between 9:00 a.m. and 6:00 p.m., Eastern Time.

Ce recueil contient des actualités qui ont paru sur Internet entre 9h00 et 18h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

TOP STORIES / MANCHETTES

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Matthew remnants hit Atlantic Canada; wind, rain, flood risk
Parts of Atlantic Canada are set for a massive deluge, courtesy of moisture from Hurricane Matthew. The storm is no longer a hurricane, and its remnants are tracking away from the southeastern U.S., where it caused deadly flooding. Though it will not directly impact Atlantic Canada, it will still bring intense rainfall to areas of Nova Scotia and Newfoundland, where rainfall warnings are in effect. In Nova Scotia, the rain is already falling, moving east to west through the day, ending in the afternoon and evening after bringing a general 40-60 mm. "However over the eastern mainland Nova Scotia and parts of Cape Breton significantly higher amounts are possible and total amounts will likely exceed 100 millimeters in some areas," Environment Canada warns. Wind is also an issue across the Maritimes, with widespread gusts higher than 70 km/h on Monday afternoon. Northumberland Ferries has cancelled crossings between Caribou, N.S. and Woods Islands, P.E.I. until further notice. High winds have also caused restrictions on the Confederation Bridge, and the RCMP warns people to expect delays as they leave the island. Vehicle restrictions are in place for cars with trailers, motorcycles, highsided vehicles, tractor trailers, recreational vehicles, and buses. The Weather Network; CBC News

Why the risk of the 'Big One' in B.C. is heightened every 14 months - 1,000s of tremors — earthquake precursors in slow slip event — are expected on Vancouver Island
Roughly every 14 months, for about a two week period, seismologist Alison Bird won't park underground. That's because she knows the chances are higher of a big earthquake striking. Almost like clockwork, thousands of tiny tremors rumble unfelt across the Pacific Northwest indicating a 'slow-slip' event is taking place. Bird, an earthquake seismologist for the Geological Survey of Canada, says it's something scientists discovered at the office in Victoria when they noticed an unusual pattern on seismograms. "Every 14 months or so there's a sudden reversal of movement [of Vancouver island] for a couple of weeks," she said "It's buckling in that one direction but suddenly it settles a little bit ... it could be a last straw scenario, [where] just that little bit of extra stress that's going to cause that rupture to trigger ... the megathrust earthquake." CBC News

Climate change found to double impact of forest fires - Experts say both Canada and the U.S. must prepare for as western forests across North America grow warmer and drier and increasingly spawn wildfires that cannot be contained
Over the past 30 years, human-caused climate change has nearly doubled the amount of forest area lost to wildfires in the western United States, a new study has found. The result puts hard numbers to a growing hazard that experts say both Canada and the U.S. must prepare for as western forests across North America grow warmer and drier and increasingly spawn wildfires that cannot be contained. "Climate change is playing a substantial role in the variability of fire activity... and we expect that to continue into the future. The question is how are people going to respond to that," said John Abatzoglou, a climatologist at the University of Idaho and lead author of the study published Monday in the Proceedings of the National Academy of Sciences... Overall, they found that the amount of forest area that was dry enough to pose a high risk of wildfire grew by 75 per cent because of climate change, while the length of time during which there was a potential for wildfires grew by nine days per year. A key factor was the dramatic increase in the average dryness of the forest material that fuels wildfires. The analysis showed that just over half of that increase can be chalked up human-caused climate change. Globe and Mail

Uncharted waters: Mega-cruise ships sail the Arctic
A surge in Arctic tourism is bringing ever bigger cruise ships to the formerly isolated, ice-bound region, prompting calls for a clamp-down to prevent Titanic-style accidents and the pollution of fragile eco-systems. Arctic nations should consider limiting the size of vessels and ban the use of heavy fuel oil in the region, industry players said, after a first luxury cruise ship sailed safely through Canada's Northwest Passage this summer. The route, which connects the Atlantic and Pacific Oceans via the Arctic, was once clogged with icebergs but is now ice-free in summer due to global warming... Two shipping executives expressed concern that the one-off trip could become a trend, citing worries over safety, risks to the environment and the impact on small communities, in an area where there is no port between Anchorage

and Nuuk, in Greenland... Were a ship to be in trouble in the Northwest Passage, there would be little authorities could do given the lack of infrastructure, he said... Another concern is environmental. "Potentially, an accident involving a mega-ship could represent an environmental disaster," said Daniel Skjeldam, CEO of Hurtigruten, a cruise ship operator in the Arctic and the Antarctic, whose biggest ships can accommodate 646 passengers. Reuters

Energy East pipeline spill would affect Ottawa's drinking water within 48 hours
A new 30-page technical report commissioned by The Council of Canadians and Ecology Ottawa finds that a spill from the proposed 1.1 million barrel-per-day Energy East Pipeline could have catastrophic impacts on the Rideau, Mississippi and Ottawa rivers and put the region's drinking water at risk... The report by the independent Montreal-based technical firm Savaria Experts-Conseils Inc. finds that a spill in the Rideau River would impact Ottawa and Gatineau's drinking water within 48 hours and a spill in the Mississippi River would impact the drinking water for those cities after about 60 hours. Rabble

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

The 'New' CSIS Brings Secret Police to Canada - Third in a series to help you participate in the federal consultation on national security
An opinion piece by Michael Vonn, Policy Director of the BCCLA, states "While a democracy can incorporate the need for an intelligence agency to operate with considerable secrecy, there is no place in a democracy for a secret police. Full stop. The Canadian Security Intelligence Service was created to collect and analyze information about threats to national security. It is a civilian agency, not part of the police or military. It operates with a substantial amount of secrecy, like its approximate counterparts the CIA in the U.S. and MI5 in the U.K. Bill C-51, the Anti-terrorism Act from 2015, gave CSIS new powers beyond collecting intelligence on security and disseminating it to relevant sectors of the government. The new law amended the CSIS act so that now, if CSIS has 'reasonable grounds to believe' that an activity constitutes a threat to the security of Canada, it can 'take measures, within or outside Canada, to reduce the threat.'... There has been considerable debate about what kinds of actions ('measures') are authorized under this new law. The government's view is that these new powers do not allow CSIS to arrest individuals. It gives examples of 'threat reduction' that include modifying websites, interfering with communications, disrupting financial transactions and manipulating tools or devices. Leading national security scholars believe that the law would also authorize capture, detention, interrogation and rendition. So, although government stresses that CSIS does not have 'law enforcement powers,' what they could do in the name of threat reduction looks very much like the powers of a secret police." The Tyee

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Feds ban new embassies along Sussex Drive after RCMP flags security concerns
The federal government is forbidding the construction of new embassies on Ottawa's Sussex Drive following a stark RCMP assessment of the potential for "violent events" in the high-profile neighbourhood... Foreign Affairs Minister Stephane Dion was advised of the ban on new embassies in January by Daniel Jean, then his deputy minister, records released under the Access to Information Act show. Jean has since been named national security adviser to the prime minister... In summer 2015 the RCMP began a detailed assessment, at the request of Global Affairs Canada, of how construction of new embassies on vacant lots along Sussex Drive would affect the security of nearby Canadian and foreign facilities. The Mounties looked at "risks associated with violent events likely affecting Canadian and foreign interests," but not scenarios involving espionage or protection of critical infrastructure, such as power grids and water systems, says a letter to Global Affairs from RCMP Chief Supt. Rosemary Abbruzzese."In summary, and after considering a number of factors, the RCMP concludes and recommends that the only appropriate risk response is risk avoidance by not allowing any additional foreign missions to be located on Sussex Drive." Canadian Press (Metro News; iPolitics; Yahoo News); Radio-Canada

Nuances dans la position canadienne de ne pas négocier avec des ravisseurs étrangers
Le Canada exhorte officiellement ses pays alliés a faire comme lui et de ne plus verser de rançons aux ravisseurs. Mais quelle stratégie adoptée quand c'est un pays qui s'empare d'un de nos citoyen sous des prétexte fallacieux comme ce fut le cas tout récemment en Iran pour la canado-iranienne Homa Hoodfar? Interrogé il y a six mois sur la décapitation quelques jours plus tôt aux Philipines d'un premier touriste canadien, John Ridsdel, qui avait été kidnappé par le groupe Abou Sayyaf six mois auparavant, le premier ministre canadien avait martelé le message que le Canada ne paie pas et ne paiera jamais de rançon aux terroristes, directement ou indirectement. De préciser alors le premier ministre : « Nous ne voulons pas qu'un tel financement permette de commettre des actes terroristes contre des innocents. Payer des rançons pour des membres de notre nation mettrait aussi en danger la vie de tous les Canadiens qui vivent, qui voyagent et qui travaillent à travers le monde selon Justin Trudeau. Radio-Canada International

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Is Trudeau Really Revoking Citizenships at Record Rates?
Under Justin Trudeau, the Canadian government has revoked 184 citizenships. According to a CBC report released today, that's nearly as many revocations as the previous 27 years put together. These numbers may come as a surprise to anyone who has heard the prime minister speak on refugee and immigration issues. The CBC story sets Trudeau up as an opponent of citizenship revocation in the context of Bill C-24, which came into force in June 2015, and gave the government new powers to strip citizenship from Canadians convicted of terrorism. But Howard Anglin, former chief of staff to Jason Kenney's immigration ministry from 2011 to 2013, believes the uptick in citizenship revocations has little to do with Bill C-24 or marching orders from Trudeau. Anglin told VICE the jump from an average of 2.4 to 13 revocations per month under Trudeau is likely a holdover from the previous government. Vice News

Government officials were aware of arcane law that stripped Canadians born abroad of citizenship
The Canadian government was aware and warned repeatedly years before an arcane law began stripping longtime Canadians of their citizenship, says a man who spent decades lobbying for change. The law applies to people born between Feb. 15, 1977, and April 16, 1981, no matter how quickly after their birth they moved to Canada. It was rescinded in 2009, but the change didn't apply retroactively. The only way to prevent the automatic loss of citizenship was to apply to retain it before the age of 28 — a detail legal experts contend the government failed to adequately communicate to those affected. Janzen said he has heard numerous stories of people going to citizenship officials and being told they had never heard of the law. Canadian Press (National Post, Ottawa Citizen; Vancouver Sun)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

IAEA chief: Nuclear power plant was disrupted by cyber attack
A nuclear power plant became the target of a disruptive cyber attack two to three years ago, and there is a serious threat of militant attacks on such plants, the head of the United Nations nuclear watchdog said on Monday. International Atomic Energy Agency (IAEA) Director Yukiya Amano also cited a case in which an individual tried to smuggle a small amount of highly enriched uranium about four years ago that could have been used to build a so-called "dirty bomb"... "This issue of cyber attacks on nuclear-related facilities or activities should be taken very seriously. We never know if we know everything or if it's the tip of the iceberg." Amano declined to give details of either incident, but said the cyber attack had caused "some disruption" at the plant, although it did not prove to be very serious since the plant did not have to shut down its operations. He said he had not previously discussed the cyber attack in public... He said the attack was disruptive, not destructive, a term used to refer to incidents like the 2014 attack that destroyed data on computers of Sony Corp's Sony Pictures Entertainment and rendered some of its internal networks inoperable. Concerns about cyber attacks on nuclear sites have grown in recent years after the emergence of computer malware that can be used to attack industrial controls. Reuters

US required to declassify Yahoo spying order, say experts

he Obama administration "must declassify" a secret court order that forced Yahoo to scan the emails of its customers' emails as part of a surveillance program. The order, first disclosed by Reuters last week, directed the company "to siphon off messages containing the character string the spies sought and store them for remote retrieval" by the intelligence community. But questions remain over exactly how the intelligence community compelled the web giant to carry out the classified order -- specifically if Yahoo was forced to rewrite software at the behest of the order, or use an existing system designed to filter spam, as reported by The New York Times. California-based rights group the Electronic Frontier Foundation said in a blog post that provisions passed by Congress in the wake of the Edward Snowden revelations "require" the government to review the order for potential public release. Ordinarily, secret orders from the Foreign Intelligence Surveillance Court, which authorizes the government's surveillance requests, are never released. But Congress last year passed provisions in the Freedom Act, which replaces parts of the expired Patriot Act, after the government was found to have widely interpreted the law in secret to carry out mass surveillance. "If the reports about the Yahoo order are accurate -- including requiring the company to custom build new software to accomplish the scanning -- it's hard to imagine a better candidate for declassification and disclosure under Section 402," said Aaron Mackey, a legal fellow at the EFF. ZDNet

Data retention supported by two-thirds of Australians: ANU
A poll by the Australian National University (ANU) has found that over two-thirds of respondents support the federal government's telecommunications data retention laws for the purpose of protecting national security.The Attitudes to National Security: Balancing Safety and Privacy -- ANU poll July 2016 [PDF], conducted via a random phone survey of 1,200 individuals between June and July, found that 67 percent thought the retention of communications metadata is "justified as part of the effort to combat terrorism and protect national security". In addition, almost 70 percent approve of data retention for counter-terrorism purposes. ZDNet

LAW ENFORCEMENT / APPLICATION DE LA LOI

Surrey police seek missing woman Kyonghee Kim
Surrey RCMP are hoping tips from the public will help them find a missing 54-year-old woman who was last seen on Tuesday, Oct. 4. Four days later, police found Kyonghee Kim's grey 2012 Hyundai Sonata with B.C. licence plates 334 PXH in Golden Ears Provincial Park in Maple Ridge. She and the vehicle had been reported missing the day before by her family. CBC News

RCMP search Golden Ears Park but few details available
Concern is growing in Maple Ridge this morning after a large police presence in Golden Ears Park. Police had the entrance to the park blocked for several hours on Sunday. The RCMP's Emergency Response Team, along with police dogs were called in. But Ridge Meadows RCMP will only confirm they were carrying out some kind of search. It may be connected to the search for Kyonghee Kim, a 54-year-old Surrey woman missing since Tuesday. Global News

Missing Sask. teen Mekayla Bali believed to be in Vancouver
The mother of a missing teen from Yorkton, Sask. travelled to Vancouver to set up a poster campaign in hopes of finding her daughter. Mekayla Bali, 17, was reported missing by her family on April 12. Mekayla's mother Paula Bali spent one week putting up posters around Metro Vancouver after the RCMP received tips that Mekayla was in the area. According to police, Mekayla was last spotted at a bus depot in Yorkton where she ate lunch at a restaurant but did not buy a ticket or board a bus. Investigators are also looking for a man who may have been with her at the bus depot before she disappeared. CTV News

Police investigate after body found near Burnaby ravine
RCMP investigated the discovery of a body near a ravine in Burnaby Sunday afternoon. Several police vehicles have been in the area of North Road and Lougheed Highway for hours. The area is known to attract local homeless people living along the ravine. Police have not yet confirmed how the person died. CTV News

Creepy clowns no laughing matter: RCMP
Those who wish to participate in the creepy clown phenomenon currently taking place across North America, should reconsider as it could cost them time in prison. “It’s a criminal offence to deliberately alarm, frighten, or threaten people and when we see that, we’re going to investigate it,” said Grande Prairie RCMP Supt. Donnan McKenna. If somebody does commit a criminal offence, you have to remember, wearing a disguise makes it very, very serious: It’s an indictable offence that’s punishable by imprisonment up to 10 years.” McKenna noted that although it’s not illegal to wear a creepy clown mask or costume, he did say if his officers see these clowns on the street they will stop and investigate. “It hasn’t really been an issue here and I think that the tolerance level for that kind of nonsense in Grande Prairie is pretty low,” he said, stressing anyone who feels intimidated by someone wearing a costume should call the detachment. Grande Prairie Daily Herald-Tribune

Regina protesters prepare to gather on Indigenous Day of Action
Protesters say they'll gather at a Husky gas station in Regina Monday to demand action on Indigenous issues. They'll be part of protests across Canada to mark Indigenous Day of Action. Organizers say Indigenous "land and water protectors" will be joined by environmentalists and labour organizers at the gas station on the north end of the city. They want Prime Minister Justin Trudeau to commit to "deeds, not words" when it comes to Indigenous issues... The Husky brand has been in the news lately after a Husky oil pipeline ruptured earlier this year, releasing as much as 250,000 litres of oil and chemicals into the North Saskatchewan River. CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

The crown jewel of prisons: In search of a new purpose
Having swapped guarded inmates for guided tours, the future of Kingston’s historic penitentiary remains unknown, though full of potential. The Kingston Penitentiary stands idle and empty; an unlikely marker of time, no longer a guardian of secrets but now a custodian of history. There’s a nervousness in the air now— an uncertainty so pervading that even the cool summer breeze of Lake Ontario cannot calm it. Change is coming. As Canada’s oldest and most infamous prison, Kingston Penitentiary, originally called the “Provincial Penitentiary of the Province of Upper Canada,” or the “Provincial Penitentiary,” sits on 8.6 hectares of land located on King Street West in Ontario’s historic City of Kingston. With a sordid past as long as its roll call of famous former inmates, ‘Kingston Pen’ or ‘KP’ as it’s become known to Kingstonians has housed some of the country’s most notorious criminals. For 178 years, this fortress played host to countless thieves, murderers, rapists and the like, ranging from women and children to the infamous Paul Bernardo and ex-Col. Russell Williams. Hill Times

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NIL

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Cadieux: Embrace pot shops and marijuana

An opinion piece states, "A year into the new post-Stephen Harper era, it doesn't look like much has changed. We've done right by some 30,000 Syrian refugees, and ruffled a lot of feathers with the most recent carbon-pricing initiative, but everything else seems to be business as usual. But one thing that has quickly changed, party because of the Liberal party's platform, is the plethora of medicinal marijuana clinics that have cropped up all over the country, including Ottawa, even though they're not entirely legal – yet… Tetrahydrocannabinol (THC) is the compound responsible for the addictive psychotropic effects one gets from marijuana, and it seems to be causing all the flap. Yet there are other critical compounds in the plant, namely the cannabinoids, which latch onto none other than the body's own cannabinoid receptors within the nervous system and – you guessed it! – relieve pain… Our pharmacopoeia of painkillers is filled with faulty options and bad ideas – addiction and psychotropic side effects included – yet for some reason it's nothing short of a scandal when a medicinal marijuana clinic opens up in a neighbourhood. So how do we handle this new reality, then? We get over it, that's how. And we give it a chance. I am not saying we should all rally around the 4/20 movement, nor am I hopping on the miracle-cure bandwagon, but I am saying that the data are pouring in, and it's hard to deny that the unbiased and objective results collected by our freshly unmuzzled researchers, along with their international counterparts, point in a direction that we should take under serious consideration…" Ottawa Citizen

Ontario's medical pot vaping exemption came from consultations with two people
Ontario's Liberal government defended allowing medical marijuana users to vaporize anywhere by saying they had consulted "very broadly" -- but emails show those consultations involved the input of just two people, The Canadian Press has learned. Ultimately, the associate health minister had to defend the policy for just one day after the government backtracked on the policy within 24 hours… The new e-cigarette regulations banned the use of the devices anywhere regular cigarettes were prohibited. But the government provided an exemption for medical marijuana users, meaning they could have vaped in restaurants, at work or on playgrounds. The exemption became public Nov. 25 and by the next day, Dipika Damerla, then the associate health minister, said that based on the feedback the government had received, they were going back to the drawing board. The government ultimately decided there would be no exemption. Canadian Press (CTV News)

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Canadian military to consider leaving sex crimes with civilian courts
The Canadian Forces has launched the first internal review of the military justice system in generations and among the issues being looked at is whether all military sexual crimes should be handled by civilian courts. The military justice system has been under the microscope over the last two years following complaints that many sexual crimes committed by service members have been glossed over or ignored. Currently, such offences can be referred to either civilian court or the military court system for a court martial, depending on the circumstances. But Col. Robert Holman, the Canadian Forces' deputy judge advocate general for military justice, says that could change. Canadian Press (Toronto Star)

INTERNATIONAL

UPDATED : Syrian, Feared to Be Planning Bombing, Is Arrested in Germany
The German police arrested a Syrian man early Monday who was suspected of plotting a bombing, bringing an end to a weekend manhunt that renewed fears about a threat posed by extremists among the nearly one million refugees and migrants who arrived in Germany last year. Federal prosecutors said the suspect, Jaber al-Bakr, 22, was "urgently suspected of planning and had already taken concrete steps to plan an Islamic-motivated explosive attack in Germany." Security officials in the eastern state of Saxony said they had found the same explosive materials in the suspect's apartment as those used in Islamic

State attacks in Europe. Jörg Michaelis, president of the police in Saxony, said that Mr. Bakr had been arrested in Leipzig, in the apartment of fellow Syrians who had recognized the man from photographs circulated by the authorities over the weekend. The Syrians tied up the suspect and took a photograph of him with a cellphone, which one of them took to a nearby police station, before urging officers to come and arrest him immediately. New York Times

The Latest: No evidence German bomb suspect had firm target
Federal prosecutors in Germany say there is no evidence a young Syrian man arrested in an alleged bomb plot Monday had picked a target to attack. Federal prosecutors said in a release Monday that police found some 1.5 kilograms of an "extremely dangerous explosive" and other material in the apartment where 22-year-old Jaber Albakr had been staying in Chemnitz. They say Albakr allegedly was "planning an Islamist motivated attack with high explosives in Germany" but so far investigators have no evidence he "already had a concrete target for his bombing attack." They say Albakr had been searching online for instructions on how to make explosives and "equipment for jihad" at least since the beginning of the month. Canadian Press (Yahoo News)

'Like a nuclear bomb,' cholera and destruction after hurricane in Haiti
Patients arrived every 10 or 15 minutes, brought on motorcycles by relatives with vomit-covered shoulders and hoisted up the stairs into southwest Haiti's Port-a-Piment hospital, where they could rest their weak, cholera-sapped limbs. Less than a week since Hurricane Matthew slammed into Haiti, killing at least 1,000 people according to a tally of numbers from local officials, devastated corners of the country are facing a public health crisis as cholera gallops through rural communities lacking clean water, food and shelter… Out on the streets, the scene was also shocking. For miles on end, almost all the houses were reduced to little more than rubble and twisted metal. Colorful clothes were littered among the chaos. The region's banana crop was destroyed with vast fields of plantain flattened into a leafy mush. With neither government or foreign aid arriving quickly, people relied on felled coconuts for food and water. The stench of death, be it human or animal, was everywhere. Reuters

North Carolina flood dangers rise in Hurricane Matthew's wake
Hurricane Matthew is gone, but the disaster its rains unleashed will slowly unfold all this week as rivers across eastern North Carolina rise to levels unseen since many of the same areas were destroyed by a similar deluge from Hurricane Floyd in 1999. Emergency planners are now using models that can pinpoint exactly how high the rivers can get and which buildings will be flooded days in advance. But they can't predict dams and levees breaking from the stress of more than a foot of rain in some places… The storm killed more than 500 people in Haiti and at least 21 in the U.S. — nearly half of them in North Carolina. Most were swept away by flood waters. McCrory and others fear the death toll may rise as impatient people drive around road barricades into swiftly moving floodwaters. Globe and Mail

Italy Expels Tunisian Accused of Supporting Islamic State
Italy says it has expelled a Tunisian man who pledged support to the Islamic State group on his Facebook page and was allegedly planning to go to the Syrian-Iraqi region to fight. Monday's expulsion marked the 122nd person Italy has kicked out since January 2015 on security grounds related to Islamic extremism. Interior Minister Angelino Alfano said the investigation was conducted alongside French authorities because the Tunisian, who came to Italy in 2003, was in touch with an underage Frenchwoman of Italian origin. Alfano said that French authorities had identified him from his activity on a jihadi chat board, adding that he "clearly intended to reach the Syrian-Iraqi theater." A plane carrying the 32-year-old left Palermo, Sicily, on Monday, bringing to 56 the number of people kicked out this year. Associated Press (ABC News)

U.S. Navy ship targeted in failed missile attack from Yemen: U.S.
A U.S. Navy guided missile destroyer was targeted on Sunday in a failed missile attack from territory in Yemen controlled by Iran-aligned Houthi rebels, a U.S. military spokesman told Reuters, saying neither of the two missiles hit the ship. The attempted strike on the USS Mason, which was first reported by Reuters, came just a week after a United Arab Emirates vessel came under attack from Houthis and suggests growing risks to the U.S. military from Yemen's conflict. Reuters

UN chief urges independent investigation of Yemen attacks
Secretary-General Ban Ki-moon on Monday urged the U.N. Human Rights Council to immediately establish an independent body to investigate rights abuses and other violations in Yemen, especially following last weekend's "horrendous attack" on a funeral hall reportedly by the Saudi-led coalition. The U.N. chief told reporters that Saturday's airstrikes in Yemen's capital Saana, which killed over 140 people and injured more than 525 others, were the latest disasters in the Yemen conflict, which has left over 20 million people — "an astounding 80 per cent of the population" — in need of humanitarian aid. "Aerial attacks by the Saudi-led coalition have already caused immense carnage and destroyed much of the country's medical facilities and other vital civilian infrastructure," Ban said. "Bombing people already mourning the loss of loved ones is reprehensible." "This latest horrific incident demands a full inquiry," he said. "More broadly, there must be accountability for the appalling conduct of this entire war." Earlier Monday, U.N. human rights chief Zeid Ra'ad al-Hussein denounced the airstrikes and faulted the Human Rights Council for not doing more in the face of a "climate of impunity" in the impoverished, war-torn country. Associated Press (Metro News)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

redwoodwoof
@RalphGoodale Thank you for your support of Canada's first responders!

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

MacleansMag
Fort McMurray says thanks to Canadians http://ow.ly/ZqAz3050XDW

CBCCanada
Why the risk of the 'Big One' in B.C. is heightened every 14 months http://ift.tt/2dWTHJM

JustinTrudeau
Action de grâce difficile pour les gens touchés par les inondations et la pluie au Canada atlantique. Restez prudents & en sécurité ce soir.

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

TheTyee
The 'New' CSIS Brings Secret Police to Canada http://thetyee.ca/Opinion/2016/10/10/New-CSIS-Secret-Police-Canada/?utm_source=twitter&utm_medium=social&utm_content=101016-2&utm_campaign=editorial-1016 … #cdnpoli

NATIONAL SECURITY / SÉCURITÉ NATIONALE

CBCManitoba
CSIS, Bill C-51 and Canada's growing metadata collection mess http://ift.tt/2e7vjsV

hscoffield
Feds ban new embassies along Sussex Drive after RCMP flags security concerns http://ow.ly/yzh63052rTt #cdnpoli via @JimBronskill

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

vicecanada
Is Trudeau really revoking citizenships at record rates? https://t.co/rAFtSWYhOe

VancouverSun
'28-year rule' catches hundreds who had Canadian citizenship revoked https://t.co/khzjSlvM3o

CYBER SECURITY / CYBERSÉCURITÉ

ReutersWorld
IAEA chief: Nuclear power plant was disrupted by cyber attack

ZDNet
US required to declassify Yahoo spying order, say experts http://zd.net/2dqFuUM @zackwhittaker

LAW ENFORCEMENT / APPLICATION DE LA LOI

GlobalBC
RCMP search Golden Ears Park but few details available https://t.co/Ga2H0WHhjb

OACPOfficial
Our female cops rock! Representing the very best of Canadian policing. U make all our officers proud @OWLE1 @rcmpgrcpolice @CACP_ACCP https://twitter.com/OWLE1/status/785419593925926912

berryonline
Thx to @RCMPONT, @OPP_News, @WRPSToday & @CityKitchener security for making our @KW_Oktoberfest keg-tapping safe! #CanadasSafestMayorsOffice

SurreyRCMP
Join us for a Neighbourhood Safety Meeting October 13th at École Woodward Hill Elementary School. @Cloverdale_BC @Newton_BIA

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

peggylam
For those located in Prince George @TheCurrentCBC is hosting a public forum about #MMIWG on Oct.13 https://t.co/LFWbpNkrZ0

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

motherboard
A weed grower with a GoPro takes us inside a cannabis farm http://bit.ly/2dKsPhC

OCHeadlines
Cadieux: Embrace pot shops and marijuana - A year into the new post-Stephen Harper era, it doesn't look like mu... http://ow.ly/5h5i505iyCx

HuffPostCanada
An inside look at one of Canada's new licensed cannabis producers, by @zanneslaw http://huff.to/2dT2Ebq

INTERNATIONAL

nytimes
The German police arrested a Syrian man who is suspected of plotting a bombing, ending a weekend manhunt http://nyti.ms/2dNhw7s

HuffingtonPost

The death toll from #HurricaneMatthew tops 1,000 in Haiti http://huff.to/2dNXkCB

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

Today's News / Actualités
October 18, 2016 / le 18 octobre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

At one year in power, the Liberals have yet to face a major national security test
An opinion piece by national security expert Wesley Wark states, "The Liberal government, in its first year in power, has enjoyed the benefit of a highly advantageous environment for national security policy making: a majority in Parliament; ineffective political opposition; no terrorist attacks; a public whose attention is largely elsewhere. The pressure has been off and the government has been able to pursue its agenda at a measured pace. (…) A second major promise concerns a millstone left around the new government's neck by the passage of the Harper's government's anti-terrorism legislation (the contentious Bill C-51) in 2015. The Liberals promised to repeal its "problematic elements" and ensure a better balance between security and rights for Canadians. While the Liberal government has signalled

what it thinks the problematic elements are, its caucus may have different ideas and certainly opposition parties do. (…) The most radical promise the Liberals made was to consult Canadians and increase transparency around intelligence and security issues. In fulfilling this promise, the government launched in September a "Green" (discussion) paper on national security, addressing 10 issues about which it encourages public discussion and input. An online portal is open until Dec. 1 and has already seen some 8,000 responses. In addition, the government has consulted with experts and stakeholders; the parliamentary Standing Committee on Public Safety and National Security is touring the country, holding "open mic" sessions; **Public Safety Minister Ralph Goodale** is on the road; and even his officials have been thrust onto the public parapet. How the government will digest and respond to the Green paper exercise remains to be seen. But this is an unprecedented and welcome experiment, whether it succeeds, fails or fizzles." Ottawa Citizen

TOP STORIES / MANCHETTES

Anger flares as wildfire-hit Canadian city struggles to rebuild
Some five months after the wildfires that devastated Fort McMurray were extinguished, anger over red tape and the slow pace of insurance payouts and permit issuance is flaring in the remote northern Canadian city. More than 1,900 structures were destroyed by the wildfire last May, which forced the evacuation of about 90,000 residents and shut in more than a million barrels per day of crude output from the area around Canada's oil capital in the province of Alberta. Around 80,000 people have returned, according to Red Cross estimates, but most of those who came back to find their charred houses gutted by the fire have yet to start rebuilding as city officials and insurance companies struggle to deal with Canada's costliest disaster ever. Making the situation worse, the region's harsh winter weather is set to raise construction costs and slow progress in rebuilding even further, residents say. "People are mad and companies are mad, there have been lawsuits filed. Nobody trusts a word the city says," said Kevin Lewis, a local demolition company owner who was forced to leave during the fire but came back to find his house still standing (…) Marc Fortais, recovery team chief of staff for the Regional Municipality of Wood Buffalo (RMWB), which governs the city and local area, said the frustration of resident is understandable. Reuters

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Anger flares as wildfire-hit Canadian city struggles to rebuild
Some five months after the wildfires that devastated Fort McMurray were extinguished, anger over red tape and the slow pace of insurance payouts and permit issuance is flaring in the remote northern Canadian city. More than 1,900 structures were destroyed by the wildfire last May, which forced the evacuation of about 90,000 residents and shut in more than a million barrels per day of crude output from the area around Canada's oil capital in the province of Alberta. Around 80,000 people have returned, according to Red Cross estimates, but most of those who came back to find their charred houses gutted by the fire have yet to start rebuilding as city officials and insurance companies struggle to deal with Canada's costliest disaster ever. Making the situation worse, the region's harsh winter weather is set to raise construction costs and slow progress in rebuilding even further, residents say. "People are mad and companies are mad, there have been lawsuits filed. Nobody trusts a word the city says," said Kevin Lewis, a local demolition company owner who was forced to leave during the fire but came back to find his house still standing (…) Marc Fortais, recovery team chief of staff for the Regional Municipality of Wood Buffalo (RMWB), which governs the city and local area, said the frustration of resident is understandable. Reuters

Millions participate in annual earthquake readiness drills
More than 19 million worldwide are set to participate Thursday in the Great ShakeOut Earthquake Drills, an annual event that promotes earthquake preparedness. At 10:20 a.m. local time, participants in homes, schools and businesses will practice the "drop, cover and hold on" drill, which involves dropping to the ground, crawling for cover under a nearby desk or table and holding on securely until the earthquake

stops. The ShakeOut began in Southern California and has since grown to include participants across the USA and in Japan, Southern Italy, New Zealand and parts of Canada. USA Today

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Snowden says Trudeau afraid to kill anti-terrorism bill
Whistleblower. Hero. Traitor. Patriot. These words and more have been used to describe former cybersecurity contractor Edward Snowden, who in 2013 copied and distributed thousand of documents to reporters and whose stories of Western intelligence agencies — including Canada's Communications Security Establishment (CSEC) — shook the world. This morning Snowden told the the annual SecTor cyber security conference in Toronto that Prime Minister Justin Trudeau want to amend the controversial Bill C-51 anti-terrorism law and not repeal it because he "is afraid of being attacked for being soft on terrorism." Speaking by video from Russia, where he fled to avoid prosecution by U.S. authorities, Snowden said the legislation, needs three fixes: First, a judicial body should have oversight over federal intelligence agencies that has the power to prosecute authorities that have broken the law. Second, because intelligence agencies are trading personal information of citizens "like baseball cards" citizens should be told if the data sharing hasn't led to an arrest for criminal activity. And finally, what Snowden called the criminalization of speech through vague definitions of terrorism should be taken out of C -51. A lot of what police call terrorism is the activity of what he called "common criminals" or those who are trying to make a political point but don't constitute a "super criminal threat." IT World Canada

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Customs Tariff Classification Of Hockey Gear Goes To Ultimate Referee: The Supreme Court Of Canada
On September 29, 2016, the Supreme Court of Canada ("SCC") issued a significant judgment on customs tariff classification. As noted in the majority opinion of Justice Russell Brown, Canada (Attorney General) v. Igloo Vikski Inc.1 represents the SCC's first foray into the world of Canada's Customs Tariff - federal legislation that adopts the World Customs Organization's "Harmonized System". The ruling includes an important analysis of the Canadian "General Rules for the Interpretation of the Harmonized System" (the "General Rules"). The Canada Border Services Agency ("CBSA") brought this appeal from a 2014 decision of the Federal Court of Appeal ("FCA").4 That decision overturned a ruling of the Canadian International Trade Tribunal5 ("CITT" or "Tribunal") which had, in turn, upheld the decision of the President of the CBSA to classify goaltender ice-hockey gloves imported by Igloo Vikski Inc. ("Igloo") under heading No. 62.16 of the schedule to the Customs Tariff as "gloves, mittens and mitts" rather than under heading No. 39.26 as "other articles of plastics", as requested by Igloo. Mondaq

Brampton man with bogus Canadian citizenship jailed 15 years for cocaine smuggling at Pearson airport
A Brampton man has been jailed 15 years in a case in which nearly $3 million in cocaine was smuggled into Canada via Pearson International Airport. Bruno Anigwe, 43, was convicted by a jury of importing cocaine, possession for the purpose of trafficking, conspiracy to commit an indictable offence and possession of a counterfeit mark (Canadian citizenship). Co-accused Nestor Nnaji, 43, was acquitted of similar charges in the trial before Superior Court Justice Gordon Lemon in Brampton court. Anigwe was sentenced to a total of 15 years in jail, including 12 years for importing cocaine and an additional three years for the fake Canadian citizenship. Anigwe attempted to appeal his conviction and sentence to Ontario's top court. But, the Ontario Court of Appeal dismissed the case. Brampton Guardian

Feds want review on huge tariff on drywall imports
The federal government is asking for a quick review of anti-dumping duties on drywall imports that have hiked the cost of construction in western Canada. In September the Canada Border Services Agency slapped tariffs of up to 276 per cent on U.S gypsum board or drywall imported from the U.S. for use in B.C., Alberta, Saskatchewan, Manitoba, Yukon and Northwest Territories. The agency said it was responding to a complaint that the products are being sold in Canada at less than normal prices. The

federal finance department has asked the Canadian Trade Tribunal to hold an inquiry on the duties and report its findings by early January. There is some gypsum production in western Canada, but not enough to meet demand, so extra product must be imported from the U.S. CJOB AM 680

Ontario senior booked of 14 child-porn charges
A 71-year-old northern Ontario man has been booked with 14 charges on account of an international child pornographic investigation. Police said search warrants executed at two Sudbury homes, brought to light the seizure of computers alleged of having child pornographic films and has evidences relating to the purchases of the same. 71-year-old Jean Pierre Melaye has been charged with eight counts of possession of child pornography and six counts of accessing child pornography. The investigation also involved the U.S. Federal Bureau of Investigation, Royal Canadian Mounted Police and the Canada Border Services Agency, Sudbury police informed. India Blooms

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Obama's Concerned an AI Could Hack America's Nukes
During his eight years in office, President Barack Obama has seen hackers grow into a threat no president has faced before. US intelligence and law enforcement agencies have responded to everything from a Chinese hack of Google in 2009 to Russian digital meddling in this election. He's learned, as a result, to think a few moves ahead. And that includes preparing for possibilities that others might consider science fiction—like the possibility of an artificial intelligence trained through machine learning and tasked with stealing US nuclear codes. In an exclusive interview with MIT Media Lab director Joi Ito and WIRED Editor-in-Chief Scott Dadich, Obama discusses the possibilities—and possible dangers—of AI. In an era when hackers can steal the fingerprints of 5.6 million federal employees and or pull off a modern version of Watergate, he wonders whether sophisticated adversaries might use AI to infiltrate the government's most sensitive systems (…) This notion of an artificially intelligent hacker or hacking tool is more than prognostication. The Pentagon's Defense Advanced Research Projects Agency is developing AI software for both offense and defense. Wired Magazine (2016-10-12)

LAW ENFORCEMENT / APPLICATION DE LA LOI

Surrey RCMP Constable Dario Devic charged with luring a child
The Criminal Justice Branch (CJB) of the Ministry of Justice announced on Tuesday that a charge of luring a child has been approved against Surrey RCMP Constable Dario Devic as a result of an investigation into conduct that is alleged to have occurred between August 29 and September 7 at or near Surrey. The charge alleges communications during this period between Devic and person he believed to be under the age of 16. It is an offence to communicate by means of telecommunication with a person who is under the age of 16, or who is believed to be under the age of 16, for the purpose of facilitating sexual conduct. On September 9, Surrey RCMP arrested Devic in relation to this matter and laid an information under the Criminal Code charging him with luring a child and breach of trust by a public officer. He was released on bail. The RCMP subsequently sent a report to Crown Counsel to the CJB for formal charge assessment. Indo-Canadian Voice; CBC News

Police Join Forces To Make Human Trafficking Arrests
A joint police effort has resulted in numerous charges in a human trafficking investigation, and the rescue of sixteen victims forced to work in the sex trade. Thirty-six police forces from across Ontario, including Toronto, Halton and Peel, worked on Operation Northern Spotlight, and charged twenty-five suspects with nearly seventy offences. Charges include making and distributing child pornography, child luring and exercise control. Names have not been released. iNews 880; Metro News; Radio-Canada

Des fraudes de type « client mystère » signalées au Nouveau-Brunswick
La Gendarmerie royale du Canada dit avoir reçu des appels à propos d'une fraude ayant cours dans le comté de Charlotte dans le sud-ouest du Nouveau-Brunswick. Des résidants ont reçu de faux chèques par la poste avec une lettre leur demandant de déposer le chèque dans leur compte personnel et

d'acheter des articles pour l'expéditeur. On leur promettait de faire un profit. La GRC signale cependant que dans tous les cas, la victime ne réalise aucun profit et pourrait être obligée de payer quand on découvre que le chèque est un faux. Les enveloppes et les lettres pourraient contenir les mots « Mystery Shopper Survey » ou un autre faux nom de compagnie. Presse canadienne (Acadie-Nouvelle)

Graydon makes push for RCMP recognition
Emerson MLA Cliff Graydon is leading the charge to have Royal Canadian Mounted Police honoured with a day of recognition in the province. Graydon has introduced legislation to make Feb. 1 an annual day in Manitoba to commemorate and show appreciation for the RCMP, and for the work they do to protect and serve Manitobans and people across Canada. The RCMP were first formed on the same date in 1920. "The Mountie and the Royal Canadian Mounted Police are among Canada's most recognizable symbols," said Graydon in a release. "The brave men and women of the RCMP serve Manitobans and all Canadians with distinction and give much in terms of service and sacrifice to our communities. The Carillon

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Researcher Reveals Temporary Prison Releases Benefit Inmates' Return to Society
Carleton University's Maaike Helmus, adjunct research professor in the Department of Psychology, has examined the effectiveness of temporary absences from prison and found they benefit prisoners returning to society. "Temporary absences reduce post-release unemployment, returns to custody and reoffending rates," said Helmus. "There's a dosage effect. The more absences an inmate receives, the better their outcome." The research study, published last week, tracked post-release outcomes of over 27,000 inmates released from federal prison between 2005-2011. Correctional Service of Canada has the power in advance of an inmate's parole eligibility, to allow offenders to receive a Temporary Absence (TA) from prison. These absences can either be escorted or unescorted and can vary in duration. The releases encourage inmates to maintain family and community ties and to take advantage of rehabilitative activities, while supporting a gradual release program. They allow inmates to demonstrate appropriate community behaviour and suitability for additional forms of conditional release. Exchange Magazine

Dennis Oland's lawyer says 'mistake' about jacket not a sign of guilt
Dennis Oland's lawyer says Oland made an honest mistake about what he was wearing the day his millionaire father was bludgeoned to death, and it's unreasonable for the Crown to suggest he was trying to mislead police. Alan Gold told the New Brunswick Court of Appeal Tuesday that Oland was not intentionally lying when he told police he was wearing a navy jacket on the day Richard Oland was killed. The jacket he was wearing, a brown Hugo Boss, was later found to have minuscule blood stains and DNA matching Richard Oland's profile on it. Gold, who is seeking to overturn Dennis Oland's murder conviction, said there was no indication of guilt because of the fact the jacket was taken to the dry cleaners the day after Oland was questioned by police. Canadian Press (Metro News)

Convicted sex offender backs out of school board race after crimes come to light
A convicted sex offender running in the Saskatoon Catholic school board election is no longer on the ballot after dropping out of the race. Denis Robert Hall announced his decision to withdraw his candidacy late Monday in a prepared statement reported by the Saskatoon StarPhoenix. He stated media reports describing his previous sex crimes "misrepresent me and my ancient past in the worst possible light," adding it prevented him from continuing as a candidate. (…) Hall received a full pardon in 1994. According to the 1985 Criminal Records Act, this means the Parole Board of Canada believed he was "of good conduct" and the conviction "should no longer reflect adversely on the applicant's character." CKOM 650

'Internet Black Widow' Melissa Ann Shepard agrees to sign new peace bond
An 80-year-old woman known as the "Internet Black Widow," who gained notoriety for killing and poisoning her intimate partners, has agreed to sign a two-year peace bond at the end of the month. Melissa Ann Shepard appeared briefly during a hearing in provincial court in Dartmouth, N.S., Tuesday morning. The hearing was related to her challenge of 22 conditions imposed on her when she

was released from prison in March after serving a full sentence of just under three years for spiking newlywed husband Fred Weeks's coffee with tranquilizers in 2012 at a bed and breakfast in Cape Breton. He and Shepard had only been married a few days before he fell ill. (…) Shepard is considered a high risk to reoffend by both the police and the Parole Board of Canada. The Crown applied under the Criminal Code to impose special conditions on her freedom. CBC News

New report reveals 'alarming' use of solitary confinement in Ontario jails — 939 days of continuous segregation for one inmate

Nearly one in five inmates in Ontario spent time in a solitary confinement cell over the final three months of 2015, statistics that Ontario's Human Rights Commission said reveals an alarming and systemic overuse of segregation in the province. In a new report released Tuesday, the human rights commission said 19 per cent of all Ontario inmates – or 4,178 people – were in segregation at one point or another between October and December of last year. Nearly half of the prisoners who were placed in segregation, or 1,889 individuals, were segregated multiple times. The report said that nearly 40 per cent of the 4,178 inmates placed in segregation, or 1,594 inmates, had a mental health alert on their file, the human rights commission said. Roughly 1,383 of the segregation placements were for 15 days or longer, they said, including one inmate who had been in continuous segregation for 939 days. (…) The report notes Ontario's use of segregation is much higher than in the federal correctional system, where use of administrative segregation has dropped by nearly 40 per cent since April 2014, the report said. Ottawa Citizen

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Take-Home Naloxone Program launches in North Battleford

As part of Saskatchewan's expanding Take-Home Naloxone Program, THN kits will be available in North Battleford, starting Thursday. The program is being launched by Prairie North Health Region in partnership with the Ministry of Health, Battle River Treaty Health Centre and Battlefords Sexual Health Clinic. The THN kits will be available free of charge to individuals at risk of an opioid overdose. The kits can be obtained at the Battlefords Sexual Health Clinic between 9:30 and noon on Thursdays. At-risk individuals must first receive education on overdose prevention, recognizing and responding to an overdose and proper administration of Naloxone using the THN kit. The THN kit is then provided to the individuals at risk. Family members and friends are welcome and encouraged to participate in the training. The Battlefords Sexual Health Clinic is located in downtown North Battleford at 1192 – 101 St. Battleford News Optimist

De nombreux appels pour dénoncer les abus de policiers envers les Autochtones

Des dizaines d'Autochtones ont fait de nouvelles dénonciations d'abus commis par des policiers au moyen de la ligne téléphonique mise en place par le gouvernement du Québec pour inciter les femmes autochtones à briser le silence. Les dénonciations qui ont été faites au cours des derniers mois visent des agents de la Sûreté du Québec (SQ), mais également des policiers municipaux et des agents des corps policiers autochtones. Selon nos informations, au moins 75 appels ont été faits à cette ligne téléphonique jusqu'à présent. Les dénonciations proviennent d'un peu partout au Québec. Elles sont faites par des femmes, mais également par des hommes qui ont décidé de briser le silence, ce qui a étonné les représentants des Services parajudiciaires autochtones du Québec. « On ne pensait pas que les hommes avaient eu ce genre d'aventure là. Majoritairement, ce sont des agressions tant physiques que sexuelles […] La brutalité policière, c'est un cas assez fréquent; le harcèlement sexuel, c'est un autre cas. Il y aussi l'intimidation, les policiers font de l'intimidation envers les Autochtones », dit Jean Jolicoeur. Radio-Canada

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

MMIW families still waiting for promised help, Bernadette Smith says
The Manitoba government needs to step up with support programs and services that were promised to families of missing and murdered Indigenous women and girls, says Bernadette Smith, whose sister has been missing for eight years. In unveiling details of the inquiry earlier this year, the federal government said it would allocate $11.7 million over three years for provinces and territories to establish family information liaison units within their existing victims services departments. The units are meant to complement the work of the inquiry by supporting families seeking information about their loved ones from government institutions — including police, prosecutors, coroners and child protection services. (…) Little has been done in Manitoba since the federal money was distributed to the province months ago, said Smith, whose sister, Claudette Osborne, was 21 years old when she disappeared in 2008. "We've had numerous women go missing or be murdered across Canada while they figure this out," Smith said on Tuesday. "They've had a long time to figure this out, and I think it's time for action." (…) A spokesperson for Justice Canada told The Canadian Press that funding for family information liaison units is being directed to the provinces and territories because most of the information families are seeking is held by government institutions, which existing victims services are able to access, while at the same time being regulated by privacy legislation and accountability frameworks. CBC News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

New poll says Canadians support the idea of independent pot retailers; few support liquor store sales of cannabis
It's going to be a big business: One Bay Street economist figures pot retailers will sell $10-billion a year worth of cannabis products. I've seen estimates that the Canadian market could grow to $20-billion a year. To put that in perspective, Statistics Canada says Canucks bought $9-billion worth of beer 2014-2015. So this cannabis market could be bigger than beer! So where are we going to buy these cannabis products? Right now, the only legal way to acquire cannabis products is by mail from a licensed producer. Purchasers need a prescription. But there's a booming market — grey at best, black at worst — of what are called pot dispensaries, storefront operations where you can walk in and — so long as you've got an easily acquired prescription — buy what you need. I'll introduce you to some of these independent pot retailers in my piece today. Now, as if right on cue, Vancouver-based pollster Insights West is out today with a survey of the attitudes of Canadians about pot retailers and other cannabis issues. Some findings: 36 per cent of all Canadians say they're cool with pot being sold in stand-alone stories set up for the purpose of selling cannabis products versus 29 per cent who think it should be sold in drugstores or pharmacies, while 16 per cent think selling pot products is a job best left to liquor stores or other outlets where alcoholic beverages are sold. National Post

Cannabis performance metrics: public safety
Public Safety Canada (PSC) recently released "Cannabis Performance Metrics for Policy Consideration: What do we need to measure?" For a concise synopsis of the report, I recommend this recent piece for Lift ' by Jenna Valleriani. The report is a great first step by PSC to identify measurement and evaluation (M&E) opportunities and needs in the cannabis industry. The Trudeau government would be wise to heed their advice and invest in M&E prior to legislation in the Spring of 2017. Tracking the landscape prior to, during and post-legalization will allow them to measure whether their policy changes are having the desired effect. It will have the further benefit of strengthening the results for dissemination (positioning the Canadian government as a world leader in effective public safety policy). Below is an overview of the first of four categories outlined in the report. The first category is Public Safety; it is comprised of 18 subcategories, which have been sorted for analysis into four buckets: Law & Order, Personal Use Trends, Production, and Transportation & Point-of-Sale. Lift News

PUBLIC SERVICE / FONCTION PUBLIQUE

Nil

OTHER / AUTRES

Nil

INTERNATIONAL

Bangladesh says 3 men funded deadly Dhaka restaurant attack
A counterterrorism official says Bangladesh has discovered who funded the July 1 attack in which a group of assailants tortured and killed 20 hostages at a restaurant in Dhaka. The police counterterrorism chief, Monirul Islam, says the $101,606 in financing came from three Bangladeshis, including a pediatrician who fled with his family to Syria to join the Islamic State. Islam on Tuesday identified the other financiers as a retired army major who donated his pension and savings and a man who donated proceeds from a Dhaka apartment sale. Both were killed in police raids. Islam said the three belonged to the banned militant group Jumatul Mujahedeen Bangladesh, or JMB. The IS claimed the responsibility for the July 1 attack, but Bangladesh's government insists the JMB was behind it. Global News

Syria's Aleppo calms down after Russia halts airstrikes
Syria's northern city of Aleppo calmed down on Tuesday, as Russia has halted airstrikes in the city, a security source said. The sky over hard-hit Aleppo has never been so tranquil for a long time, Xinhua news agency quoted the source as saying. Russia announced airstrikes on rebel-held areas in eastern Aleppo have been halted from 10.00 a.m. (local time) on Tuesday, as a prelude to an eight-hour humanitarian truce in the city, which will enter into force on Thursday. The Thursday truce could see the evacuation of hardline rebels of the Jabhat Fateh al-Sham, previously known as the Al Qaeda-linked Nusra Front. The truce and the rebels' evacuation are believed to be the outcome of a recent meeting in Lausanne, Switzerland, where world powers Moscow and Washionton sought to broker a humanitarian pause and eventual political solution to the crisis. The Russian air force and the Syrian army recently upped their offensives in Aleppo in order to banish the rebels from the east of the city. The Syrian government has issued multiple statements that urged the rebels to leave eastern Aleppo and promised them a safe passage to the rebel-held city of Idlib. Can-India

Mosul battle: EU 'should prepare for returning jihadists'
The EU should be prepared for returning jihadists if the so-called Islamic State (IS) is driven out of its Iraqi stronghold, Mosul, an official warns. Security Commissioner Julian King said even a small number of militants would pose "a serious threat that we must prepare ourselves for". Iraqi forces say they have captured 10 villages near Mosul since beginning their long-awaited offensive on Monday. As many as 5,000 IS fighters are believed to remain in the city. BBC News

Cut off from internet, what's next for Julian Assange?
Midway through releasing a series of damaging disclosures about U.S. presidential contender Hillary Clinton, WikiLeaks founder Julian Assange says his hosts at the Ecuadorean Embassy in London abruptly cut him off from the internet. The news adds another layer of intrigue to an extraordinary campaign. "We can confirm Ecuador cut off Assange's internet access Saturday, 5pm GMT, shortly after publication of Clinton's Goldman Sachs (speeches)," the group said in a message posted to Twitter late Monday. Associated Press (CTV News)

Racial profiling, by a computer? Police facial-ID tech raises civil rights concerns
The growing use of facial-recognition systems has led to a high-tech form of racial profiling, with African Americans more likely than others to have their images captured, analyzed and reviewed during computerized searches for crime suspects, according to a new report based on records from dozens of police departments. The report, released Tuesday by the Center for Privacy & Technology at Georgetown

University's law school, found that half of all American adults have their images stored in at least one facial-recognition database that police can search, typically with few restrictions. The steady expansion of these systems has led to a disproportionate racial impact because African Americans are more likely to be arrested and have mug shots taken, one of the main ways that images end up in police databases. Washington Post

Why aren't the candidates talking about the next security crisis?
An opinion piece states "As we prepare for the final presidential debate of 2016, with its inevitable clashes over Donald Trump's alleged groping of women and the latest WikiLeaks revelations involving Hillary Clinton, let's pretend for a moment that we are in an alternate universe where the American people are choosing a commander in chief who may have to lead our nation through an unprecedented — and unanticipated — national-security crisis (…) I asked a number of leading national-security experts what question they would ask the candidates — a question that no one is asking today but that could come to dominate the next president's term in office. Their answers are fascinating — and terrifying. Several pointed to Pakistan as the epicenter of the next major international crisis. "Pakistan is making nuclear weapons faster than any other country on earth as its society becomes more violent, more radicalized, and more anti-American," said former CIA and National Security Agency director Michael Hayden." Washington Post

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

Ralph Goodale
Oct 18, 1929-historic day in which women were legally included in the definition of "persons". Today we celebrate #equality #BecauseofHer

Ralph Goodale
Le 18 octobre 1929 - jour historique où le mot "personne" comprend les femmes dans la loi. Aujourd'hui nous célébrons l'égalité.

MTA
Hon. Ralph Goodale @RalphGoodale (Minister of Public Safety and Emergency Preparedness) amongst others meeting with Huzoor (atba) #MTAi

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Canadian Red Cross
RT @CanRedCrossATL: Follow the discussion @RedCrossCanada-organized 10th annual Disaster Management Forum, in Moncton, NB via #DMForum10

IBC
Mobile earthquake simulator shakes up Sparks Street in Ottawa....

Philip Wood
Great sessions/info at Red Cross Disaster Management Forum #dmforum10 #beprepared @Town_BayRoberts @FraneyDean @BayRobertsFire

IBC
We're proud to support @CanRedCrossATL and are excited for a good day of engagement on #emergencypreparedness #dmf2016 @IBC_Atlantic

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

OpenMedia
TONIGHT! Come have your say at the crucial Parliamentary hearings on Bill #C51. Everyone's invited! http://ow.ly/5Uiz305huqG #Calgary

OpenMedia
#Halifax! Have your say at Friday's crucial Parliamentary hearings on Bill #C51. Everyone welcome! Details here: http://ow.ly/vnZW305cv8j

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Craig Forcese
I worry also about Canada's ability to respond to displaced foreign terrorist fighters.

Norman Spector
@cforcese How many Canadians are we talking about according to latest estimates?

Craig Forcese
@nspector4 Don't think gov has reported better figures than this. cc @AmarAmarasingam

Amarnath Amarasingam
@cforcese @nspector4 yeh, around 100 Canadians according to our research.

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Border Services
Two firearms seized at ports of entry in Northwestern Ontario #Leaveyourhandgunsathome http://ow.ly/3qbz305hYxc

Border Services
CBSA Celebrates Small Business Week! #SBW2016 http://ow.ly/FU3D305i49T

LAW ENFORCEMENT / APPLICATION DE LA LOI

Metro Winnipeg
Winnipeg police join forces with FBI to crack down on human trafficking

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

CBC Nova Scotia
'He's still my son and I loved him': Inmate's mother testifies at inquest http://bit.ly/2epg7Ee

CBC Nova Scotia
Melissa Ann Shepherd, so-called Internet Black Widow will be back in court at the end of the month

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

CRCVC
Domestic violence unit ready to roll in Prince George https://shar.es/1EwBFC via @sharethis

CRCVC
Improving Access to Services for Victims of Crime in New Brunswick http://m.marketwired.com/press-release/improving-access-to-services-for-victims-of-crime-in-new-brunswick-2165397.htm ...

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Jill Coubrough
'They should be out here, not me as a parent' Catcheway says RCMP have yet to follow up new leads in his daughter's homicide #cbcmb #mmiw

U.S. Embassy Ottawa
ICYMI: US, Canada & Mexico open NA Working Group on Violence Against Indigenous Women and Girls: https://goo.gl/pwthNX #cdnpoli #MMIW

OTHER / AUTRES

Craig Forcese
Ditto, for Canada: "The Government's Addiction to 'Secret Law'

INTERNATIONAL

Stewart Bell
Mosul battle: EU 'should prepare for returning jihadists'

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

Sent to: !INTERNAL; !INTERNAL 2; CBSA Today's News; CSC & PBC Today's News; PS Today's News; RCMP Today's News; RCMP Today's News 2

Today's News / Actualités
October 18, 2016 / le 18 octobre 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

TOP STORIES / MANCHETTES

Opération policière contre l'esclavage sexuel : 32 personnes accusées au Canada

Une descente policière coordonnée entre 53 services de police canadiens et le FBI a permis d'arrêter 32 personnes relativement à l'exploitation sexuelle et la traite de personnes au Canada, indique le service de police de Winnipeg. L'opération Northern Spotlight a comme objectif de s'assurer du bien-être de jeunes femmes qui peuvent être victimes de traite humaine et qui auraient été forcées de se prostituer. La police de Winnipeg, qui a participé à l'initiative, dit que la descente coordonnée qui s'est déroulée sur six jours en octobre a permis de venir en aide à 16 personnes à travers le pays qui avaient été forcées de travailler dans l'industrie du sexe. Plusieurs des victimes avaient moins de 16 ans. Les accusés font face à un total de 78 chefs d'accusation, dont des chefs pour agression, traite de personnes, séquestration, production et distribution de pornographie juvénile... En plus du FBI, 36 services de police ontariens et 18 autres services de police canadiens incluant la Gendarmerie royale du Canada ont participé à l'opération Northern Spotlight. Radio Canada; Postmedia Network (National Post; Ottawa Citizen); CBC News; Canadian Press (Winnipeg Sun; Toronto Sun; Ottawa Sun; Edmonton Sun; Calgary Sun; London Free Press; Whig-Standard; Cornwall Standard Freeholder; Fort McMurray Today; North Bay Nugget; Chatham Daily News; Sault Star; Brantford Expositor; Owen Sound Sun Times;)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Southern Nova Scotia still thirsty after last week's rain
Even after rain pounded Nova Scotia last week and flooded Cape Breton, southern parts of the province remain parched and hundreds of wells are still dry, according to municipal officials in Argyle and Barrington... Many people are still getting drinking water from search and rescue organizations and taking showers at schools. People are also bringing home large plastic boxes filled with water to allow them to flush their toilets. Normally those boxes are used to transport fish. CBC News

Heiltsuk First Nation calls tugboat sinking near Bella Bella 'environmental disaster' as clean-up efforts continue
The Heiltsuk First Nation caught in the middle of a diesel spill near Bella Bella is sounding the alarm and calling the situation an "environment disaster." The tugboat Nathan E. Stewart with more than 59,000 gallons of diesel fuel onboard sank at the entrance to Seaforth Channel, west of Bella Bella after running aground Thursday morning, causing booms and oil skimmers to be deployed. The barge that the tug was carrying was empty of cargo and has since been moved to a safe anchorage. Heiltsuk First Nation Chief Councillor Marilyn Slett says the spill is devastating the clam beds that the community relies on for income. Slett says only 6,554 gallons of the 59,924 gallons of diesel onboard the tug were able to be pumped from the vessel before it sank. She says since then, the sunken vessel has been leaking diesel into an area of enormous ecological, economic and cultural significance to the Heiltsuk Nation. Slett says spilled diesel has already fully blanketed the most important clam beds in Heiltsuk Territory. Global News

Sydney flood-contaminated items not safe for 'garbage pickers'
Some people make a hobby, or even a small income, from picking household items out of garbage left at the curb and fixing them up to sell. But these "garbage pickers" are now being warned off hauling away home goods that were contaminated with sewage or furnace oil during the Thanksgiving Day flood in Cape Breton Regional Municipality. Flood victims have been told to leave all their damaged or destroyed items on the curb for special collection, to prevent disease or mould inside their homes. "It's well known that sewage contains many different types of biological agents," said Bill Rideout, the acting manager of environmental health with the Nova Scotia Department of Environment. CBC News

Environment Canada confirms tornado hit Stayner, Ont. Monday
Environment Canada has confirmed that a tornado touched down in Stayner, Ont., about 130 kilometres northwest of Toronto, on Monday afternoon. Investigators are still working to determine the strength of the tornado, which landed around 4 p.m. in the community near the southern tip of Georgian Bay, uprooting several trees and overturning a trailer, the agency said on Tuesday. CBC News

Canada-bound plane crashed in Pennsylvania
A small airplane that lost contact with flight controllers while flying from Virginia to Canada has been found crashed in north-central Pennsylvania, with all three occupants killed... The Federal Aviation

Administration says the Canadian-registered Piper PA-28 took off from Richmond International Airport in Virginia. It was headed to St. Catharines/Niagara District Airport when the wreckage was found Late Monday. The coroner says the plane was found crashed in Keating Township in southern Potter County. That's about 150 miles northeast of Pittsburgh. Potter County borders New York. The FAA lost contact with the flight over Potter County about 7 p.m. Saturday. The National Transportation Safety Board is heading the crash investigation. Associated Press (Winnipeg Sun; Toronto Sun; Ottawa Sun; Edmonton Sun; Calgary Sun)

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

We Need A Human Rights-Based Approach To National Security
A blog post by Amnesty International Canada Secretary General Alex Neve states "Human rights or security? In Canada and around the world the debate rages on; but it is an utterly false debate. We must, finally and firmly, reject the assumption and assertion that more of one necessarily leads to less of the other. There is no security without human rights (…) This week the federal government's review of Canada's national security framework has begun in earnest. The House of Commons' Public Safety Committee is holding hearings in five cities from coast to coast. Ministers Goodale and Wilson-Raybould are holding a roundtable in Ottawa with civil society groups. Members of Parliament are conducting town-halls in their ridings. And Canadians in all corners of the country are being encouraged to take part in online consultations. Amnesty International has been researching, reporting and campaigning on the grim human rights toll of unjust national security practices around the world, including in Canada, for decades. We have highlighted that without security, human rights remain precarious (…) At the same time we have demonstrated time after time that human rights violations stand to deepen insecurity. Allowing torture, discrimination or unfair trials as part of a counter-terrorism strategy creates more victims, fosters resentment and deepens divisions. There is no long-term security down that road. Canada can chart a different course, and that can start now by making a clear choice to develop and adopt a human rights-based approach to national security. There are three main components. Huffington Post

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Why are three of the world's richest countries doing so little to stop corruption?
One of the best-known data points in the anti-corruption field is the estimate from Global Financial Integrity that US$ 1.1 trillion in proceeds of corruption, crime and tax evasion are taken from developing countries every year and invested in Western banks, real estate, and luxury goods… If you've ever found yourself wondering how this scale of pillage is possible, the most recent round of reports from the Financial Action Task Force has the answer. The Financial Action Task Force (FATF) is the world's anti-money laundering standard-setter. Every seven years FATF assesses how much each of its 180 member countries has done to stop dirty money from being used to buy real estate, high-end cars and other luxury items, or be deposited into a bank account. In other words, how good is a country at preventing itself from aiding the corrupt. Recently released reports on Austria, Canada and Singapore show how the corrupt have few roadblocks to parking and spending cash in these three countries. Similar to previous reports, the latest batch received limited media coverage aside from on specialist websites… Following a Supreme Court decision in 2015, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its regulations were found to breach attorney-client privilege insofar as record-keeping, client identification and verification, and compliance inspection by Canada's Financial Intelligence Unit (FINTRAC) were concerned. The Government had previously withdrawn the reporting requirement for the law profession following injunctions by law societies. Though lawyers are subject to anti-money laundering rules set by Canadian law societies, according to the FATF the exemption of lawyers from federal legislation "constitutes a serious impediment to Canada's efforts to fight money-laundering" Transparency International

The Liberals after Year One - A mixed report card, but only themselves to blame

An opinion piece states, "Is it fair to judge a government only a year after an election? If the government in question made 325 promises during the campaign, as the Liberals did, then yes. Given our four-year election cycle, they had better be one-quarter of the way through checking off their pledges. Of course, only a deliverology guru could calculate this for sure. So let's just do a quick fly-by:... Indigenous Affairs - A "renewed nation-to-nation relationship" was among the government's most significant promises to Indigenous Canadians. Some things did happen: budget funding of $8.4 billion over five years is coming, and an inquiry is underway into missing and murdered indigenous women. Not accomplished: equal funding for First Nations children... Security - Canadians still haven't seen the changes coming to the "problematic" anti-terrorism act, Bill C-51. But there will be an all-party national security oversight committee and there are broader security consultations... Justice - The government spent the first half of the year wrestling down assisted-dying legislation. Now, disarray looms on the legalized-marijuana file. A task force will report, legislation will emerge - and meanwhile, illegal pot shops have sprung up with impunity..." Postmedia Network (Ottawa Citizen)

Progress report on Justin Trudeau's election campaign promises, one year later

An opinion piece states, "When it comes to keeping promises, Canadians know full well that politicians are not at all like Horton, the Dr. Seuss character who "meant what I said and I said what I meant: an elephant's faithful, 100 per cent." They make many promises to win elections, but often find it impossible to deliver on them once they take office... Here's a look at the main ones: Promises Kept - ...Launch a national inquiry into missing and murdered indigenous women. Create a parliamentary oversight committee on national security operations... Repeal Conservative legislation that allowed the government to revoke the citizenship of dual citizens convicted of terrorism, treason or espionage. In Progress - Legalize marijuana. A task force is to report by Nov. 30 and the government is promising legislation next spring... Amend controversial anti-terrorism legislation passed by the previous Conservative government. The government has launched consultations and is in the process of creating a parliamentary oversight committee on national security... Still to Come - Create an office of counter-radicalization to deal with the phenomenon of home-grown extremists..." Cape Breton Post

CATSA extends airport screening contracts

The federal agency in charge of security at Canada's airports has renewed screening contracts with three private-sector firms, GardaWorld, Securitas and G4S. The Canadian Air Transport Security Authority says the total value of the contract extensions is about $2.6 billion. They'll run from April 2017 through March 2022. CATSA says GardaWorld will receive contracts worth about $1.4 billion for 28 airports in Ontario, the three Prairie provinces and Northwest Territories. Securitas Transport Aviation gets contract extensions worth $632 million for Quebec and the four Atlantic provinces, while G4S Secure Solutions gets extensions worth $510 million for British Columbia and Yukon Territory. Canadian Press (Brampton Guardian)

Screening at Canadian airports should be faster, smarter and safer

An opinion piece by Senator Colin Kenny, former chair of the Senate Committee on National Security and Defence, states, "If you've flown anywhere in Canada recently, you will have noticed that wait times are getting worse. Since 2013, the length of screening times has deteriorated so badly that the Canadian Airport Council referred to security screening services as a being in a state of crisis. Not only are we waiting more, we are paying more. And getting less service... While it's annoying to wait in long lines, more important is the security risk these lines pose. A new wave of terrorist attacks on airports in Moscow, Brussels and Istanbul have all occurred between the sidewalk and the security inspection line. Instead of viewing screening lines as an annoyance, officials should see these lengthening lines as a soft spot for terrorists. Another problem with airport security highlighted in David Emerson's 2015 Review of the Transportation Act, is the strange restrictions faced by CATSA. Essentially, CATSA has no control over security screening policy. This has led directly to poor service and long wait times. Emerson recommends adopting the U.S. model wherein a single "agency has responsibility for both regulatory oversight and operations"... But perhaps the greatest failing of the Canadian model is with our trusted traveller program: NEXUS... NEXUS cardholders are also offered a special line at security screening. The problem is, it's not that special. NEXUS users are still forced to submit to the same cumbersome screening procedures as other passengers. The question is: If our border officials allow these pre-screened travellers to enter the country quickly and safely, why doesn't the same practice apply at airport

security? Replacing this "one-size-fits-all" approach to passenger screening with a risk-based, intelligence-driven approach was a key recommendation in the Emerson review..." Postmedia Network (Montreal Gazette)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Fliss Cramman doesn't think she would survive deportation to U.K.
A hospitalized 33-year-old woman facing deportation from Nova Scotia to the U.K. says she's terrified of what could happen to her if she's forced out of Canada. "I've been here 25 years of my life. My kids are here, my family is here, everything I know is here," Fliss Cramman said Tuesday from her room in Dartmouth General Hospital... A hospitalized 33-year-old woman facing deportation from Nova Scotia to the U.K. says she's terrified of what could happen to her if she's forced out of Canada. "I've been here 25 years of my life. My kids are here, my family is here, everything I know is here," Fliss Cramman said Tuesday from her room in Dartmouth General Hospital. Cramman was released on parole in June, but immediately arrested by the Canada Border Services Agency to start the deportation process. She's been under guard in hospital since August, when she suffered a perforated bowel and needed multiple followup surgeries due to complications. For several weeks, Nova Scotia corrections officers kept Cramman shackled to her hospital bed. She was unchained after Nova Scotia Justice Minister Diana Whalen intervened... According to the Elizabeth Fry Society, Cramman became a ward of the court around age 12, but no one secured her Canadian citizenship. According to documents from the Parole Board of Canada, Cramman suffered from the effects of violence and alcoholism in her home. As a minor, she also suffered violent sexual abuse outside her home. The Elizabeth Fry Society said Cramman is being punished by a system that was supposed to care for her... Halpern said Cramman is at risk of being deported next month, despite the fact her surgeon and health-care team believe it's essential for her to stay in Canada for a year to follow up on her medical care, including a colostomy reversal procedure... ramman lost her health coverage when she was placed under an immigration removal order. The Canada Border Services Agency will only pay for medical expenses while she's in custody. CBC News

2 men charged with conspiracy to smuggle person across St. John River
Two New Brunswick men have been charged with conspiracy to smuggle a person across the Canada-United States border in the northwest of the province. A 67-year-old man from Edmundston and a 50-year-old man from Baker Brook appeared in Edmundston provincial court on Oct. 17. The incident that incited the charges took place in July. Authorities were made aware of a 46-year-old woman who crossed into the United States illegally across the St. John River using a paddle boat. The woman, a citizen of Ecuador, was apprehended in Van Buren, Maine. She is still in the United States. The two men charged were arrested by the RCMP on July 28. CBC News

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

B.C. auditor general warns info on government mobile devices at risk
British Columbia's auditor general says appropriate security controls are not always in place for thousands of mobile devices used by government employees, putting sensitive information at risk. Carol Bellringer says there is no central record of devices such as smartphones and tablets and that's concerning because information can't be protected without an inventory of the equipment being used. Bellringer has issued a report on security of mobile devices used by the Office of the Chief Information Officer and five ministries with the highest security risks. She says any loss, theft, or exposure of information accessed via mobile devices could have serious implications for the government and B.C. residents. Globe and Mail

Businesses cooperate with government mass surveillance at their peril, says Edward Snowden
Resisting government mass surveillance isn't just the right thing to do - it's good for business, whistleblower Edward Snowden told a Toronto cybersecurity conference Tuesday. Speaking via video

link to the annual Canadian industry event SecTor, Snowden brought up the recent revelation that Yahoo! Inc. had agreed to scan customer's emails for U.S. intelligence... nowden cited Open Whisper Systems, which makes the encrypted messaging app Signal, as an example of an organization that benefited from pushing back against a government request for cooperation in a surveillance program. With the help of the American Civil Liberties Union, Open Whisper Systems fought a gag order on a subpoena for information associated with two phone numbers.

Ultimately, Open Whisper Systems had comply with the subpoena, but the damage was mitigated because of another Snowden-approved policy: Only retaining as much personal data as absolutely necessary. The subpoena asked for browsing history and tracking data stored in web browsers, but Signal doesn't collect that information... Snowden questioned whether mass surveillance programs are beneficial to national security in the first place, citing reports by a review board appointed by U.S. President Barack Obama and the U.S. Privacy and Civil Liberties Oversight Board that found the mass collection of telephone records had failed to contribute significantly to any terrorism investigations. He argued there's no reason why tech and telecom companies should be required to build so-called back doors into their products to help law enforcement retrieve information. Postmedia Network (National Post)

LAW ENFORCEMENT / APPLICATION DE LA LOI

De nombreuses dénonciations d'abus de policiers envers les Autochtones
Des dizaines d'Autochtones ont fait de nouvelles dénonciations d'abus commis par des policiers au moyen de la ligne téléphonique mise en place par le gouvernement du Québec pour inciter les femmes autochtones à briser le silence. Les dénonciations qui ont été faites au cours des derniers mois visent des agents de la Sûreté du Québec (SQ), mais également des policiers municipaux et des agents des corps policiers autochtones. Selon nos informations, au moins 75 appels ont été faits à cette ligne téléphonique jusqu'à présent. Les dénonciations proviennent d'un peu partout au Québec. Elles sont faites par des femmes, mais également par des hommes qui ont décidé de briser le silence, ce qui a étonné les représentants des Services parajudiciaires autochtones du Québec. Radio Canada

Culture of fear prevents Indigenous victims of police brutality from reporting alleged crimes
At least 75 Indigenous men and women have come forward to report incidents of police brutality, intimidation and other mistreatment by Quebec police officers since the provincial government launched a tip line in April. But the people taking those calls worry a culture of fear is preventing many alleged victims from making formal complaints to police. The tip line was set up after Radio-Canada's investigative program Enquête uncovered stories of sexual violence by Sûreté du Québec officers toward Aboriginal women in Val-d'Or, about 600 kilometres northwest of Montreal. Managers of the tip line have received calls from across the province, from both men and women, complaining of abusive behaviour by SQ officers as well as members of Indigenous and municipal police forces. CBC News

Opération policière contre l'esclavage sexuel : 32 personnes accusées au Canada
Une descente policière coordonnée entre 53 services de police canadiens et le FBI a permis d'arrêter 32 personnes relativement à l'exploitation sexuelle et la traite de personnes au Canada, indique le service de police de Winnipeg. L'opération Northern Spotlight a comme objectif de s'assurer du bien-être de jeunes femmes qui peuvent être victimes de traite humaine et qui auraient été forcées de se prostituer. La police de Winnipeg, qui a participé à l'initiative, dit que la descente coordonnée qui s'est déroulée sur six jours en octobre a permis de venir en aide à 16 personnes à travers le pays qui avaient été forcées de travailler dans l'industrie du sexe. Plusieurs des victimes avaient moins de 16 ans. Les accusés font face à un total de 78 chefs d'accusation, dont des chefs pour agression, traite de personnes, séquestration, production et distribution de pornographie juvénile... En plus du FBI, 36 services de police ontariens et 18 autres services de police canadiens incluant la Gendarmerie royale du Canada ont participé à l'opération Northern Spotlight. Radio Canada; Postmedia Network (National Post; Ottawa Citizen); CBC News; Canadian Press (Winnipeg Sun; Toronto Sun; Ottawa Sun; Edmonton Sun; Calgary Sun; London Free Press; Whig-Standard; Cornwall Standard Freeholder; Fort McMurray Today; North Bay Nugget; Chatham Daily News; Sault Star; Brantford Expositor; Owen Sound Sun Times;)

Police help 18 women believed to be involved in Windsor sex trade
Numerous charges have been laid by police in Ontario following a national investigation to stop human trafficking, while providing information to people involved in the sex trade. Operation Northern Spotlight was a five-day investigation in early October that involved 36 police services across the province... n Windsor, police spoke to 18 women believed to be involved in the sex trade industry. Those women were from cities across Ontario and the United States, and they ranged in age from 20-40 years. All were provided safety plans and resources to exit the sex trade. It is not known how many accepted the help from police and service agencies. Across the province, police also interviewed 16 people who were working in the sex trade as a minor against their will. Police provided information and attempted to connect them with agencies in the community to help remove them from the sex trade. According the to OPP, a total of 207 police officers in Ontario and support staff engaged with 199 people and offered them information and contacts with community-based support agencies. CBC News

9 Manitobans charged in 'semi-organized' thefts across Western Canada
Nine Manitobans face numerous charges and 11 more people are wanted after police recovered more than $300,000 in stolen goods - including RCMP uniforms, camper trailers and blank passports - from a "semi-organized" crime ring spanning the four western provinces. Winnipeg police say 20 suspects have been identified in connection with Project Heavy Metal, a "complex stolen property investigation" that began late last year. The investigation targeted a number of break-ins and thefts in Winnipeg and the surrounding area, but investigators found some of the suspects were also active in Saskatchewan, Alberta and British Columbia, said Insp. Barry Kostchuk... The Winnipeg Police Service worked with the Calgary and Edmonton police services and the RCMP in the investigation. CBC News

Police arrest seven people from two organized crime rings in ATM thefts
Alberta police services have arrested seven people from two organized crime rings involved in ATM thefts, which have affected more than 60 communities across the province. ALERT said in the first six months of 2016, there were more than 130 instances of ATM thefts at banks, credit unions, gas stations and convenience stores. At an ALERT press conference Tuesday morning, Staff Sgt. Dave Knibbs says both groups targeted "small town Alberta" and terrorized rural communities. A total of 101 charges have been laid against the seven suspects. Postmedia Network (Edmonton Journal; Edmonton Sun; Calgary Sun); CBC News

IHIT charges 27-year-old man in connection with Langley homicide
27-year-old Jason Wallace has been arrested and charged with second-degree murder in connection with the homicide of Robert Green on Oct. 16. RCMP arrested Wallace at 152 Street and 71A Avenue in Surrey. He is currently in custody. Police said Wallace was not affiliated with the Hells Angels. Investigators are appealing to the public for information about the death of a 56-year-old Burnaby man who was a senior member of the Hells Angels. Around 10:30 a.m. Sunday, RCMP were called to the 23700-block of 72 Avenue in the Township of Langley, where a male victim was found suffering from severe injuries. Despite the best efforts of first responders, the victim died of his injuries at the scene soon afterwards, and the Integrated Homicide Investigation Team (IHIT) took over the investigation. Police have determined the homicide was targeted and not random, and are continuing to gather information. Global News

Elderly Bonnyville man's death was a homicide, RCMP say
Police said the death of an elderly man found in a Bonnyville home has been ruled a homicide. Bonnyville RCMP officers responded to the report of a death at a residence at about 1:30 p.m. Sunday. An autopsy Tuesday determined the case was a homicide. Police had been looking for a truck that was believed to belong to the deceased man. They said they found the missing pickup on the Kehewin Cree Nation, which is located about 20 kilometres south Bonnyville. The RCMP major crimes unit was leading the investigation. Edmonton Journal

Dressing up as clown illegal if you harass or intimidate public, say Airdrie RCMP
While it's not illegal to dress up in costume, Airdre RCMP are reminding anyone thinking of smearing pancake makeup on their face to remember to only do it in "good fun."... She said anyone who does that

could face criminal code charges, including mischief, causing a disturbance or uttering threats. CBC News

Charlottetown police searching for travelling diamond thieves
A surveillance image shows two individuals suspected of stealing approximately $20,000 in diamonds from a Charlottetown jewelry store last week. City police are asking anyone able to identify the two to come forward. Thieves swap "useless stones" for $20,000 in diamonds A Charlottetown jewelry store is victim to a brazen swap that netted thieves two diamonds valued at about $20,000... Charlottetown Deputy Police Chief Gary McGuigan says police believe the pair is the same two people wanted for a similar incident in Saint John, N.B. where a diamond worth $10,000 was stolen from W. Smith and Co. Fine Jewellers on Oct. 7. The store, which police are not naming, was hit last Wednesday. Guardian

Driver flees crash scene involving stolen car on P.E.I.
A young man crashed a stolen car into the ditch near Mount Stewart Monday, then took off. Now Queens District RCMP is asking for help finding that man. A 911 call came in about 5 p.m. Monday, Oct. 15, from a resident reporting that a vehicle had just gone into the ditch near his residence on Route 351 in Mount Stewart. "The caller saw a young male running away from the vehicle, through a field and then towards the river in Mount Stewart," said a police report issued Tuesday... The Police Dog Service was called in was not able to locate the suspect. Guardian

Graydon makes push for RCMP recognition
Emerson MLA Cliff Graydon is leading the charge to have Royal Canadian Mounted Police honoured with a day of recognition in the province. Graydon has introduced legislation to make Feb. 1 an annual day in Manitoba to commemorate and show appreciation for the RCMP, and for the work they do to protect and serve Manitobans and people across Canada. The RCMP were first formed on the same date in 1920. The Carillon

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Rights commission decries 'shocking' Ontario solitary-confinement numbers
Ontario's solitary-confinement cells are stocked with a "shocking" proportion of inmates who have mental-health issues, medical problems or other health challenges, including one prisoner who has spent more than four years in isolation, according to figures released by the Ontario Human Rights Commission... The commission requested the figures last January to help inform its submission to an internal review of segregation practices the province has been conducting for the past 19 months. It did not intend to make them public. But when Chief Commissioner Renu Mandhane finally saw the data, she decided it was so alarming as to warrant broader interpretation. "Given these shocking numbers, the OHRC again calls on the government to eliminate the use of [segregation]," states a commission submission to the province released on Tuesday... The commission, however, told reporters during a technical briefing on Tuesday that the numbers capturing the duration of segregation placements may mask on-the-ground practices. Every time an inmate is transferred, their total segregation counter is reset to zero. The resetting of segregation clocks was found to be a factor in the deaths of Ashley Smith and Eddie Snowshoe, two federal inmates whose deaths in solitary-confinement cells three years apart galvanized public support for segregation reform across the country. The federal correctional service has since phased out the practice. Globe and Mail; CBC News

Glen Wareham inquest hears inmate pushed system 'beyond its limit'
The first goal of the Shepody Healing Centre in dealing with Glen Edward Wareham was to protect him from himself, an inquest into the inmate's was told on Tuesday. Louis Blanchard, an institutional psychologist in Dorchester, testified he started working with Wareham in May 2007 and stated that all treatment options for Wareham had been exhausted and staff at the Shepody Healing Centre were mainly waiting for Wareham to be transferred elsewhere by the Correctional Service of Canada. Wareham, 28, from New Waterford, N.S., died in hospital in Moncton in 2010 from complications from self-harm. He was an inmate at the Shepody Healing Centre, which is a mental health facility for

prisoners operated by the Correctional Service of Canada. Chief Coroner Gregory Forestell is presiding over an inquest into Wareham's death in Moncton. CBC News

Dennis Oland murder appeal hears concerns from top judge about trial
New Brunswick's top judge expressed concerns during Dennis Oland's appeal of his murder conviction on Tuesday about how the trial was conducted last year. But Court of Appeal Chief Justice Ernest Drapeau stopped short of saying those concerns would be enough to overturn Oland's conviction in the 2011 bludgeoning death of his father, multimillionaire Richard Oland. Drapeau was responding to defence lawyer Alan Gold's suggestion that lead Crown prosecutor P.J. Veniot may have crossed a line in his remarks to the jury by speculating about what transpired between Dennis Oland and his father. CBC News

Ontario pathologist contradicts 2012 testimony at ex-judge Jacques Delisle's bail hearing
A forensic pathologist called to testify at the bail hearing for Jacques Delisle — the only judge in Canada to have gone to prison for first-degree murder — says the bullet that killed Delisle's wife entered the left side of her skull at a 90-degree angle, testimony that differs radically from the evidence at Delisle's original trial. CBC News

Reducing solitary confinement doesn't need more study. It needs action
An opinion piece states, "Ontario Corrections Minister David Orazietti actually said this on Monday, about his government's overuse of solitary confinement in provincial prisons: "After a thorough internal review and extensive consultations with a broad range of experts, it is becoming apparent to me ... that a more thorough and comprehensive review into the complex nature of the corrections system in Ontario needs to be conducted."... The United Nations, for instance, says putting a healthy, adult prisoner in solitary for more than 15 days in a row is a form of torture, and that it should never be used on youths and mentally ill inmates. Howard Sapers, the federal prisons ombudsman, says the maximum time in solitary should be 15 days. The Ontario Human Rights Commission has called for a complete ban on solitary in Ontario prisons. The union representing Ontario corrections workers says segregation is no place for inmates with mental illness, and that the province should build separate facilities for them. In January, President Barack Obama banned solitary for juvenile offenders in U.S. federal prisons... There is no question that corrections systems are complex. But the issue of solitary confinement is not. It is abusive, and it harms inmates suffering from mental illness, making it harder for them to rejoin society when their sentences are complete. Mr. Orazietti can request all the studies he wants, but it won't hide the fact that Ontario's perpetual inaction on solitary confinement is failing not only inmates but also the broader public." Globe and Mail

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Traite de personnes : un projet de loi pour porter des accusations sans le témoignage des victimes
La traite de personnes est une réalité méconnue au pays. Ces jeunes filles, souvent recrutées sur Internet - parfois dès l'âge de 10 ans - se font entraîner dans la prostitution. Soumises à des proxénètes, elles sont exploitées sexuellement, souvent pendant de nombreuses années. De nombreux criminels ne sont pas arrêtés : la peur empêche trop souvent les victimes de parler. Les services policiers à travers le pays se retrouvent fréquemment les mains liées quand vient le temps d'arrêter les proxénètes, selon Maria Mourani, criminologue et sociologue spécialisée en gangs de rue. Le plus gros problème est que les victimes ne veulent pas toujours dénoncer leurs souteneurs, craignant les conséquences. Le projet de loi C-452, modifiant le Code criminel (exploitation et traite de personnes), vise justement à permettre aux services policiers de déposer des accusations sans le témoignage des victimes, comme cela se fait pour les cas de violence conjugale. Radio Canada

6 ans pour avoir eu deux blondes de 13 ans
Un homme de 21 ans qui sortait avec deux filles de 13 ans en même temps et qui a fait six victimes au total a été déclaré délinquant à contrôler. Il passera six ans au pénitencier. Tomy Éthier n'a que 21 ans,

mais il en est déjà à sa quatrième condamnation pour des crimes de nature sexuelle sur des mineures. Il venait à peine de sortir de prison en août 2015 lorsqu'il a utilisé les réseaux sociaux pour faire six nouvelles victimes âgées de 12 à 15 ans. Éthier était notamment en couple pendant plus de trois mois avec une enfant de 13 ans en mentant sur son âge. Pendant cette période, il a également eu une autre relation amoureuse avec une autre fille de 13 ans en plus de séduire son amie de 12 ans. Encore aujourd'hui, il ne reconnaît pas que ce qu'il a fait était grave puisque selon lui, plusieurs personnes utilisent aussi les réseaux sociaux pour séduire des personnes mineures. Il n'a entrepris aucune thérapie et son risque de récidive est considéré comme étant élevé. Son séjour en détention a été turbulent et il s'est retrouvé en confinement à quelques reprises. Éthier a plaidé coupable à 16 chefs d'accusation dont attouchement et incitation à des attouchements sur des mineures de moins de 16 ans. QMI (Journal de Québec; Journal de Montréal)

Toronto lawyer charged in sex assault of teens has licence temporarily suspended
A Toronto lawyer accused of sexually assaulting three teenage girls has had his licence temporarily suspended. The Law Society Tribunal says Francois Lesieur won't be allowed to practise law until he has a chance to respond to a motion brought forward Tuesday morning by the Law Society of Upper Canada. Toronto police charged Lesieur with four counts of sexual assault in late September, alleging he assaulted the girls -- aged 14, 15 and 16 -- in public places such as subway stations and a food court. CTV News

Nurses demand workplace safety
Janet Hazelton, president of the Nova Scotia Nurses' Union says an incident in a Middleton hospital should have been given more consideration in light of the serious nature of the threat and the escalating frequency of violent behaviour in health care facilities across the province. She, like other health care advocates, is very concerned about this issue, calling on government to make workplace violence a priority. Last week a Kings County man, once charged with plotting to kill police officers in Newfoundland, was charged with firearm-related offences after a disturbance at Soldiers Memorial Hospital in Middleton... Police responded to a call from the hospital about a man acting erratically. When they arrived, they found and arrested 60-year-old man. He has been charged with possession of a firearm while prohibited, unauthorized possession of a firearm and careless use of a firearm... The Nova Scotia Nurses' Union has been in talks with health care stakeholders for several months, since the NSNU released a study in January 2016 identifying violence in the workplace among 15 significant problems plaguing our health care system. Chronicle Herald

Online safety being highlighted by OPP
Police across the province are hoping to raise people's online security awareness this month as they focus on cyber safety. In a four-part series, OPP are reminding people how to keep information safe online. Topics in the series include Free Wi-Fi use and password protection, phishing and ransomware (on both personal and corporate devices) scams, e-mail attachments and online child safety. Belleville Inteligencer

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Explore B.C.'s notorious Highway of Tears in new virtual reality documentary
When Matilda Wilson's daughter Ramona went missing in 1994, Wilson never imagined that 22 years later, she would still be searching for answers about what happened... The RCMP have acknowledged that 18 girls and women have gone missing or been murdered along the stretch of highway between Prince George and Prince Rupert and nearby routes since 1969. Indigenous leaders say that number is closer to 50... CBC's first virtual reality documentary, Highway of Tears transports viewers to the Wilson home and then onto the notorious stretch of Highway 16, providing a visceral experience of the landscape and the personal tragedies that haunt that landscape and that have affected so many Indigenous people in Canada. The documentary was directed by Anishinaabe filmmaker Lisa Jackson... On Sept. 1 of this

year, the federal government launched a national inquiry into missing and murdered Indigenous women and girls. The inquiry came in the wake of emotional pleas from relatives and community members, news stories and police reports that underscored what is now recognized as the decades-long vulnerability and victimization of Indigenous women in Canada... Against this backdrop, The Current launched its virtual reality documentary at a public forum Oct. 13 in Prince George, a community with close links to the highway and the tragic stories associated with it. More than 250 people attended, many of whom came with their own personal stories of loved ones gone missing or affected by violence. CBC News

Anti-racism group slaps warning labels on Halloween costumes
Despite public protests, some costumes like Dream Catcher, Native Royalty and Pocahottie are still on store shelves in Saskatchewan and will remain there... On Sunday, members of Colonialism No More and the Saskatchewan Coalition Against Racism (SCAR) entered the Spirit Halloween store located at 2220 Willow Rd and put their own warning labels on costumes and other items they deemed in appropriate. The warning labels stated, "The items contained in this package are offensive and promote the sexualization of indigenous women and peoples. Please avoid contact with these dangerous materials"... in addition to the warning label, the activists placed information about missing and murdered indigenous women and girls in Canada as a way to help educate others about why the costumes are offensive to some people. Postmedia Network (Leader-Post)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Alberta justice minister to research cannabis policies in Colorado
Alberta's justice minister is travelling to Colorado this week to research the legalization of cannabis first-hand. Kathleen Ganley will be going to Denver Thursday to meet with the attorney general, police, fire and environmental health officials. She says the two-day trip will cost just over $4,000 but will help prepare the government for the eventual legalization of marijuana. Ganley says Colorado is an ideal location to research the issue since it legalized cannabis more than two years ago. She says she hopes the trip will help Alberta avoid problems during the legalization process. Ganley says the research will help cabinet ministers during the development and implementation of a cannabis framework for Alberta. Canadian Press (660 News)

Weed still on police radar, even though busts down
You won't find many, if any, people working in law enforcement ready to admit that marijuana trafficking isn't still on their radar. In fact, they will go to great lengths to tell you otherwise. But when you are dealing with the emergence of the province's deadliest killer drug fentanyl -- a synthetic opioid 100 times more toxic than morphine -- limited policing resources have to be focused on saving lives. Postmedia Network (Edmonton Sun; Calgary Sun)

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Supporters of Raif Badawi worried lashings will resume in Saudi Arabia
Supporters of a blogger jailed in Saudi Arabia are concerned he will once again be subject to lashings and are calling for his release. Raif Badawi, whose wife lives in Sherbrooke, Que., was arrested in 2012 and sentenced in 2014. In a statement, the Raif Badawi Foundation said it had received word from a "private source" that the Saudi government will resume the lashing punishment... Mireille Elchacar, a spokesperson for Amnesty International in Quebec's Eastern Townships, where Badawi's wife lives, said the organization is trying to independently confirm the claim... Badawi is not a Canadian citizen, but his wife, Ensaf Haidar, and their three children were granted political asylum in 2013. CBC News; Radio Canada; Postmedia Network (Gazette)

INTERNATIONAL

NIL

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

RalphGoodale
Félicitations à @evanjbray, nouveau Chef de Police de Regina. Nous sommes fiers de vous avoir! @reginapolice

RalphGoodale
Fier d'avoir rencontré Sa Sainteté Mirza Masroor Ahmad, le Chef de la Communauté Musulmane Ahmadiyya.

davidakin
.@jyduclos,@SocDevSoc,@RalphGoodale ,Emergency Shelter housing,Melfort,SK,$ 800 000,SK,#Ottawaspends
CPC Riding @MPRandyHoback

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

NatashaFatah
Anger flares as wildfire-hit Canadian city Fort McMurray struggles to rebuild #cdnpoli http://reut.rs/2eAax5F

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

davidakin
#SECU 31 meets now in Calgary. National Security Framework. Link to details: http://bit.ly/1o8816t #cdnpoli

OpenMediaOrg
ICYMI: @OpenMediaOrg's @ltribe delivering your voices against #C-51 at crucial public hearings in #Vancouver: http://ow.ly/JTFt305jnBU

DesmondCole
There's a public meeting on Bill C-51 in Toronto tomorrow. Details:

MattDube
Every single member of the public tonight has called for the repeal of C-51. #RepealC51 #SECU

MattDube
Tsuu T'ina First Nation Councillor Regena Crowchild says C-51 reminds her of other laws that infringe on First Nations' rights. #SECU

MattDube
En route vers notre prochaine destination: Calgary. #SECU

Rob_Oliphant
#SECU committee is in #Calgary today hearing from Cdns on the #NationalSecurityFramework at the Delta Downtown. http://bit.ly/2e0kKpk

canadaCJFE
TONIGHT in #Calgary the Committee on Natl. security is holding the first #C51 consultation. Turn out, have a say! http://cjfe.org/calgary_consultation …

deltatux
#SecTORca: @Snowden & @mgeist does shout outs for @OpenMediaOrg, #bclu and the Canadian Civil Liberties Union!

NATIONAL SECURITY / SÉCURITÉ NATIONALE

UTLaw
Op-ed, Prof. Kent Roach and @cforcese: "Renewed Bill **C-51** questions: Balancing national security with civil liberty" https://t.co/r7nzhpV8JV

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

TopBramptonNow
Brampton man with bogus Canadian citizenship jailed 15 years for cocaine smuggling at Pearson airport Brampton… http://www.bramptonguardian.com/news-story/

LAW ENFORCEMENT / APPLICATION DE LA LOI

UBCIC
.@CBC_Aboriginal Culture of fear prevents Indigenous victims of police brutality from reporting alleged crimes http://ow.ly/WwLf505zCi5

CBCSaskatoon
Police uniforms, passports among items stolen by 'semi-organized' ring, officers say http://www.cbc.ca/1.3810226 #yxe #ypa via @CBCManitoba

https://twitter.com/edmontonjournal
Police arrest seven people from two organized crime rings in ATM thefts http://ow.ly/tOFj305iLki

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

globeandmail
Rights commission decries 'shocking' Ontario solitary-confinement numbers http://trib.al/aVyFXAe

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

CBCVancouver
Experience The Highway of Tears via VR & @TheCurrentCBC http://ow.ly/UDIR305iIju #MMIW

AngelaSterritt
#MMIW families still waiting for promised help, Bernadette Smith says http://www.cbc.ca/1.3809854

ONWA
'It's time for action': Manitoban wants promised MMIW inquiry family liaisons https://t.co/mF9bEkX3nE

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

660NEWS
#Alberta justice minister to research cannabis policies in Colorado: http://www.660news.com/2016/10/18/alberta-justice-minister-research-cannabis-policies-colorado/ …

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

Today's News / Actualités
October 19, 2016 / le 19 octobre 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Snowden: 'Politics of fear' keep Trudeau from repealing Canada anti-terror law
Edward Snowden has waded into the simmering debate over Canada's controversial anti-terror law, saying that Justin Trudeau was reluctant to repeal the law out of a fear of appearing soft on terror. Speaking to an audience in Toronto on Tuesday, Snowden pointed to a campaign promise by the Canadian prime minister to amend the sweeping legislation, which gives security forces heightened powers to apprehend suspected terrorists and disrupt their activities. "But he's been in office a little while now and we haven't seen that actually come to pass," said Snowden, appearing at the SecTor

cybersecurity conference via videolink from Russia. (…) Last month the Liberal government launched a wide-ranging consultation on national security, meaning any potential changes to the law will probably be delayed until next year. The extra time will offer the government the opportunity to get it right, said **Ralph Goodale, Canada's public safety minister**, as he announced the consultation. ***"A lot of people felt shut out, and we promised to give them the opportunity to be heard."*** Guardian

TOP STORIES / MANCHETTES

Nil

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Flooding in Prince County possible on Friday and Saturday: Environment Canada
Environment Canada has issued a special weather statement, warning of potential heavy rain and localized flooding in Prince County. The weather will be caused by a "vigorous low pressure system," expected to cross the Maritimes on Friday and Saturday. CBC News: Compass weather specialist Kevin "Boomer" Gallant says the system is coming off the Great Lakes, and is absorbing tropical moisture from a low to our south. CBC News

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

A mania for consultations
What do you think of The Fisheries Act? Got some thoughts about workplace flexibility? How about foreign aid? And where do you stand on a national immigration detention framework? These are just a tiny few of the literally hundreds of consultations the Trudeau government has completed or is in the midst of completing in its first year… As of this writing, there are precisely 78 different "open consultations" the federal government is engaged in right now. That link will take you to the federal Web site: ConsultingCanadians.gc.ca where, if you were so inclined, you could review the 316 consultations that the Trudeau government has already completed just since January 1. Most of these consultations are the self-service kind. But for the big headliners when it comes to consultations, MPs are needed, whole committees of MPs, which have been criss-crossing the country in search your views on electoral reform, the next federal budget, Canada Post and national security:… We've all got opinions about national security right? Of course we do. And that was just the thinking behind the MPs on the House of Commons Standing Committee on Public Safety and National Security as it decided to do its own national cross-country listening tour. Don't miss them today in Toronto, tomorrow in Montreal, and Friday in Halifax. National Post

NATIONAL SECURITY / SÉCURITÉ NATIONALE

The other hell: Lt.-Gen. Roméo Dallaire's new book is a brutally revealing memoir about his own inner torment
An editorial piece states, "One night after he was medically discharged from the army in April 2000, former Lt.-Gen. Roméo Dallaire drank most of a bottle of scotch in his Hull, Que., apartment before he opened a metal box containing his father's medals and his 50-year-old razor. Very slowly, he began to slice himself, first his thighs, then his arms. It was another of Dallaire's rolls of the dice, another in what has become an uncountable number of attempts, stretching over two decades, to kill himself "accidentally," through behaviour so reckless it is a wonder he is alive now. Much of it, in Africa to start and later in Canada, involved driving, including reaching 150 km/h on a Quebec road with his young children in the back seat. As UN commander in Rwanda during the still tense days after that nation's 1994 genocide bled to a halt, Dallaire would drive up, alone and at night, to checkpoints manned by heavily

armed teenagers as skittish and traumatized as he was. (…) If PTSD has had a face in Canada over the last 20 years, it is Roméo Dallaire's. His life story, in effect, is a personal history of how Canada, and the modern world in general, has responded to PTSD. "That's putting a lot on my shoulders," he protests, before conceding its inevitability and discussing the incomprehension that faced him when he returned to Canada in 1994, an incomprehension he fully shared." Macleans

Concordia's MIGS to host program to fight on-line extremism
As he was sipping a well-made latte in Montreal's Mile-End neighborhood, Kyle Matthews told *The Suburban* that violent extremism has already become one of the more important challenges to peace and security within the western world. "Everybody knows that ISIS is a genocidal force that wants to squash anyone who is different from what they are," said Matthews, "… but at this point, it's going to take a lot more than a 1-888 help-line number to do something about it." As the Executive Director of MIGS — the Montreal Institute for Genocide and Human Rights Studies — Matthews believes that ISIS and other radical jihadist groups would have been nothing but a collection of local (yet deadly) political movements if it had not been for the convergence of their radical ideology combined with the power of the new social media that's still being used to promote their cause and to lure vulnerable young people into joining their ranks. (…) "These were not isolated incidents," said Matthews. "We have several cases in Canada where individuals are being radicalized online and targeted by online (jihadi) recruiters in much the same way as sexual predators scour the web to find their victims" Suburban

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Les services frontaliers souhaitent identifier un mystérieux détenu anonyme
L'Agence des services frontaliers du Canada (ASFC) demande l'aide du public pour identifier l'individu qui se trouve en détention puisqu'il a été «jugé interdit de territoire» au pays. Pour ne pas nuire à l'enquête, l'ASFC n'a pas précisé depuis combien de temps l'homme est détenu. L'agence a tout de même révélé quelques autres détails. «L'enquête de l'ASFC révèle que l'individu est arrivé au Canada le 2 août 1969 à Montréal, à bord du train numéro 9 du chemin de fer de la fonction de Napierville, en provenance de la ville de New York. On croit que l'homme aurait de la famille à New York ou aux États-Unis», a indiqué l'Agence des services frontaliers par voie de communiqué. À ce jour, l'inconnu soutient être venu au Canada pour éviter la conscription. QMI Agency (Journal de Québec; Journal de Montréal); 680 News

Canada Acknowledges Antidumping
This has never happened before. This is very important. Trade lawyers outside Canada (and inside Canada) will be shocked by the steps being taken in Canada during an active antidumping proceeding. On October 16, 2016, the Department of Finance asked the Canadian International Trade Tribunal to commence a section 18 (of the *Canadian International Trade Tribunal Act*) reference concerning the effect of preliminary and final antidumping duties on gypsum board (also called drywall and wall board) from the United States into Western Canada (British Columbia, Alberta, Saskatchewan, Manitoba and the Yukon and Northwest Territories). The antidumping proceedings at the center of the request are the Canada Border Services Agency ("CBSA") dumping investigation that commenced on June 8, 2016 and the Canadian International Trade Tribunal ("CITT") injury inquiry that commenced on September 6, 2016. Mondaq

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Russian Hacker Suspected in LinkedIn Breach Arrested - ABC News
A suspected Russian hacker has been arrested in the Czech Republic for his alleged role in a cyber-attack on social media giant LinkedIn, sources told ABC News. Category. News & Politics. License. Standard YouTube License. Show more. Show less. ABC News

Innovation expert Alec Ross shares tech predictions in Saint John

Alec Ross has seen the future - and, believe it or not, it's not totally dystopian. "I do think tomorrow will be better than today," said Ross, a former senior adviser for innovation to Hillary Clinton, who is the Democratic nominee running in the U.S. presidential election. He has travelled to 41 countries, observing technologies that will radically alter the way people live in the coming decades. His New York Times best selling book, The Industries of the Future, examines the role of robotics, cyber security, the commercialization of genomics, and big data on world markets. Among the lessons Ross gleaned in his travels and research is that data, in the same way that land and iron were the raw material of past ages, is the raw material of the information age. "He or she who owns the data, controls the data, or can draw meaning from the data, is who creates the businesses and industries of the future," said Ross. Coding is crucial. In addition to the importance of big data, Ross says coding is also changing our lives in fields ranging from healthcare to warfare. "The weaponization of code is the most significant development in conflict since the weaponization of fissile material," said Ross. "The difference being creating a nuclear weapon requires access to the scarcest of scarce scientific talent, and transuranium elements, whereas hacking is a lot easier." On a similar scale are innovations like the robotics being pioneered in Japan - including Robina, a robot programmed to take care of the elderly - which can be read as a sign of where Western culture is heading. "I think the robots of the cartoons and movies of the 1970s are going to be the reality of the 2020s," said Ross. CBC News

LAW ENFORCEMENT / APPLICATION DE LA LOI

Ottawa police shouldn't investigate Nunavut RCMP: MLA
A Nunavut politician is calling for an end to a contract that sees Ottawa police investigate his territory's RCMP officers in cases of potential wrongdoing. Former Nunavut justice minister Paul Okalik says an Ottawa police sergeant's racist remarks after the death of Inuk artist Annie Pootoogook show the capital's force cannot be trusted to investigate the territory's Mounties... Insp. Jamie Dunlop, who oversees the training of Ottawa officers who perform those investigations, disagrees... The agreement between the Ottawa police and the Nunavut RCMP has been in place since 2012 and has resulted in 14 investigations, said Dunlop. Of those 14, two have resulted in charges being laid against police. Dunlop acknowledged the public might have questions about police forces investigating each other... Dunlop said there is currently no plan to end the agreement between Ottawa police and Nunavut RCMP. Metro News

Child sexual exploitation bust in northern Alberta nets 14 suspects
Fourteen suspects have been charged with online child sexual exploitation following a lengthy investigation across northern Alberta. An investigation by Alberta Law Enforcement Response Teams (ALERT) resulted in 33 charges. The people charged are from communities across northern Alberta. ALERT's Internet Child Exploitation (ICE) unit launched Operation ICE Reign between June and October 2016. ICE is an integrated unit with members from both the Edmonton police and the RCMP. CBC News

Coke, meth, guns seized in co-ordinated raid in Western Manitoba
A seven-month police investigation has taken down an alleged drug trafficking network in western Manitoba. At a press conference at RCMP headquarters in Winnipeg today, officers with Brandon police, the RCMP and Winnipeg police had big bags of cocaine, methamphetamine and marijuana on display next to a table of firearms and photos of vehicles seized during Project Derringer. Between Oct. 12-15, police executed search warrants and made arrests in the Brandon and Griswold, Man. areas as well as in the Toronto area. Leslie Gerald Bisson, 36, of Griswold, Justin Tyler Reimer, 28, of Brandon and Javed Ali, 29, of Georgetown, Ont. face numerous charges. The investigation was conducted by the Manitoba Integrated Organized Crime Task Force. The investigation is ongoing with further charges pending, police said. Winnipeg Free Press; Canadian Press (Metro News); Brandon Sun; CTV News

Fed up with crime, Langley residents demand action from RCMP
Miranda and her sister were sound asleep last July when their father encountered an intruder with a hunting knife hiding in the basement of their Langley home. Jamie Shaw believes the man had been in the family home for almost two hours... The incident wasn't isolated: Residents of a rural Langley neighbourhood say they've seen an alarming escalation in break-ins and property theft... haw is now part of a Block Watch program that's pinpointed several local properties believed to be tied to the spike in

crime. He's one of dozens of people demanding authorities to do more to protect them, and on Tuesday night, dozens of citizens fed-up with break-ins and living in fear came together to call for action from their mayor and the RCMP. One woman said when she has spoken to police she was "brushed off." "We're told we should not worry, and it won't happen again," she said... The mayor of Langley, also a victim of theft, says he plans to work with the community to find a solution. Langley RCMP Spt. Murray Power said it's alive to the concerns of the community. "We've been in contact with a number of people. We know the concerns have been out there since the incident in July, which concerns us all," he said. Langley RCMP have plans to meet with concerned residents in the coming weeks to organize a coordinated block watch involving both neighbours and police. CTV News

OPP officer's son, who pleaded guilty to sex crimes against kids and animals, designated dangerous offender

An Ontario man who pleaded guilty to sex crimes against young children and animals has been designated a dangerous offender. A Barrie, Ont., judge said Shayne Lund has shown a "complete inability to control his sexual impulses" and only expressed a desire to do so after his arrest in 2013. Justice Joseph Kenkel told the court Lund could not be trusted to commit to psychological treatment given his "history of manipulation and deceit" and that sexual gratification has so far been the main focus of his life. The dangerous offender designation means Lund could be imprisoned indefinitely... Lund's father, an Ontario Provincial Police constable, appeared distraught as the ruling was read in court Wednesday. Mark Lund, a 27-year veteran of the force, was recently charged with obstruction of justice. Police have released no other details but say he was off-duty at the time of the alleged offence. Canadian Press (National Post)

Man, 19, charged with sexual assault in Port aux Basques

A man from Port aux Basques has been charged with sexual interference and sexual assault involving a minor following an incident last month, the RCMP say. Police said in a statement on Wednesday that a 19-year-old is facing charges following a complaint of "alleged inappropriate interaction" between the man and a complainant who is under 16. The incident is alleged to have occurred in September, according to Const. Matthew Christie... The RCMP and the Department of Children, Seniors and Social Development jointly investigated the complaint. The 19-year-old was charged Saturday and is set to appear in court in December. He has been released from custody. CBC News; Gulf News

Human trafficking sweep catches Sudbury senior

The Sudbury senior charged with child pornography counts this week was one of 32 accused swept up in a six-day co-ordinated investigation into human trafficking across Canada. Police say officers laid 78 offences during the sweep. More than 390 officers from 53 Canadian police services, plus the FBI in the United States, directly engaged with people suspected of working in the sex trade, potentially against their will. Most of the arrests in Operation Northern Spotlight occurred in Ontario where 25 people were charged with 67 offences. Sudbury Star

US man admits raping boy, 6, after Canadian authorities intercept broadcast

A Pennsylvania man has admitted he sexually assaulted a six-year-old boy after Canadian authorities intercepted an Internet broadcast of him raping the child. U.S. authorities later discovered 10 other recorded assaults of the boy. PennLive.com reports 20-year-old William Byers Augusta pleaded guilty in Carlisle on Tuesday to charges including rape of a child. Prosecutors say Canadian authorities intercepted a broadcast of Byers Augusta sexually assaulting the boy in July 2015. Investigators found videos showing Byers Augusta assaulting the child, including one of him and 62-year-old Ira Task simultaneously sexually assaulting the child. Associated Press (Winnipeg Sun, Toronto Sun, Ottawa Sun, Edmonton Sun, Calgary Sun)

Tweet targeting Quebec women with reference to Marc Lépine prompts police probe

Quebec provincial police are investigating after someone tweeted a threat against women, making reference to the infamous hit list drawn up by Montreal Massacre shooter Marc Lépine. The tweet was in response to a new book celebrating the success of women in Quebec... nvestigators met with the man who sent the tweet on Tuesday, and Crown prosecutors will decide whether or not to press charges.

According to SQ spokeswoman Andrée-Anne Bilodeau, past cases that involved uttering threats or intimidation have resulted in anything from no jail time to a five-year sentence. Clermont-Dion said she was happy to see the SQ react so fast and to see that other men were taking a stand against the comments made against her and other women. CBC News

Man on P.E.I. tasered three times by police
A Cornwall man the police Tasered three times before managing to subdue him will be back in court next month for sentencing after he pleaded guilty to resisting arrest. Paul Godfrey, 51, appeared before Chief Judge Nancy Orr in provincial court in Charlottetown where the case was adjourned for sentencing... The officer followed the truck as it drove a short distance at a high speed before pulling into Godfrey's driveway. After pulling in behind Godfrey's truck the officer got out and ordered him to stop, saying he didn't want to have to chase him into the house. He eventually stopped and after a second officer arrived Godfrey struggled with them during his arrest for impaired driving... Godfrey managed to slip away and one of the officers ordered him to stop or he would use his Taser. Godfrey didn't stop and the officer Tasered him. Once the Taser finished cycling Godfrey got up and ran away. The second officer Tasered him again, but Godfrey was able to get up and go into his house. Once inside the police chased him through the house, Tasered him a third time and tackled him in the garage. MacDonald said on the way to the detachment Godfrey told the police he didn't feel well. An officer pulled the Taser prongs out of Godfrey at the detachment and he went to the Queen Elizabeth Hospital. Gander Beacon

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Dangerous offender's conviction stands, but sentence reduced
Although met with failure at attempting to have his conviction and dangerous offender designation overturned, Donald Francis Wilton had some success in appealing the length of his sentence... The 39-year-old appealed and, in June, the Saskatchewan Court of Appeal heard arguments from Crown prosecutor Dean Sinclair and Wilton's lawyer Kevin Hill. Hill argued the verdict was unreasonable and further urged the court to toss out the DO designation on grounds the sex offence - the first conviction of its kind for Wilton - does not fit a pattern of previous violent, criminal behaviour. Hill then asked the court to reduce Wilton's custody term, arguing sentencing Justice Guy Chicoine basically tacked on time after considering Wilton would receive parole or statutory release that could start before programming is completed or has taken effect... While the province's highest court didn't agree with Wilton's position on conviction or the DO finding, it found Chicoine had erred in sentencing and replaced the 45 months with 36. The court noted Chicoine's decision placed much of its focus on offender rehabilitation, with an estimated 18 months to three years needed to complete core programming, if everything went well... While the appeal court found Chicoine did not err in considering early release when deciding on sentence, it added there is no guarantee Wilton will receive such a release. Rather, the court noted there is a distinct possibility the parole board could hold Wilton until the end of his custody term - meaning the sentencing judge erred in assuming early release when crafting his sentence. Postmedia Network (Leader-Post)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Website aims to connect community with cops
The Sidney North Saanich Community Consultative Committee launched their website Monday with an aim to help the community connect with local police to help solve community problems. In spring of 2015, local police decided they didn't have an informal platform to communicate with. "We felt like there were probably issues of community concern that we weren't hearing about, because people only phone us for certain reasons," said Corp. Erin Fraser of Sidney North Saanich RCMP. Fraser said it's about increasing communication overall, not just bringing issues to RCMP attention. She said it's also a way to network in the community to get to know residents better. The committee, which has existed now for around two years, initially hosted a series of town hall presentations to try and procure volunteers. The committee

ended up with 14 volunteer members representing a cross section of Sidney and North Saanich residents. Peninsula News Review

Le théâtre pour sensibiliser les jeunes à la cyberintimidation
Après un passage sur la Côte-Nord, la compagnie Samsara Théâtre s'arrête en Gaspésie et au Bas-Saint-Laurent pour présenter sa pièce « Noyade(S) » qui aborde la construction de l'identité à l'ère numérique. Depuis deux ans, la compagnie de théâtre sillonne le Québec pour raconter devant des élèves des histoires de cyberintimidation et de suicides. Radio Canada

Case of N.S. teens accused of sharing intimate images put over to November
Police and lawyers are seeing a rise in the number of investigations involving the sharing of intimate images without consent, according to a Crown attorney handling one of the largest such cases Nova Scotia has faced following the introduction of legislation dealing with the disturbing phenomenon. Peter Dostal said Wednesday that the case involving six Nova Scotia teens charged with sharing images of at least 20 high school girls is not the first to test the relatively new legislation, but it is one of the biggest and most complex... Several lawyers representing the young men were in provincial youth court in Bridgewater to request more time before entering pleas. They are due back in court on Nov. 28. Dostal said a trial could be lengthy due to the number of people charged in the matter and the volume of evidence, much of it taken from electronic devices and cellphones. Dates in July, August and September have been set aside for a possible trial... Police in Bridgewater launched a year-long investigation in response to complaints from school officials, leading to the seizure of a number of electronic devices -- mainly cellphones -- which were handed over to the RCMP Technological Crime Unit for analysis. The Mounties found more photos, and a search warrant was drafted to obtain information from Dropbox, a U.S.-based file-sharing service. Using an international treaty, Canadian officials obtained the files through the FBI. The case is one of the first in Canada involving legislation introduced in late 2013 after the death of Nova Scotia teen Rehtaeh Parsons, which captured national attention. CTV News

RCMP presents crime statistics
RCMP Sgt. Mark Harrison presented an update on the crime statistics in Pincher Creek at the Committee of the Whole meeting of council last Thursday. Harrison had the statistics for the first three-quarters of 2016, comparing them to the past several years of work in Pincher Creek. Although most of the statistics presented were concurrent with previous years, there was one stand-out that Harrison outlined. Over the first three-quarters of 2016, there was an increase in drug trafficking, but contrary to assumption, Harrison assured that the increase was a positive sign. There were 11 incidences of drug trafficking issues brought to RCMP for the first three-quarters of 2016, compared to seven in 2015, and two in 2014. Harrison said that this is not necessarily an increase in trafficking issues, rather, the RCMP has been better able to investigate and disrupt drug operations. Pincher Creek Echo

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Indigenous women focus of Museum exhibit
The Peace River Museum, Archives and Mackenzie Centre (Museum) is honouring murdered and missing women as well as the historic struggle of all women in its newest exhibit. Titled “Silent Dreams: Their Story”, the exhibit puts a spotlight on both indigenous and non-indigenous women’s struggle in obtaining personhood in Canada. It also looks at the traditional role indigenous women played in their societies, and how colonization disrupted the traditional matriarchal structure integral to aboriginal culture. “It’s really important to be able to understand that historical context,” said Laura Gloor, Coordinator with the Museum. “It’s not about pointing fingers and creating blame, it’s about understanding. That’s where it originated. That’s where those derogatory words, those expressions, that attitude came from.” Peace River Record-Gazette

Inuit women's group frustrated by lack of communication on MMIW inquiry

It's been almost two months since the inquiry into missing and murdered Indigenous women and girls began its work and the national Inuit women's group says it's still waiting to hear from the organizers. "What we're frustrated about is we haven't heard anything," says Rebecca Kudloo, president of Pauktuutit. "We don't even have phone numbers to contact them. There's no connection." Kudloo says her organization has not heard a word about the timeline or the work of the inquiry since August when the names of the commissioners were announced. The inquiry officially started its work on Sept. 1, and is expected to last more than two years. CBC News

«On voit des signes positifs et encourageants»
De grands défis restent à réaliser pour amener une cohabitation totalement harmonieuse un an après la crise de Val-d'Or. Des pas ont toutefois tracé le chemin vers le «mieux vivre ensemble», selon le maire Pierre Corbeil. «Le 22 octobre 2015, l'émission Enquête diffusait un reportage sur une situation critique vécue par des femmes autochtones de Val-d'Or. Ce fut un choc. La problématique a été mise en évidence et il fallait se relever les manches pour trouver des pistes de solutions, a fait valoir M. Corbeil lors d'un point de presse, le 18 octobre. «Une mobilisation sans précédent de notre milieu s'est enclenchée et des actions se sont déclinées sous plusieurs formes tout au long de l'année. Toutes visaient à dénoncer les formes de violence faites aux femmes autochtones et allochtones, a-t-il ajouté. L'Écho Abitibien Le Citoyen

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Alberta Justice Minister to get cannabis crash course in Colorado
Minister Kathleen Ganley will travel to Colorado from Thursday to Saturday, with hopes of learning how they've handled the legalization of marijuana. Alberta Justice Minister and Solicitor General Kathleen Ganley won't be trying any of the brownies when she heads down to Colorado for a crash course in cannabis. Instead, she hopes Alberta can learn from how Colorado has proceeded since marijuana was legalized in 2012, as Canada prepares for bud to hit the legal market in spring of 2017. The two biggest problems that Ganley hopes to address during her $4,000 trip south are keeping cannabis out of the hands of youngsters, and creating a system to detect those that drive under the influence. "They are still working on the science of what constitutes impairment. They measure your ability to walk straight and a lack of coordination, but there is no set content level and a method for testing (like with alcohol impairment)." Metro News; Edmonton Sun

A spiritual perspective on the legalizing of pot
An opinion piece states, "The city is gaining a surprising number of cannabis dispensaries recently. But maybe that shouldn't be a surprise. The wisdom of the drug war is finally coming under intense scrutiny, for good reason. Current policy has led to imprisonment, marginalization and needless deaths, including over 300 illicit drug-related deaths in B.C. in just the first months of 2016, in part due to toxic additives. Add to this the heavy social and economic costs of illegal activities and law enforcement. We've spent decades assisting too few to lift themselves out of addiction and too many to ill-gained wealth. On the other hand, our misgivings about decriminalization may result from a fear that it would lead to increased recreational use among all ages, particularly youth. It's a legitimate concern. Alcohol is currently the most widely used and abused drug by a wide margin. Health Canada reports that 78% of the population consumed alcohol in the last year surveyed. Of those, almost 20% exceeded Canada's Low-Risk Alcohol Drinking Guidelines. Consequences of abuse range from disruption in family life to safety issues. "In Canada, alcohol has been a factor in 30% - 40% of road deaths for the past 15 years," says the public education group Change the Conversation. No doubt people wonder what would happen if a large increase in drugged driving were added to these figures, if street drugs were as freely available and accepted as alcohol." Vancourier

PUBLIC SERVICE / FONCTION PUBLIQUE

Nil

OTHER / AUTRES

Bone of Connor Hayes, Ottawa man swept away in a New Zealand landslide, found
A hunter in New Zealand has found a bone belonging to a 25-year-old Ottawa man who was swept away with his girlfriend in a landslide in 2013. Connor Hayes and Joanna Lam, 24, were travelling together in New Zealand in 2013 before Lam was scheduled to start a job as a medical imaging specialist with a health board on the country's South Island. The couple was last seen on Sept. 10 that year. New Zealand Police then discovered pieces of the couple's rented camper van two weeks later in a gorge on the Hasst River. Days later police discovered Lam's body. Hayes's remains weren't found. But in August 2016, a hunter found a human thigh bone where the Haast and Burke rivers meet, according to New Zealand officials. DNA analysis confirmed the bone belonged to Hayes. Police and volunteers conducted another search of the area the bone was found in on Oct. 16. "A number of items of interest" were recovered from the riverbed but police haven't yet confirmed whether they belong to Hayes. Insp. Mel Aitken with New Zealand Police says anything believed to belong to Hayes, including bones, will eventually be released to his family in Canada. CBC News

INTERNATIONAL

As territory shrinks, IS group looks for new money sources
As the Islamic State group sees its territory shrink to half its original size and its dreams of a caliphate evaporate, the extremist fighters are losing access to the sources of revenue that once gave them their power, prompting them to turn to extortion, kidnapping or foreign donations like their predecessors, the militant group al-Qaida. The Islamic State group had a unique ability to capitalize on the natural resources of its territory in Iraq and Syria and swiftly implement a system of taxation and governance that allowed it to rule an area that once was the size of Switzerland. As the battle gets underway to retake Mosul, the group's largest stronghold in Iraq, the Islamic State group is being denied access to revenue sources such as oil and gas and cash reserves that once amounted to more than $1 billion in 2014, said Daniel Glaser, the Treasury Department's assistant secretary for terrorist financing. With those resources slipping away, the Islamic State group is expected to revert to "traditional methods we see al-Qaida using — whether it's deep-pocket donors, whether it's charities, whether it's NGOs, whether it's criminal activity," Glaser said in a recent discussion at the Washington Institute for Near East Policy. Metro News

UPDATED: Prominent Iranian human rights activist blocked from leaving country
Mansoureh Behkish was subpoenaed to court on the morning of Sunday, Oct. 16. A family member said the subpoena letter was delivered to Mansoureh Behkish in her apartment in Tehran, and she was given five days to show up at Evin revolutionary tribunal court. Background story below. Iran has once again targeted a prominent human rights activist, who lost six family members to state executions and killings in the 1980s. Mansoureh Behkish, who's been jailed several times for her past advocacy work, had her passport confiscated indefinitely and without explanation by authorities. It happened as she was about to board a plane to Ireland, where her daughter lives. Behkish said security agents did not tell her why they stopped her from boarding and took her passport at Tehran Imam Khomeini International Airport on Sept. 16. CTV News

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

@LarryMillerMP

Liberals voted against my PMB C-230 & against law-abiding gun owners I have commitment from Lib PS 2 Min Goodale they will fix it #yaright

@alissaskins
.@JustinTrudeau @RalphGoodale remember when you promised to amend Bill C-51 but it's been a year now& no #RealChange

Colinfreeze
14. Committee has raised issue of @NoFlyListKids several times but no one offers way forward. Ball appears to be im Min @RalphGoodale court

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Colinfreeze
51. The #cdnpoli Lib chair of #SECU (oliphant) just reminded audience that the party that promised to repeal #C51 was the NDP & they lost.

@Terjohns
This is our last chance to repeal #C51 and restore our privacy rights. Speak out: http://om4.me/ZT6 #SaveOurSecurity #YourNatlSec

@guardianworld
Snowden: 'Politics of fear' keep Trudeau from repealing Canada anti-terror law https://www.theguardian.com/us-news/2016/oct/19/edward-snowden-canada-anti-terror-law-justin-trudeau?CMP=share_btn_tw … #C51

Colinfreeze
43. FYI a Canadian named Tamim Chowdhury published an article that I found really interesting in the context of #C51

TOAdamVaughan
@cwenraed @neville_park Middle? 2 meetings left in term.C51 being fixed now. Consultations in TO this week. New housing $ delivered- proud!

cancivlib
Tonight our @isukanya is in Ottawa to raise concerns about #BillC51 with the Ministers of Public Safety and Justice! #C51onTrial

cancivlib
Torontonians! Join us tonight 5:30pm at the Radisson Admiral Hotel for the national security consultation (government ID required).

MattDube
Canadian Journalists for Free Expression call for repeal of C-51. #RepealC51 #SECU

Colinfreeze
21. !! Segal says existing review bodies -SIRC OCSEC- should be mothballed as currently constructed to make way for UK style leg review.

Colinfreeze
20. Segal says C22 leg committee too small as currently constructed. Now 9 should be 12. Needs to have its chamber located far from CSIS HQ

Colinfreeze
15.MP raises what @rcmpgrcpolice Commish Paulson said 2 weeks ago about police "going dark" due to encryption @canadaCJFE says no backdoors!

Colinfreeze
14. Committee has raised issue of @NoFlyListKids several times but no one offers way forward. Ball appears to be im **Min @RalphGoodale** court

Colinfreeze

11. Cases of RCMP trying to ferret out sources of journos @BMakuch & Bellavance raised at #cdnpoli #secu as eg of how C51 could chill.

Colinfreeze
6. Atkey says "broad overview" by C22 MPs allowed into govt chamber o secrets a worthwhile end. "Don't get bogged down in details" he says.

Colinfreeze
5. Atkey says C51 disruption warrants prima facia unconstitutional. Next @marcomendicino asks if C22 committee risks redundancies with SIRC?

Colinfreeze
4. Lib @marcomendicino asks ex CSIS watchdog Atkey about constitutionality of C51 law where CSIS can go to court for disruption warrants.

Colinfreeze
3. 2nd #SECU speaker is @canadaCJFE which has a litany of issues with govt surveillance:CSE Metadata, C51 SCISA, CSIS disruption warrants...

Colinfreeze
2. First speaker is Ron Atkey, ex-CPC ex-SIRC, says why not make PM's natsec advisor a referee for C-51 SCISA sharing of govt data? #cdnpoli

Colinfreeze
1. Looking in on legislative branch review of #cdnpoll national security -- such as it currently is -- today. HOC #SECU in Toronto today.

canadaCJFE
Executive director of @canadaCJFE Tom Henheffer preparing to address the expert witness panel on C51. Stay tuned on FB. #C51onTrial

canadaCJFE
Tom Henheffer references chilling effect of #C51 on protest. "The 2010 G20 repression happened before #C51 was law. What would happen now?"

Rob_Oliphant
On Now: #SECU cmtee is hearing from witnesses in #Toronto. Join for the open mic at 5:30pm. http://bit.ly/2e0kKpk

davidakin
#SECU 33 meets now in Toronto. National Security Framework. Link to details: http://bit.ly/1o8816t #cdnpoli

Rob_Oliphant
Day 3 of #SECU consultations on the #NationalSecurityFramework. Join us in #Toronto at the Radisson on Queen's Quay: http://bit.ly/2e0kKpk

OpenMediaOrg
TONIGHT! Come have your say at the crucial Parliamentary hearings on Bill #C51. Everyone's invited! http://ow.ly/uknk305j0HJ #Toronto

OpenMediaOrg
@Claire_Wahlen @bccla hi! here's a debrief of the Vancouver #C51 hearings + video of @ltribe's testimony: https://openmedia.org/en/laura-tribe-testifying-c-51-public-hearings-vancouver …

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CBAImmigration
CBSA seeks name of alleged draft dodger, 47 years later - CityNews http://www.citynews.ca/2016/10/19/border-patrol-seeks-name-alleged-draft-dodger-47-years-later/ … via @CityNews

CYBER SECURITY / CYBERSÉCURITÉ

@dharpan
LinkedIn blames Russian hacking suspect for 2012 breach #Cybersecurity
http://www.pcworld.com/article/3132931/linkedin-blames-russian-hacking-suspect-for-2012-breach.amp.html ...

LAW ENFORCEMENT / APPLICATION DE LA LOI

rcmpmb
Project DERRINGER was a 7 month investigation into an alleged drug trafficking network supplying Brandon & communities in western MB #rcmpmb

metroottawa
Former Nunavut justice minister says Ottawa police shouldn't investigate Nunavut RCMP http://bit.ly/2ei3Pjh

CTVVancouver
Frightening home invasion galvanizes rural community to demand action on crime. @CTVSarah
http://bc.ctvnews.ca/fed-up-with-crime-langley-residents-demand-action-from-rcmp-1.3122027 …

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

UBCIC
.@CBC_Aboriginal Inuit women's group frustrated by lack of communication on MMIW inquiry
http://ow.ly/aEB1505BR4E

BlackPressMedia
Call from #Chilliwack for expanded #MMIW inquiry to add men and boys http://bit.ly/2dr3czA

INTERNATIONAL

@canadaCJFE
Activist Mansoureh Behkish detained in #Iran and stripped of her passport for her advocacy work on human rights.
http://bit.ly/2edPPVU

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

Sent to: !INTERNAL; !INTERNAL 2; CBSA Today's News; CSC & PBC Today's News; PS Today's News; RCMP Today's News; RCMP Today's News 2

Today's News / Actualités
October 20, 2016 / le 20 octobre 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

The night Colten Boushie died: What family and police files say about his last day, and what came after

… The killing of Colten Boushie has set Saskatchewan on edge. On Aug. 9, 22-year-old Colten and his friends set out from the Red Pheasant reserve, about 150 kilometres west of Saskatoon, for a day of swimming and drinking. The car they were riding in had a flat tire and they pulled into the yard of a local farmer named Gerald Stanley. What happened next is uncertain, but one thing is clear – Colten wound up dead. To summarize the competing views of the tragedy in their extremes: either Colten was the victim of

a racially motivated killing, or Colten's friends were trespassers and thieves who met swift, vigilante "justice." There are a number of other possibilities, too, of course… As the court process plays out, tensions are high and the facts contested. The aftermath has brought angry protests and signs that the white community is fearful of a backlash. One local pastor told the Saskatoon Star-Phoenix that Colten Boushie "is the Rodney King of Western Canada," and said his killing had unleashed a lot of hidden ugliness. Hundreds of people gathered to protest outside the court house for Mr. Stanley's first court appearance, watched carefully by RCMP on rooftops, and there was anger when he was granted bail on a $10,000 cash surety. Five days after the shooting Saskatchewan Premier Brad Wall called for an end to the flood of racist comments on social media directed at Indigenous people. And in late September, after armed, masked assailants threatened a farm hand in the province, local news was flooded with stories of farmers arming themselves for the harvest season. In response to the growing tensions, including Facebook pages featuring photos of farmers carrying firearms, the RCMP Superintendent held a press conference to ask residents to put their guns away. Mr. Boushie's killing lingered like an unspoken subtext. His slaying has become a symbol of a broken relationship between Indigenous people and their white neighbours. The anger that fuelled protests outside the bail hearing for Gerald Stanley, the 55-year-old farmer accused of second degree murder in connection with Mr. Boushie's death, has not subsided. Kimberly Jonathan, a vice-chief with Saskatchewan's Federation of Sovereign Indigenous Nations, said one of the principal reasons that violence hasn't erupted is that the Boushie family has called for peace. Ms. Jonathan, who urged that the shooting be investigated as "a crime based on race," said she met with **Public Safety Minister Ralph Goodale** and warned him of the seriousness of the situation. "I said, 'You ought to thank the family, because they came out with peace in memory and love for Colten. They could have gone the other way and there would have been, and I'm not exaggerating, there would have been a lot more blood shed.' "But I said we can't promise it's going to continue that way because of how the [justice] system has been lacking." Globe and Mail

MP Miller's firearm bill defeated
A private member's bill to amend the Criminal Code by Bruce-Grey-Owen Sound Larry Miller has been defeated. The House of Commons voted on Bill C-230 — An Act to amend the Criminal Code (firearm — definition of a variant) on Wednesday, where it was defeated 202-81… Miller said he was not surprised his bill was defeated, but he intends to write **Ralph Goodale, Minister of Public Safety and Emergency Preparedness**, and his parliamentary secretary Michel Picard and urge them to make the changes.
"I would have withdrawn my bill if they would have put something on the table that would fix it. That is all I want is this thing fixed," said Miller. "It is an obvious flaw." Owen Sound Times

TOP STORIES / MANCHETTES

CBSA arrest five men in three separate cocaine seizures - The drugs were allegedly destined for Alberta
Weighing in at 445.7 pounds, cocaine, seized by Canada Border Services Agency (CBSA) in three separate busts over the last two months, has led to the arrest of five men. According to the CBSA, the first bust took place Sept. 2 in Coutts, when officers conducted a search of a commercial truck as it entered Canada with a load of televisions. During their search of the truck they discovered 60 packages of cocaine, weighing 69 kilograms, secured in the load of televisions. As a result of the seizure, two men were detained by CBSA for smuggling, under the Customs Act, and RCMP out of Raymond were contacted and asked to attend the port of entry. The following day, the RCMP charged 29-year-old Gurpreet Singh Cheema and 28-year-old Gurpreet Singh with Importing a Controlled Substance and Possession for the Purpose of Trafficking a Controlled Substance under the Controlled Drugs and Substances Act. The two men have already appeared in court and have been released with strict conditions. They're scheduled back in Lethbridge provincial court Oct. 24. Metro News; CBC News; Postmedia Network (Calgary Herald; Calgary Sun)

Seizure of fentanyl south of Nanaimo one of the largest in B.C., RCMP say
RCMP are calling a bust near the Nanaimo Airport one of the largest seizures of fentanyl in B.C. in the past few years. Mounties say a suspicious vehicle was pulled over on the highway just south of the airport on Oct. 10 around 5 p.m. Police say the driver, a Vancouver Island man, was arrested and his vehicle

was searched. Cash and one kilogram of powdered fentanyl was found, according to RCMP. Police state in a release "this makes the seizure one of the largest for the RCMP in British Columbia over the past few years." "Locating and reducing the importation and distribution of fentanyl continues to be a priority for the RCMP, especially given the number of opioid deaths in British Columbia," states Cpl. Tammy Douglas in the release. The man arrested has been released and no charges have been laid at this point. The Federal Serious and Organized Crime Group on Vancouver Island has taken over the investigation. Nanaimo News Now; CTV News; Canadian Press (Times Colonist); Cowichan Valley Citizen; Global News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Cape Breton prepares for more rain after historic flood
Cape Breton Regional Mayor Cecil Clarke says he's "petrified" of a looming rainstorm as the Sydney area continues to recover from severe flooding less than two weeks ago. A special weather statement issued by Environment Canada predicts heavy rains could cause more flooding this weekend in areas of the municipality badly damaged by more than 200 millimetres of rain on Thanksgiving Day.It's not yet known whether the weekend storm will actually cause trouble in Cape Breton, but the picture will become clearer early Friday morning, Clarke said Thursday. CBC News; Cape Breton Post

Mariners-in-training get a lesson in surviving Arctic waters
Swimming in Frobisher Bay in October is not everyone's idea of a fun time but for sailors who hope to navigate Arctic waters it's a necessary skill to have. This morning a group of sailors in training braved the frigid waters near Iqaluit to practise abandoning ship. It's something people who want to work on fishing vessels or sealift ships have to learn and mandatory training required by Transport Canada... The class is run by the Nunavut Fisheries and Marine Training Consortium, which trains between 200 and 300 people a year from across the territory. It's the only organization offering marine safety training in the Arctic. CBC News

Not just an earthquake drill, The Great BC Shakeout is a call to be prepared
When the big one hits, local officials hope that Vancouver Islanders will be ready. A massive province wide earthquake drill called The Great BC Shakeout took place today with an estimated 800,000 participants. Nanaimo emergency program manager Karen Lindsay says participating in the drill that was broadcast on 102.3 The Wave and 106.9 The Wolf is important, but in general she hopes people will go over their emergency plans and update their earthquake kits. Nanaimo News Now

Think before calling 911 in quake aftermath, operators plead
Many Metro Vancouver residents remember the night of Dec. 29, 2015, when a magnitude 4.7 earthquake rattled homes, jolted people out of bed and briefly left some wondering if The Big One was about to hit. Operators at E-Comm, the region's 911 dispatcher, certainly remember that night. That's because they were flooded with hundreds of non-emergency calls that tied up their limited and valuable resources, which should be reserved for helping people in dire need... The earthquake was the strongest felt in the region in more than a decade, but despite leaving people understandably concerned, there was virtually no fallout. No one was hurt, and no damage was reported. That won't be the case during The Big One, which is why E-Comm has asked the public to think before calling 911 in the aftermath of that or any other earthquake. CTV News

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

We still don't have the right balance between security and civil rights
An opinion piece by Sukanya Pillay, Executive Director and General Counsel of the Canadian Civil Liberties Association, states "The Liberals campaigned on a promise to fix the "problematic" aspects of Bill C-51 - which passed into law as the Anti-Terrorism Act, 2015 last year - but have yet to close the deal.

As the Oct. 22 two-year anniversary of the tragic shooting of Cpl. Nathan Cirillo looms, concerns regarding the act, and accountability, remain. The government's recently released Green Paper, 'Our Security, Our Rights,' forms the basis for public consultations on Canada's national security framework but does not assuage concerns about the anti-terrorism act. Bill C-22 was also introduced this year to create a parliamentary committee to review national security activities and intelligence in order to fill the Canada's current gap of no parliamentary oversight of national security. But it doesn't go far enough. As such, the potential for rights and accountability failures, and errors, persists and Canada is not safer. The anti-terrorism act included new and secret powers for the Canadian Security Intelligence Service (CSIS) and rampant information-sharing among 17 agencies and more than 100 departments. These and other concerns about the act are exacerbated by accountability failures." Ottawa Citizen

Bill C-51 panelists urge Canadians to take part in national security consultation
Osgoode professor Faisal Bhabha joined a group of panelists at Ryerson University's Centre for Free Expression, or CFE, last Thursday to discuss the impact of Bill C-51 in relation to terrorism, national security and activism. The discussion was largely critical of the bill: Bhabha and his fellow panelists, Tom Henheffer of Canadian Journalists for Free Expression and Sukanya Pillay of the Canadian Civil Liberties Association, all questioned the need for Bill C-51 as well as the legislation's obscurity and effectiveness. Also known as the Anti-terrorism Act of 2015, the bill broadened the rights of government agencies to share personal information more easily in the name of national security... On September 8, 2016, the Liberal government announced a consultation on national security, which is open to public participation until December 1. The panelists, as well as the moderator, James Turk of the CFE, encouraged the audience to participate. Excalibur

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Two years after attack on the Hill - Now we've got security right
An opinion piece by Senator Vern White, a former Ottawa police chief and Durham region chief, states, "Saturday Oct. 22 will mark the two-year anniversary of the lone-wolf attack on a soldier at the National War Memorial and on Parliament Hill. Michael Zehaf-Bibeau shot and killed Cpl. Nathan Cirillo at the memorial, then continued to Parliament... After wrestling with and wounding a security officer at the door, Zehaf-Bibeau proceeded down the centre hall of the building with his rifle, engaging in a firefight with police and security guards who were in pursuit. He was fatally shot multiple times by officers from the parliamentary security detail, RCMP and the Sergeant-at-Arms. These events had a profound impact on Canadians. The impact was made greater by the fact the gunman was able to get within 40 metres of the prime minister, cabinet members and parliamentarians who were meeting in various locations adjacent to the Hall of Honour... Today, the two internal agencies have been combined into one, been given firearms and a single communications capability, and are managed as a single entity. The RCMP now covers the grounds with an extensive force and a level of security that I believe better manages a potential threat, as well as overseeing the new combined internal agency. Any threat to Parliament needs to be met with the level and capability of force that can suppress it quickly. Removing a threat needs to be done at the gates, on the front lawn or at the doors of Parliament and not inside the Hall of Honour. I believe that the security force and RCMP model now in place can and will do that, should such an attempt occur again. Since the attack, the changes that have been implemented on Parliament Hill identify a level of security more in tune with today's reality and threat..." Postmedia Network (Ottawa Citizen)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CBSA arrest five men in three separate cocaine seizures - The drugs were allegedly destined for Alberta
Weighing in at 445.7 pounds, cocaine, seized by Canada Border Services Agency (CBSA) in three separate busts over the last two months, has led to the arrest of five men. According to the CBSA, the first bust took place Sept. 2 in Coutts, when officers conducted a search of a commercial truck as it entered Canada with a load of televisions. During their search of the truck they discovered 60 packages

of cocaine, weighing 69 kilograms, secured in the load of televisions. As a result of the seizure, two men were detained by CBSA for smuggling, under the Customs Act, and RCMP out of Raymond were contacted and asked to attend the port of entry. The following day, the RCMP charged 29-year-old Gurpreet Singh Cheema and 28-year-old Gurpreet Singh with Importing a Controlled Substance and Possession for the Purpose of Trafficking a Controlled Substance under the Controlled Drugs and Substances Act. The two men have already appeared in court and have been released with strict conditions. They're scheduled back in Lethbridge provincial court Oct. 24. Metro News; CBC News; Postmedia Network (Calgary Herald; Calgary Sun)

Broadcast Media / Médias télédiffusés :

Border agents have made the largest ever seizure in the Prairies, intercepting more than 200 kilograms. Five men were arrested and charged. The [unintelligible] is worth $10 million. The drugs were found in three separate raids. (CTV News, 18:45 ET)

Pearson airport presses Ottawa to fix security backlogs
Officials at Pearson International Airport are pressing Ottawa to cough up more funding to ease backlogs at security and customs checkpoints that have left thousands of air travellers fuming. The problem even has the attention of the prime minister's office after Gerald Butts, the principal secretary to Justin Trudeau, took to social media to express his frustration at recent lineups... In a Friday presentation to the Commons' finance committee — which is conducting prebudget hearings — the authority will press Ottawa to invest millions of dollars more to improve security and border services. Scott Collier, the authority's vice president of customer and terminal services, will call for at least $5 million in extra funding for the Canada Border Services Agency, responsible for customs and immigration screening of arriving international passengers, to improve services at Pearson. During May, authority staff were forced to hold passengers outside a jammed customs hall an average of twice a day with wait times topping 30 minutes. The authority is also urging Ottawa to earmark another $20 million to the Canadian Air Transport Security Authority to improve security screening at Pearson alone. This would allow 95 per cent of passengers to be screened in 10 minutes or less. Postmedia Network (Toronto Star)

Akwesasne resident gets three years for human smuggling
Terri Ann Bush, age 43, of Hogansburg and St. Regis, Quebec, Canada, was sentenced Wednesday to 36 months in prison for her role in a human smuggling conspiracy, according to the U.S. Department of Justice. Bush pleaded guilty on June 21. In the evening of Nov. 17, a New York State Police trooper in rural northern New York performed a traffic stop on a southbound vehicle. A male citizen of Israel, Bush, and the driver, also from Hogansburg, told the trooper they were headed from the international border area to New York City... Later, troopers and Border Patrol determined that the Israeli man was known to immigration officials and not lawfully in the United States. The next morning, Border Patrol agents stopped the same vehicle northbound with the Israeli man was absent. After a search, federal agents found and arrested him in Philadelphia. He was brought back to New York for prosecution for illegal entry to the United States from Canada, and later pleaded guilty. The driver from Hogansburg also pled guilty to an alien smuggling charge, Hartunian said. North Country Now

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Cyber security in Canada overdue for an update, experts tell Senate open caucus
Cyber security in Canada needs a major overhaul, one that looks at the problem beyond just the virtual scope; that was the message that panelists delivered at a public open caucus meeting hosted by Senate Liberals this past Wednesday during Cyber Security Awareness Month. "The rate and nature of change requires an evergreen cyber strategy," said Peter Sloly, executive director with Deloitte Canada, who works in the cyber section of the risk advisory services. "There's no point in having one in 2010 and updating it in 2014 or having one in 2016 and then updating it four years later around an election cycle." Sloly, a former deputy chief of the Toronto Police Service, emphasized that like policing, cyber security is more than law enforcement; it requires prevention, engagement, and the protection and promotion of rights. These same elements can, and should, apply to cyber security. Hill Times

"I've seen pretty much all your tech secrets"
Government prosecutors intend to file additional "serious felony charges" against a former NSA contractor who was arrested in August and charged with stealing a massive trove of top-secret intelligence documents. In court papers filed Thursday [you can read them below], the government said Navy veteran Harold T. Martin III stole 50,000 gigabytes of data over the course of two decades, which far exceeds the number of documents Edward Snowden took from the NSA and leaked to journalists. (One gigabyte can store about 10,000 pages.) Prosecutors say Martin, who had been a contractor with Booz Allen Hamilton — the same company that employed Snowden at the time of his leak — is a national security threat and a flight risk, and must remain behind bars until a trial in his case begins next year.... "Some of the documents are marked 'Unclassified/For Official Use Only,' and many are marked 'Secret' and 'Top Secret,'" the court filing says. "Many of the documents marked 'Secret' and 'Top Secret,' also bear special handling caveats. The information stolen by the Defendant also appears to include the personal information of government employees." Vice News

LAW ENFORCEMENT / APPLICATION DE LA LOI

Seizure of fentanyl south of Nanaimo one of the largest in B.C., RCMP say
RCMP are calling a bust near the Nanaimo Airport one of the largest seizures of fentanyl in B.C. in the past few years. Mounties say a suspicious vehicle was pulled over on the highway just south of the airport on Oct. 10 around 5 p.m. Police say the driver, a Vancouver Island man, was arrested and his vehicle was searched. Cash and one kilogram of powdered fentanyl was found, according to RCMP. Police state in a release "this makes the seizure one of the largest for the RCMP in British Columbia over the past few years." "Locating and reducing the importation and distribution of fentanyl continues to be a priority for the RCMP, especially given the number of opioid deaths in British Columbia," states Cpl. Tammy Douglas in the release. The man arrested has been released and no charges have been laid at this point. The Federal Serious and Organized Crime Group on Vancouver Island has taken over the investigation. Nanaimo News Now; CTV News; Canadian Press (Times Colonist); Cowichan Valley Citizen; Global News

Police pull gun, drugs and fake $100 bills out of Saskatoon home
Police in Saskatoon have released more details today about what they found when they executed what they describe as a high risk warrant. Yesterday, police moved in on a home in the 1600 block of Avenue C N. with back-up from their guns and gangs unit and the tactical support unit. A 36-year-old man was arrested. Inside the home, police now reveal that they found a rifle, along with some methamphetamine and marijuana. Police also found a small stack (10) of $100 bills. The man arrested now faces weapon and drug charges along with possession of counterfeit money and breach of undertaking. Police said their investigation is on-going. CBC News

Police seize more drugs in Nunavut's capital
For the second time this month police have seized a large amount of drugs in Iqaluit. On Oct. 12 investigators from the RCMP V Division Federal Operations Section in Iqaluit executed a search warrant and seized cash and drugs from a residence in the city. The search resulted in the seizure of $700 in cash, about a kilogram (more than two pounds) of marijuana, roughly a half a kilogram (one pound) of hashish, and a small amount of cocaine. Two Iqaluit men have been charged in relation to this investigation, police said Oct. 19. Nunatsiaq Online

RCMP investigating 80 arson cases in southeast communities
RCMP have determined 80 fires in southeast New Brunswick have been deliberately set over the past two years. The fires have been in several communities policed by the Richibucto, Bouctouche and Elsipogtog detachments of the RCMP. About half of the fires have been set in abandoned or vacant residences, cottages, trailers and vehicles and have happened at night. RCMP say the remaining fires have involved other structures and properties, including businesses and residences that were inhabited, but not occupied at the time of the fires. No injuries have been reported in the fires. CBC News

A B.C. city is building 'red zones' to banish repeat offenders from its downtown. Can cities really do that?
This week, the Ridge Meadows RCMP announced that they were a mapping out a "red zone" for downtown Maple Ridge, B.C., a suburb east of Vancouver. Covering a roughly 15-block section of the downtown's core known for its high crime, it would be a "designated area" where habitual offenders could be arrested on sight. Or, as the Mounties put it, it would be a "legal tool to arrest a repeat offender who is simply in a geographical area." The National Post called up the experts to get the details on B.C.'s most cinematically named crimefighting tool. Can you really just banish offenders from places?... How does it work?... Why would a city do this?... Does anybody else do this?... Is it legal? Postmedia Network (National Post)

Duo nabbed in diamond-swapping theft, police suspect nationwide spree
Jewellers across the country are being warned to check their stock for fake diamonds after a Toronto-area couple were charged in a daring diamond switch that could be connected to a string of similar heists nationwide. Police in Saint John, N.B., said Grigori Zaharov, 70, and Natalia Feldman, 44, of Vaughan, Ont., were arrested overnight Thursday outside a condo tower in Vaughan. The Saint John force said the couple "are suspects in numerous other jurisdictions for similar incidents," and multiple police agencies are working "to determine the entirety of their actions." CTV News; CBC News

54-year-old Kasabonika Lake man dead after reported altercation
Ontario Provincial Police have charged a 30-year-old man with murder in Kasabonika Lake First Nation after a reported altercation Wednesday morning left another man dead. Police charged George Darren McKay, 30, with second degree murder in the death of Alec Tom McKay, 54... According to police, an officer with the Nishnawbe Aski Police Service responded to a call at a home in the community about a disturbance outside the residence at about 7:00 a.m., CT. Alec McKay was subsequently transported for medical assistance, where he was pronounced dead by medical staff, police said in a press release Thursday. A post-mortem was scheduled in Kenora, Ont. on Thursday... Officers with the OPP and NAPS continue to investigate. Kasabonika Lake is a fly-in community located about 450 km northeast of Sioux Lookout, Ont. CBC News

L'armée doit se concentrer à protéger le Canada selon les conservateurs
L'armée canadienne doit concentrer ses énergies à défendre le Canada et l'Amérique du Nord au détriment de sa participation à des opérations de maintien de la paix de l'ONU, suggère le Parti conservateur dans un mémoire présenté mardi... La volonté des libéraux de renouer avec les opérations de paix des Nations unies nécessitera la mobilisation de quelque 600 militaires canadiens et 450 millions $ sur trois ans. Des policiers de la GRC et de différents corps provinciaux et municipaux seront aussi affectés aux opérations, ainsi que des spécialistes civils. TVA Nouvelles

Drogues, armes véhicules volés... coup de filet payant de la GRC à Kedgwick
Cinq personnes ont été arrêtées dans le cadre d'une enquête sur le trafic de drogue menée à Kedgwick. Deux d'entre elles ont été accusées. Mercredi, des agents du Groupe fédéral des crimes graves et du crime organisé ont exécuté un mandat de perquisition dans une résidence de la région de Kedgwick. La GRC affirme que les policiers ont saisi d'importantes quantités de différentes drogues. Ils auraient entre autres saisi plus de 20 000 comprimés, ainsi que des substances qu'elle croit être de la cocaïne, du haschisch et des champignons hallucinogènes. Acadie Nouvelle

Missing 13-year-old may have travelled to Winnipeg
Police are requesting the public's help in locating a missing girl. St. Pierre-Jolys RCMP say Samantha Gabriel, 13, was last seen last Monday, Oct. 10 in the rural municipality of De Salaberry, Man. Police believe she may have travelled to Winnipeg... Police describe her as an "at-risk youth" and say they are concerned for her wellbeing. CBC News; CTV News

Christopher Garnier heading for 2017 trial in death of Catherine Campbell
Christopher Garnier will go to trial late next year on a charge of second-degree murder in the death of off-duty Truro police officer Catherine Campbell. Dates for a five-week jury trial were set Thursday morning in

Nova Scotia Supreme Court in Halifax. Garnier appeared via videolink from the jail where he is being held. His trial is scheduled to begin on Nov. 20, 2017. CBC News

Why did Canadian police cars become so menacing?
An opinion piece states, "When did our community policing culture shift from one of assistance to perceived intimidation, and where did our honoured, approachable peace officers go? Are we following the footsteps of US police forces, which are armed with riot gear, armoured vehicles and other military-grade equipment? Having built my life as a design professional in the field of visual culture over the past 20 years, I have to ask what purpose is served by the recent shift in police vehicle design in cities across Canada..." National Observer

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Mentally ill inmates don't belong in prison, coroner's inquest hears
A retired social worker who worked with a dying inmate in the Shepody Healing Centre in Dorchester told a coroner's inquest Thursday that mentally ill people should not be in a federal penitentiary. John Lutz was testifying at the inquest into the 2010 death of Glen Edward Wareham, 28, of New Waterford, N.S., who died as a result of complications from extensive self-harm. "A mental health psychiatric facility is where he should be, but the justice system was responsible for putting him there," said Lutz. The Shepody Healing Centre is the Correctional Service of Canada's facility in Atlantic Canada for inmates with mental health issues. Lutz said a mental health psychiatric facility would be a more appropriate setting for inmates like Wareham. "The Shepody Healing Centre, key people are correctional officers," said Lutz. "At a psychiatric facility there are no officers to egg patients on." CBC News

Decision in appeal of Dennis Oland's murder conviction expected Monday
Dennis Oland is expected to learn Monday if he'll continue to serve a life sentence for the murder of his father, win acquittal, or be ordered to stand trial all over again. Defence and Crown lawyers finished presenting arguments before three justices of New Brunswick's Court of Appeal Thursday on whether the guilty verdict delivered by a jury in December should stand or be overturned. Canadian Press (Global News; Chronicle Herald); Radio Canada; CBC News

Edmonton lawyer who smuggled meth into remand centre off to prison after appeal fails
A young lawyer convicted of smuggling drugs into the Edmonton Remand Centre has one week to turn himself in, after his appeal was rejected this week. In September, Justin Sidhu was sentenced to four years in prison for smuggling six grams of methamphetamine into the remand centre. CBC News

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Pill-making machine could produce 6K fentanyl pills an hour: RCMP
Alberta police and politicians are meeting in Sherwood Park, Alta. over the next two days to address how they can work together to combat the dangers of fentanyl. The two-day Fentanyl Conference will look at issues like the risks of fentanyl use, toxicology of the drug and its importation. It will also allow various agencies, such as police, Alberta Health Services (AHS) and Health Canada, to share ideas and discuss case studies... Boechler said fentanyl is the drug of choice because it is easy to obtain online and drug traffickers can easily find it and import it. On Thursday morning, he demonstrated to the media how the illicit drug is made using a pill processing machine, often with counterfeit parts. Boechler said RCMP are concerned because there is no quality control. The pill processing machines can create up to 6,000 tablets an hour. RCMP are currently rolling out a new product in the fight against fentanyl – a nasal naloxone spray. The products cost approximately $150 and Mounties have ordered approximately 13,800 for officers across the country. Global News; Postmedia Network (Edmonton Journal; Edmonton Sun)

Broadcast Media / Médias télédiffusés :

> Provincial and federal officials gathered in Edmonton to confront the fentanyl crisis… This is a two-day conference… Hundreds across Canada attended including police officers, health officials, and politicians. (CTV News, 18:45 ET)

Nova Scotia RCMP given Naloxone kits amid spreading fentanyl crisis
RCMP in Nova Scotia say 25 per cent of members are carrying Naloxone nasal spray kits in an effort to get ahead of a potential rise of the deadly opiate drug, fentanyl, which is rapidly spreading across the country. CTV News

South Surrey crime watchers call on RCMP for better communication
Block Watch captains in the Grandview Heights area of South Surrey say they are frustrated by a lack of communication from police and what they describe as a "one-way flow" of information around crimes occurring in their neighbourhood… According to Surrey RCMP Sgt. Alanna Dunlop, communication with Block Watch captains is among areas under review as part of a City of Surrey reorganization of RCMP volunteers that began in recent weeks. The communication review is "to ensure continued effectiveness of the relationship and the program," Dunlop told Peace Arch News this week after hearing of concerns. Dunlop described the relationship between Surrey RCMP, the City of Surrey and Block Watch volunteers as a good one. The reorganization that's underway, she said, is "to provide more consistency and oversight for the program," which has also seen some changes in personnel. The Now

Drug death toll reaches new peak in B.C. with 555 fatalities in nine months
The number of illicit drug deaths in British Columbia surpassed last year's death toll after just nine months. The Ministry of Public Safety says in the first nine months of this year there were 555 deaths because of illicit drug overdoses, compared with 508 for all of 2015. The ministry says fentanyl remains the major contributor to the high number of deaths and in more than 60 per cent of them, the drug was detected. Globe and Mail; Times Colonist

'They don't want to die': Families who lost loved ones to opiates say government must do more
It's been two years since Arlene Last-Kolb's son Jessie died of a fentanyl overdose, and she says Manitoba's opiate problem has only gotten worse since then. On Thursday, Last-Kolb joined a dozen other people who have lost loved ones to fentanyl and carefentanil to demand the Manitoba government do more to fight the rise of opiates in the province. They were there to support a new NDP private members' resolution demanding the Progressive Conservative government put together an anti-opiate strategy. CBC News

Davantage de fusillades à Ottawa, mais moins de violence attribuable aux gangs de rue
Une mise à jour de la Stratégie d'Ottawa relative aux gangs de rue montre que la violence dans la rue est de moins en moins attribuable aux bandes organisées. Cette Stratégie, qui est coordonnée par une vingtaine d'organismes et de groupes communautaires, a été mise en place il y a trois ans. Dans la mise à jour faite au Comité des services communautaires et de protection de la Ville d'Ottawa, jeudi, les responsables de la Stratégie indiquent qu'il y avait, en 2015, huit bandes de rue en activité, regroupant 435 membres. Mais le rapport souligne un changement dans l'activité criminelle. « Le commerce de la drogue, les infractions relatives aux armes, la violence et le commerce du sexe ne sont plus l'apanage de bandes de rues bien organisées. Actuellement, la violence dans la rue est plutôt attribuable à des individus vaguement reliés », peut-on notamment y lire. Radio Canada

Edmonton police officers say more training needed to interact with Somali-Canadians
Junior officers with the Edmonton Police Service say they are not adequately trained to interact with members of the Somali-Canadian community, according to a report being presented Thursday to the police commission. "The majority of constables, including beat officers, stressed that having more knowledge about the community would significantly help them in their day-to-day interactions," reads the 34-page report, co-authored by Dr. Sandra Bucerius, a criminologist at the University of Alberta. The findings are the result of 57 in-depth interviews with officers of various rank last year in a project approved by Chief Rod Knecht… The report said while some officers described receiving cultural competency training, it was not usually specific to Somali-Canadians. They stressed it would be helpful to receive knowledge before taking on a new beat requiring community interaction… Researchers, who also

interviewed 301 members of the Edmonton Somali community between 16 and 30, said the majority still describe the relationship with police as "difficult." But relations have improved, they stated... One inspector described the shift that has occurred as going from "playing the big bad cop" to a strategy of reaching out to communities and building relationships, not just to solve crimes but to come up with preventive strategies and programs. CBC News

Teen's death points to need for more substance use programs for youth, says watchdog
B.C.'s Representative for Children and Youth is once again calling for a comprehensive system of substance use services, as part of its report into the death of 15 year-old Nick Lang. The report released today says the Métis teenager's parents were unable to access suitable, culturally specific services to help address their youngest son's escalating substance use problem... This is the second time in less than six months that the RCY's office recommended a more comprehensive substance abuse policy. The report released today, Last Resort: One family's tragic struggle to find help for their son, found Nick had increased the use of methamphetamine and was hesitant to accept voluntary treatment. Investigators concluded that Nick may not have ended up in a provincially funded rehabilitation centre if the proper supports had been available when they were needed. The report also recommended that the province, in partnership with Métis leadership,develop and implement a strategic plan to deliver culturally responsive services for Métis. CBC News; Globe and Mail

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Preliminary hearing begins for three arrested in medical marijuana raid
A preliminary hearing began Thursday for three people arrested in a high-profile police raid at a Saskatoon medical marijuana dispensary last year. The dispensary's owner Mark Hauk, alongside the two others, appeared in Saskatoon Provincial Court for the hearing as police officers involved in the raid were questioned on the witness stand. Hauk's defence lawyer said he plans on bringing forward a constitutional challenge of Canada's medical marijuana laws, if a trial is ordered. The medical marijuana dispensary, known as The Saskatchewan Compassion Club, was raided Oct. 29 last year. Several charges initially laid against the accused were dropped in January. The charges related to derivatives like cannabis oil. The three who appeared in court Thursday are still facing charges of possession and trafficking of an illegal substance. The preliminary hearing is scheduled to resume in December, when more officers are expected to be questioned. CTV News

Toronto pot shop owners and employees fined by courts
Employees and owners of six pot shops have been fined by the courts after pleading guilty to Planning Act and Licensing Bylaw charges, the city says. The charges stem from enforcement efforts May 26 by Toronto police and the Municipal Licensing and Standards Division. The courts imposed sentences between $550 for an employee and $2,500 for an owner in addition to closing orders under the City of Toronto Act. The city said a closing order means the property is immediately closed "for any business use involving the sale of any form of edible marijuana foodstuffs intended for human consumption" for up to two years. "Residents, local Business Improvement Areas and other community leaders have been expressing their concern about the illegal storefront marijuana dispensaries over the last number of months," the city said in a news release Thursday, Oct. 20. There are 210 charges currently before the courts. Inside Toronto

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Ottawa breaching Indian residential school settlement agreement: Sen. Murray Sinclair
Ottawa breached the multi-billion dollar Indian residential school settlement agreement by allowing its lawyers to use legalistic tactics to defeat and limit compensation claims from survivors during private hearings, says Sen. Murray Sinclair, who was chair of the Truth and Reconciliation Commission.Sinclair said he doubts many residential school survivors would have agreed to the settlement agreement, which was finalized under the Liberal government of Paul Martin, if they knew federal government lawyers would resort to splitting jurisdictional hairs to disqualify compensation claims under the Independent Assessment Process (IAP) which was created by the settlement agreement. APTN News

Dion leads UN effort to ramp up pressure on Russia, Syria over Aleppo
Foreign Affairs Minister Stephane Dion is at the United Nations in New York to try to ratchet up pressure on Russia and the Syrian government to stop bombing Aleppo and allow in much-needed humanitarian assistance. Dion will call out Russia and Syrian President Bashar Assad by name during a special session of the UN General Assembly organized by Canada and supported by more than 70 other countries.The minister will ask the UN Security Council to break the impasse that has prevented the international community from intervening Syria, where more than 400,000 people have been killed since 2011. He will also remind Russia and Assad of their responsibilities to protect civilians and call for an immediate end to airstrikes against rebel-held parts of Aleppo, and access to humanitarian aid for the estimated 250,000 people trapped in the city. Dion says Canada asked for the special session so countries could express frustration at the current situation in Syria, and to try to put extra pressure on Russia and Syria to end five years of fighting. Canadian Press (CTV News; Winnipeg Free Press)

INTERNATIONAL

NIL

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

RalphGoodale
En souvenir aujourd'hui de l'adjudant Patrice Vincent, victime de terrorisme à Saint-Jean-sur-Richelieu il y a déjà deux ans. #Honneur

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

EComm911_info
NEWS RELEASE: Calling 911 for info during an earthquake puts lives at risk. Learn more: http://ow.ly/aQac305nsWg #911EmergOnly #ShakeOutBC

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

davidakin
#SECU 35 meets now in Sherbrooke, QC: National Security Framework. Link to details: http://bit.ly/1o8816t #cdnpoli

Rob_Oliphant
#Montreal: the #SECU committee is here today for consultations on the #NationalSecurityFramework. #Cdnpoli http://bit.ly/2e0kKpk

PamDamoff
#NationalSecurityFramework hearings continued in Toronto. Thx @TimmyB707 for attending as rep for Oakville + District Labour Council #SECU

JohnBrassardCPC
Back in Ottawa after a day at #secu Committee hearings in Toronto. Amazing # of people upset on broken Liberal promises. #barrie #innisfil

NATIONAL SECURITY / SÉCURITÉ NATIONALE

info_radical
A delegation from the Standing Committee on Public Safety and National Security visited @info_radical #SECU @MattDube @DianneLWatts

MattDube
Une excellente visite au Centre de prévention de la radicalisation menant à la violence (@info_radical) à Montréal avec le comité. #SECU

bobzimmermp
Well done @jamesbezan for recognizing Patrice Vincent & Nathan Cirillo for their ultimate sacrifice 2 years ago today & Oct 22. #RestinPeace

JasonLeopold
My latest: Federal prosecutors say ex-NSA contractor Harold Martin stole 50,000 GB of info dating back to 1996 https://news.vice.com/story/nsa-contractor-stole-10000-gigs-of-data-over-20-years-prosecutors-say?cl=fp ...

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

660NEWS
Authorities make three major drug busts at #Alberta crossing: http://www.660news.com/2016/10/20/authorities-make-three-major-drug-busts-alberta-crossing/ … #CBSA

CanBorderPRA
These September long weekend seizures are the most #cocaine seized in one weekend by #CBSA in #AB. #Coutts #YYC

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

josephfcox
Wow: judge orders FBI to reveal the true extent of its global hacking operation. Wants total number of IP addresses https://www.documentcloud.org/documents/3149220-Order-on-Motion-to-Compel-Tippens.html ...

Safety_Canada
#DYK everyone is vulnerable to #cybercrime. Stay #cybersafe & protect yourself: http://ow.ly/IYxm305n1Hz #CSAM

Securite_Canada
#SVQ Tout le monde est vulnérable au #cybercrime. Soyez #cybersécuritaire et protégez-vous. http://ow.ly/R6u9305n1Qf #CSAM

LAW ENFORCEMENT / APPLICATION DE LA LOI

bcRCMP
It's two tongues for #TongueOutThursday! Tig and his girlfriend Molly, love working in the bush together.

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

WoodfordCHNL
#Breaking latest overdose stats from BC Coroners Service say illicit drug deaths to date now exceed all of 2015. #fentanyl #bcpoli

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

YWCAToronto
#LetsTalkHousing to address the root causes of #MMIW and #poverty in Indigenous and racialized communities. #ActOnHousing #WWV16

ciffic
Media coverage of #MMIW made a difference. Our next talk explores coverage of other #Indigenous issues. #aboriginal https://t.co/Bloiz2ubQY

takentheseries
Tomorrow night at on @APTN on @takentheseries, the story of a beloved 21-years-old Claudette Osborne-Tyo went missing in 2008 #MMIW #MMIWG

Joan_Jack
#MMIW Wondering what the inquiry will really produce? We know what we need now - resources in our communities. https://t.co/sukARIhsrE

WinnipegCP
Support for families of MMIW to increase https://t.co/IUclZPr8P4

PUBLIC SERVICE / FONCTION PUBLIQUE

CBCTheNational
Government has 'much work to do' to meet Oct. 31 Phoenix deadline but falling behind http://www.cbc.ca/1.3810807

OTHER / AUTRES

althiaraj
Jody Wilson-Raybould announces 24 new judicial appointments — and a new system to appoint new judges http://news.gc.ca/web/article-en.do?nid=1140619 …

AngelaSterritt
Ottawa breaching Indian residential school settlement agreement: Sen. Murray Sinclair http://aptn.ca/news/2016/10/20/ottawa-breaching-indian-residential-school-settlement-agreement-sen-murray-sinclair/ … via @APTNNews

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

Today's News / Actualités
October 23, 2016 / le 23 octobre 2016
9:00 - 18:00 ET

This collection contains news items that appeared online between 9:00 a.m. and 6:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 9h00 et 18h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

TOP STORIES / MANCHETTES

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

The storm that wasn't (and the earthquake that will be)
The frustrating news spread quickly among Vancouver Island parents at last weekend's B.C. Taekwando Master's Cup in Burnaby: the ferries were cancelled and we would all have to spend the night on the mainland (...) Onboard the 7 a.m. sailing from Tsawwassen to Swartz Bay the following morning, I laughed at some of those jokes on Twitter, and I confess I did wonder if perhaps BC Ferries had been a bit too cautious in cancelling so many sailings on that route the previous day. But the obvious question is what would have happened if they hadn't cancelled them, especially if the storm had been as big or even bigger than expected? What would have been the public backlash if people's lives had been put in jeopardy? Now that the storm is a week behind us, it might be useful to turn our attention to the much bigger natural disaster that will strike one day and the task of managing the risk beforehand. Of course I'm talking about a major earthquake (...) If the Big One hits British Columbia soon, it seems highly unlikely that the second-guessing after the disaster will bear any resemblance to the response to last weekend's storm. Last weekend, many of us asked if those in charge of public safety did too much. If a major earthquake were to happen next weekend, I'd wager, most of us would ask why they didn't do more. CBC News

Booms fail, diesel fuel spills from tug sunk near Bella Bella B.C. - Heiltsuk Chief Marilyn Slett questions why seaworthy booms were not installed?
The booms containing spilled diesel fuel from a sunken tug 20 kilometres west of Bella Bella have failed in rough weather conditions. A spokeswoman from Kirby Offshore Marine, which owns the tug, says crews are now working to reposition and replace the damaged booms as Gale winds and three-metre waves continue to batter the remote central coast. The spokeswoman says while it is unclear how much fuel has spread into the open water, no oiled wildlife have been detected or captured since the rough weather began Friday. But Heiltsuk Chief Marilyn Slett says her community is in shock of the incident and is questioning why more seaworthy booms weren't installed. Canadian Press (CBC News, Vancouver Sun)

Six months after wildfire, Fort McMurray on long road to recovery
Six months after one of the largest evacuations in Canadian history, no one in Fort McMurray seems to have a clear idea of just how many residents have returned to the fire-ravaged city. The local public school board says attendance was down by 270 students, or about four per cent, as of Sept. 30. Attendance at Catholic schools was down by 400 students this fall, about 6.5 per cent. The Regional Municipality of Wood Buffalo has tried to keep track of how many people have returned. As of Sept. 2, a total of 77,158 residents had registered at information centres in the municipality. But officials say those numbers don't offer a complete or reliable picture, since some may have returned without registering while others may have registered more than once. Despite the lack of firm numbers, there are indications that for some residents things are beginning to return to normal. The Alberta Electric System Operator said power usage dropped off during the evacuation period in early May. CBC News

Earthquake 'swarm' in New Brunswick unlikely to rattle residents: seismologist
A seismologist says a cluster of earthquakes was detected in southern New Brunswick over a two-week period, but it's unlikely residents in the area even felt a tremble. Maurice Lamontagne of Earthquakes Canada says a total of 10 earthquakes occurred around Sussex between Sept. 19 and Oct. 5. Lamontagne says the earthquakes were of such low magnitude -- about 2.3 on the Richter scale -- that people in the sparsely populated area may have heard a rumble, but probably felt nothing beneath their feet. He says the quakes were relatively shallow and focused less than five kilometres beneath the earth's crust. Canadian Press (Chronicle-Herald, CTV News)

Halifax hit with 55 to 80 mm of rain during weekend storm - Cape Breton Regional Municipality saw between 25-35 mm
Cape Bretoners braced for a repeat of the Thanksgiving storm, but for many, the wind and rain over Friday and Saturday didn't quite compare. Rainfall totals in Cape Breton, a region which saw widespread flooding which displaced homeowners on Thanksgiving Monday, averaged about half of what Halifax

County saw in the last 48 hours. The Cape Breton Regional Municipality said Thursday its infrastructure could handle 30 to 40 millimetres of rain, which is about what the area received. CBC News

Power out in many parts of P.E.I.
Power is out some parts of the Island, including Charlottetown. A Maritime Electric spokeswoman said crews are on their way to out to work on getting it restored. A list of communities currently without power is on the Maritime Electric website. CBC News (Yahoo! News); Charlottetown Guardian

Flood victims warned of scavengers in Sydney
Officials with the Cape Breton Regional Municipality are warning flood victims to watch for people scavenging from the water-soaked items they've put out at the curb. John Phalen, public works manager with CBRM, said the municipality has received reports of people rooting through flood victims's damaged belongings that are put out on the street for pick up (…) Phalen said the municipality is trying to discourage "treasure finders," from the practice, which can be common on regular large garbage pick-up days. He said picking through the trash of flood victims can be unsafe. "A lot of these places have had sewage and oil contamination, so there is a health hazard there as well. So stay away from it," said Phalen. "They're having a hard enough time as it is." CBC News

Winds, rain and snow cause power outages and flooding across Quebec
As of noon Sunday, 36,000 homes in Quebec were without electricity, almost half of them in the Montérégie, as strong winds and wet snow caused branches drooping under the weight to come into contact with power lines across the province. Hydro-Quebec said more than 140 of their crews had been deployed to restore power in the Montérégie, but also in the Eastern Townships, Lanaudière, the North of Quebec and Quebec City regions. Heavy winds followed several days of rain that also caused minor flooding in some areas, especially in the Beauce, as several rivers, including the Etchemin, Chaudière, Beaurivage, Famine, Ouelle and Nelson rivers overflowed their banks. Several regions, including Charlevoix, Saguenay-Lac-Saint-Jean, Lanaudière, Laurentides, Mauricie and the Montérégie had received rainfall warnings. The Quebec Public Safety department continued to monitor the situation of other rivers as well, Sunday afternoon. Montreal Gazette

Plusieurs rivières sous surveillance; inondations en Beauce
Les précipitations soutenues des derniers jours ont gonflé des cours d'eau où l'on signale ce matin des inondations mineures, dans les régions de la Beauce et de la Capitale-Nationale. Les niveaux des rivières Chaudière, Beaurivage et Nelson étaient toujours en hausse, ce matin, dans le secteur Saint-Étienne-de-Lauzon à Lévis, à Saint-Joseph-de-Beauce et à dans le secteur Val-Bélair à Québec, où l'on signalait déjà des inondations mineures. Quelques débordements ont aussi été signalés sur la rivière des Hurons, à Stoneham-et-Tewkesbury, et en bordure de la rivière Famine à Saint-Georges, en Beauce. La rivière Chaudière, en particulier, est sous surveillance. Les débits enregistrés à plusieurs endroits montraient des signes préoccupants, alors que de légères précipitations continuent de tomber sur la région. La Presse

Police searching Lake Simcoe for missing man Halai Li - An empty kayak was found floating in the lake on Wednesday
South Simcoe Police, York Regional Police, and the Canadian Coast Guard are searching for Toronto man who may have gone missing on Lake Simcoe over the past week. Halai Li, 57 years old, didn't show up for work on Tuesday, according to South Simcoe Police. Li was known to go fishing, and Monday was his day off. South Simcoe police found Li's car sitting in a marina, and a yellow kayak was found floating in Lake Simcoe on Wednesday. The search for Li began Friday, and continued Saturday before pausing overnight. Police resumed the search Sunday morning, and are asking residents along Lake Simcoe to check the nearby shoreline. CBC News

Barge to chill on Toker Point
A fuel barge that ran aground north of Tuktoyaktuk on Sept. 2 will spend the winter where it sits on Toker Point, said Tuktoyaktuk mayor Darrel Nasogaluak. Attempts to free the Fathom Marine barge were unsuccessful, so the vessel is now being prepared to spend the winter on the beach about 25 kilometres north of Tuktoyaktuk (…) Plans to remove fuel from the barge were originally scheduled to begin the

week of Oct. 5, but were delayed. On Oct. 20, fuel was being removed from the barge and brought to Tuktoyaktuk via helicopter, Nasogaluak said. The Canadian Coast Guard could look at establishing a maritime rescue sub-centre in the Arctic. "As we move around the Arctic and talk to people, it could be something we look at," said Peter Garapick, search and rescue superintendent for the central and Arctic region. "Could it be that there is a need for a marine rescue sub-centre in the Arctic? It's a possible question, something that we're open-minded to and we'll ask questions and evaluate the benefits of that." Nunavut News North

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Private Eyes
It was a powerful piece of technology created for an important customer. The Medusa system, named after the mythical Greek monster with snakes instead of hair, had one main purpose: to vacuum up vast quantities of internet data at an astonishing speed. The technology was designed by Endace, a little-known New Zealand company. And the important customer was the British electronic eavesdropping agency, Government Communications Headquarters, or GCHQ. The leaked files, which were provided by a source through SecureDrop, show that Endace listed a Moroccan security agency implicated in torture as one of its customers. They also indicate that the company sold its surveillance gear to more than half a dozen other government agencies, including in the United States, Israel, Denmark, Australia, Canada, Spain, and India. Some of Endace's largest sales in recent years, however, were to the United Kingdom's GCHQ, which purchased a variety of "data acquisition" systems and "probes" that it used to covertly monitor internet traffic. Documents from the National Security Agency whistleblower Edward Snowden, previously disclosed by The Intercept, have shown how GCHQ dramatically expanded its online surveillance between 2009 and 2012. The newly obtained Endace documents add to those revelations, shining light for the first time on the vital role played by the private sector in enabling the spying. The Intercept

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

NIL

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Chinese firm acknowledges inadvertent role in cyberattack
The hazard of having so many household devices connected to the internet is even more obvious after Friday's cyberattack. A Chinese firm that makes components for surveillance video cameras now admits their technology was used, in part, to carry out the unprecedented strike. XiongMai Technologies acknowledged that a piece of malware known as "Mirai" that's spreading around the internet targets vulnerabilities in their products. "Mirai is a huge disaster for the 'Internet of Things,'" XiongMai representative Cooper Wang told CNNMoney in an email. "[We] have to admit that our products also suffered from hackers' break-in and illegal use." It appears hundreds of thousands of internet-connected devices, such as security cameras and DVRs, were used without their owners' knowledge to help leverage Friday's attack, according to security firm Flashpoint. XiongMai acknowledged that the weaknesses in their products were identified last year and hackers continue to exploit them. Users were unable to change the default password on their devices, which allowed hackers to install malware and commandeer them for the DDoS attack. CNN

Cyber warfare: The new international warfront
To enter the Arizona Cyber Warfare range (AZCWR), a person must have a signed waiver, the consent from the strict private security firm that guards the facilities, and the fortitude to withstand the salty language and messy environment created by the hackers inside. "This is the only place in the world where the good guys can learn to hack from good guys who really know how to hack," Brett Scott, one of the founders of the AZCWR, told Al Jazeera inside their hacking headquarters (...) In the US, Scott explained, hackers still face witch-hunts and harsh penalties when the government should offer employment. AZCWR is there to force decision-makers to re-evaluate their stance on technologically-capable but legally questionable computer users. "World War III is already here, and it's happening on the internet," the hacker said. While the assertion that WWIII is happening on the internet sounds hyperbolic, there are those in the US government who agree with the sentiment. Al Jazeera

LAW ENFORCEMENT / APPLICATION DE LA LOI

Creep Catcher vigilantes accused of threatening women who question group's tactics
A Red Deer, Alta., woman says she fears for her safety since going to police with allegations that a member of the Creep Catcher vigilante group planned to use a 14-year-old girl to bait and trap a suspected predator (...) Red Deer RCMP confirm they received a report from the woman relating to a missing girl but say they have no ongoing investigations concerning the complainant, the girl or the vigilantes. "This is not work that should be done by amateurs," Cpl. Karyn Kay said. "They don't have the skills or training, they may damage ongoing police investigations, and they certainly don't follow privacy legislation or due process." Chinksi denies he ever intended to put the girl in contact with the alleged predator. He said he only planned to ask the teen if the man knew her real age and to confront him if she said yes (...) Since she went to police and voiced her concerns on Facebook, the Red Deer woman said she's received threatening voice messages from the group's Calgary-based founder, Dawson Raymond. CBC News

Muskrat Falls protesters 'fighting for land and food'
Protesters who broke through a gate and entered the Muskrat Falls work site in central Labrador Saturday night say they were proud to make their voices heard (...) Adam Pardy attended the protest with his daughters and said it was a bit cold but he too was proud to protest. He arrived just before the road closed. On Saturday, RCMP closed Route 510, the Trans-Labrador highway, in response to the protests. "I think it's completely against the law, what they're doing," Pardy said. "They can't just block the road and not let people through for a peaceful protest." The RCMP reopened Route 510 Sunday morning to traffic both north and southbound. Police also asked motorists to continue to drive with caution as some pedestrians may be near the highway. CBC News; APTN

RCMP on scene by Red River in East Selkirk
For a second day, Manitoba RCMP officers are stationed at a scene by the Red River in East Selkirk. On Saturday, a reporter with the Selkirk captured a photo of an officer carrying a cardboard box and officer wearing thin purple gloves. RCMP have been on scene at the end of CIL Road near the Manitoba Hydro

Plant since 1:30 p.m Saturday. Police tape surrounds trees and an RCMP van, and another vehicle. CTV News; CBC News; AM640

Suspect arrested after woman stabbed on Kawakatoose First Nation
Punnichy RCMP have arrested 20-year-old Kayla Blueeyes, who was wanted in relation to a stabbing on the Kawakatoose First Nation. Emergency crews were called to a home on the First Nation around 11:30 p.m. on Friday. A 30-year-old woman was taken to the Royal University Hospital in Saskatoon by STARS Air Ambulance with serious injuries, RCMP said in a media release. CTV News; Global News

Possible human remains found in Abbotsford, IHIT taking over case
The Integrated Homicide Investigation Team (IHIT) has taken over a case where human remains were found on a rural Abbotsford B.C. property Oct. 22. A resident found the remains at around 2 p.m. PT Saturday on Downes Road near Mt. Lehman Road. Police say officers, major crime detectives and forensic identification members along with the B.C. Coroners Service are on the scene and are still in the early stages of the investigation. CBC News

Police officer charged racist comments posted online
Ottawa police have confirmed they have charged one of their own after accusations were made of racism after online comments were made following the death of acclaimed Inuit artist Annie Pootoogook. Sgt. Chris Hrnchiar has been charged with two counts of discreditable conduct under the Police Services Act. An internal investigation was launched after a comment on the Citizen's story about Pootoogook's death on Sept. 19 seemed to blame Indigenous people for their own hardships: "Because much of the aboriginal population in Canada is just satisfied being alcohol or drug abusers, living in poor conditions etc. (...) they have to have the will to change, it's not society's fault." Several members of Indigenous communities and other rights groups expressed outrage at these comments, reigniting accusations of racism in the force. "I have no evidence to indicate we have racist officers," Bordeleau said at the time, while condemning the comments. Hrnchiak is expected to make his first appearance to face the charges on Nov. 1, said Police Chief Charles Bordeleau. Ottawa Citizen; APTN; Metro News

No trust in Ottawa Police: Okalik calls on Justice minister to find new reviewers for incidents involving RCMP
When a police force struggles with racism toward Inuit, is it the right one to be conducting independent reviews of incidents that involve Nunavut's RCMP officers? That's what former Justice minister and Iqaluit-Sinaa MLA Paul Okalik's wanted to know at the legislative assembly Oct. 18. "The tragic death in Ottawa of Annie Pootoogook has called into question the attitudes of the Ottawa Police Service towards Inuit and other indigenous Canadians given what we have learned about the investigation into racist comments made by at least one senior member of the force," said Okalik. "Given this situation, it is obvious that the Ottawa Police Service can no longer be trusted to undertake independent and objective investigations into incidents that occur here in Nunavut," he said. "Why has the minister not said anything publicly about this serious situation?" Peterson said he understood "there is a bit of an investigation going on." Nunavut News North

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

NIL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

More funding needed to help curb family violence: Lynn Moore
A prominent St. John's defence lawyer says more funding needs to be provided at the federal and provincial levels to help curb family violence. Lynn Moore's recommendations come on the heels of a report from Canada's Chief Public Health Officer that identified family violence as a major health issue. In Dr. Greg Taylor's 2016 report on the state of public health, he spoke of the "staggering" statistics

surrounding family violence, He said that population surveys tell us that one third of the population, or 9 million people, have reported experiencing abuse before they were 15 years old (…) According to Moore, preventing family violence should be one of the government's main goals. "It most definitely is a public issue, it's a safety issue, and it's really a law and order issue," she said. CBC News

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Veterans allowed too much pot, says former NDP MP Peter Stoffer
Former NDP MP Peter Stoffer agrees that medical cannabis can have benefits for veterans, but says he's worried about the amount of cannabis former soldiers are allowed under Veterans Affairs Canada rules. Stoffer, who was veterans affairs critic for the NDP until he was defeated in the 2015 election, believes that the high level of medical marijuana allowed by Veterans Affairs — up to 10 grams a day — is fostering overuse. "Ten grams a day is an awful lot of marijuana to give one person. It is an incredible amount." Stoffer is now public affairs advocate for Trauma Healing Centres, a company that works with veterans, first responders and others dealing with trauma and chronic pain. While he says cannabis can help veterans who are suffering, he says the goal is to help manage their pain, not to get them high (…) Veterans Affairs doesn't actually give veterans medical marijuana, but the department allows them to be compensated for up to 10 grams a day through insurance. Veterans Affairs Minister Kent Hehr said back in March that he was launching an internal review of medical marijuana policy, after data showed the number of prescriptions had increased tenfold in two years. The results of that review will be released "in the coming weeks," Veterans Affairs Canada spokeswoman Sarah McMaster told CBC News. CBC News

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

NIL

INTERNATIONAL

Where Are Women in F.B.I.'s Top Ranks?
When the call came in that a bomb had exploded in Manhattan, Amy Hess quickly got to work.
She helped direct teams of F.B.I. agents to New York to collect evidence, set up secure command posts in the streets so agents could discuss classified information, and alerted the digital forensics, fingerprint and facial recognition experts she manages in Quantico, Va., site of the F.B.I. academy and its lab. By the next day, she and her team had played a crucial role in identifying Ahmad Khan Rahami, the man charged with planting the bomb in Chelsea along with a second, unexploded device. "We pulled out all the stops," said Ms. Hess, who as head of the bureau's science and technology branch oversees more than 6,000 F.B.I. employees. Inside the F.B.I., women in particular look up to Ms. Hess, and not just because they have nicknamed her the "rocket scientist" with a degree in aeronautical and astronautical engineering from Purdue University. She is also the first woman to head the science branch — one of few female agents commanding such an important job at the F.B.I., a clubby agency where men are more

predominant in senior positions than they were even three years ago. Ms. Hess, 50, put it simply: "There is a lack of women in leadership roles (...)" James B. Comey, the F.B.I. director, has described the lack of women — and also minorities — in the F.B.I. as a serious problem that can undermine investigations and keep the agency out of touch with the communities it serves. New York Times

Two Police Killed, 19 People Wounded in Bomb in East Turkey: Sources
Two police officers were killed and 19 people were wounded when a car bomb exploded near a passing police vehicle in the eastern Turkish province of Bingol on Sunday, security sources said.
The bomb, planted by militants from the outlawed Kurdistan Workers Party (PKK), was detonated near the district governor's office, the security sources said. Five police officers were among the injured, they said. Reuters (New York Times)

83 Nigerian soldiers missing after Boko Haram attack
Senior military officers say 83 soldiers are missing after Boko Haram Islamic extremists attacked a remote base in northeastern Nigeria. Officers said the soldiers were unable to fight back because they were poorly equipped. They spoke on condition of anonymity because they are not authorized to give information to reporters. Associated Press (CBC News)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

connie_walker
BREAKING: Booms fail, diesel fuel spills from tug sunk near Bella Bella B.C. https://t.co/WK6Ws2qLMS

The Vancouver Sun
Storms hamper attempt to clean up, contain fuel spill off B.C. coast

GgNewsCA
Halifax hit with 55 to 80 mm of rain during weekend storm - CBC.ca https://t.co/QJRbwZa2Pw

GgNewsCA
Power out in many parts of P.E.I. https://t.co/rqMH5j2phj

CBCCanada
'Who wants this?': Fort McMurray residents struggle to recover 6 months after the fire http://ift.tt/2el1Rk3

CBCAlerts
Local and regional police, Canadian Coast Guard searching for Toronto man missing on Lake Simcoe over the past week: https://t.co/8EadqKqRnB

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Stewart Bell
The Prime MInister's itinerary on the 2nd anniversary of the Ottawa terrorist attack.

Toronto Star
Countering Daesh propaganda, and skeptics at home http://on.thestar.com/2dAoRW6 @shephardm

Colinfreeze
Terrorism investigations tax RCMP's ability to fight Canada's organized crime /via @globeandmail
https://t.co/oMnuK99J6G

OttawaCitizen
Remembering Oct. 22: Could a shooter make it past today's 'armed to the teeth' Hill security?
http://bit.ly/2evchgR #ottnews

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

cyblesoleil
Un site de la diplomatie russe piratée, un hacker américain revendique https://t.co/v23qYw5FAz

SCMagazine
Election misdirection: Scammers exploiting presidential race with malware, spam and bots https://t.co/jtZEWgzduo

cnni
Chinese firm acknowledges inadvertent role in cyberattack http://cnn.it/2ekxCHM

LAW ENFORCEMENT / APPLICATION DE LA LOI

APTN National News
"We had to take drastic measures. Myself and 3 others are now on a hunger strike." #MuskratFalls – Watch more here: https://goo.gl/qRr7wu

Elyse Skura
Workers leave Muskrat Falls site as protesters remain, via @LukasWallCBC http://www.cbc.ca/1.3817947 #inuit #nunatsiavut

GgNewsCA
Protesters break into Muskrat Falls hydroelectric site, form blockade outside - The Globe and Mail https://t.co/ZLRpvZibRx

CBCAlerts
Water levels in area of Muskrat Falls hydroelectric site will remain unchanged until after Tuesday meeting between NL premier & protesters.

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

The Vancouver Sun
Fentanyl front lines: First responders going from 'call to call to call'

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

globalnews
Marijuana will be the great unifier of polarized U.S.: Jesse Ventura https://t.co/K7p0uyNSWA

PUBLIC SERVICE / FONCTION PUBLIQUE

OttawaCitizen
Move over, Boomers: Trudeau shakes up PS top ranks with more young blood http://bit.ly/2eahLtP #cdnpoli

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

Today's News / Actualités
October 31, 2016 / le 31 octobre 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 9:00 a.m. and 6:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 9h00 et 18h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Montreal Cops Have Tracked a Journalist's Cellphone for the Past Year
Montreal police, investigating the possibility of crooked cops on the force, obtained warrants to surveil a journalist's iPhone, and even obtained permission to use his GPS chip to track his whereabouts at all time. But the **federal minister of public safety, Ralph Goodale, stopped short of discouraging police forces from going to the courts to obtain judicial orders against journalists**. Asked directly by NDP Member of Parliament Matthew Dubé on Monday about whether he'll issue a directive to create more formal rules around how police deal with journalists, **Goodale would only say that *"we take the***

freedom of the press in this country very, very seriously." Dubé raised the question after on Monday after Montreal newspaper La Presse published details on surveillances warrants, at least 24 in total, obtained to surveil journalist Patrick Lagacé. The MP also referenced another case, where federal police are working to obtain chat records from a VICE journalist's cell phone, as evidence that action needs to be taken. Vice News

SPVM: le ministre Coiteux est surpris par une procédure contre un journaliste
Le ministre de la Sécurité publique, Martin Coiteux, a exprimé sa surprise, lundi, en apprenant que la police a surveillé les appels téléphoniques d'un journaliste. M. Coiteux a entamé des vérifications pour établir si les procédures ont été respectées par le Service de police de la ville de Montréal (SPVM). «J'ai été très surpris et c'est pour ça qu'on fait des vérifications», a-t-il dit. La ministre de la Justice, Stéphanie Vallée, effectuera également une évaluation des procédures qui ont mené un tribunal à accorder à plusieurs reprises un mandat au SPVM, cette année… À Ottawa, **le ministre de la Sécurité publique, Ralph Goodale, a affirmé que la situation est toujours délicate quand le journalisme et les enquêtes policières se rencontrent. *«Il s'agit d'un cas qui relève des compétences provinciales, mais la position fédérale est d'affirmer que la liberté de presse est une valeur canadienne fondamentale»,* a-t-il dit.** La Presse Canadienne (L'actualité)

Affaire Lagacé : Goodale prêt pour «une discussion sérieuse» sur les règles policières
À la lumière de l'affaire Patrick Lagacé, **le ministre fédéral de la Sécurité publique Ralph Goodale se dit *« certainement prêt à avoir une discussion de politique sérieuse »* et *« à entendre les représentations »* des médias sur la façon dont les forces policières devraient concilier leurs enquêtes avec la protection des sources journalistiques et la liberté de presse. Le ministre Goodale, qui n'a pas voulu commenter le cas de Patrick Lagacé mais qui se dit *« profondément préoccupé par ce genre de dossier »,* s'assurera prochainement auprès du commissaire de la GRC Bob Paulson que les directives fédérales en vigueur sont respectées dans les faits.** Depuis 2003, une directive ministérielle demande aux forces policières de porter une « attention spéciale » au statut des médias dans le cadre d'enquêtes sur la sécurité nationale. ***« Au regard de ce dossier au Québec, qui est sous juridiction provinciale, c'est une question qui doit être posée [à la GRC]. Je n'ai pas encore eu l'occasion de le faire [hier], mais je le ferai [prochainement]. C'est une question juste de demander [à la GRC] de s'assurer que la directive ministérielle qui requiert un très haut standard soit appliquée dans les faits »,* dit le ministre Goodale en entrevue à La Presse. Le ministre Goodale, qui croit que la liberté de presse est *« une valeur fondamentale »* au Canada, n'a pas voulu s'avancer à savoir si des changements législatifs sont nécessaires afin de protéger la liberté de presse dans le cadre d'enquêtes policières. *« Nous devons traiter de cet enjeu sérieusement et je suis certainement prêt à entendre les représentations [des médias et d'associations de journalistes comme la FPJQ] sur ce qui pourrait être un meilleur ensemble de règles »,* dit le ministre Goodale…** La Sûreté du Québec a saisi en septembre l'ordinateur d'un journaliste du Journal de Montréal à la demande du Conseil de la magistrature en rapport avec un dossier traité par le conseil. **Le ministre Goodale, qui n'a pas voulu commenter sur ces cas précis, fait valoir que *« les cas vont suivre leur cours pour voir s'ils respectent les critères de la Cour suprême »* en matière de protection du matériel et des sources journalistiques.** La Presse

Liberals rapped as $900M unspent by Indigenous Affairs among 'lapsed' funding for fiscal 2016
Like the Harper government before it, the Trudeau government left billions of dollars unspent on everything from national parks to veterans services to economic development grants during the 2015-16 fiscal year. The so-called "lapsed" funding for fiscal 2016 is $9.7 billion, according to the Public Accounts of Canada. All of those unspent funds were used to pay down the federal debt. ublic Safety Canada, which includes the RCMP, the Correctional Service of Canada, and Canada Border Services Agency, was authorized to spend $9.2 billion in fiscal 2016 but left unspent 11.6 per cent of that — about $1 billion. **Scott Bardsley, press secretary to Public Safety Minister Ralph Goodale,** said the lion's share of the lapse — about $700 million — was related to disaster relief for the provinces that, while booked by the federal government in 2016, was not paid out. National Post

TOP STORIES / MANCHETTES

Pepper spray use with little accountability concerns prison watchdog
Canada's prison watchdog is raising red flags about the "go-to" use of pepper spray in federal penitentiaries, which his office found has tripled in a five-year period with little accountability. In his annual report tabled in Parliament Monday, Correctional Investigator Howard Sapers said pepper spray was used in 60 per cent of the 1,833 use-of-force incidents in 2015-2016. "The link between institutional safety and the increasing use and reliance on inflammatory agents is tenuous at best," said Sapers. The correctional investigator partly blamed the increase on a policy change back in September 2010 that allowed correctional officers to carry pepper spray canisters on their belts. Before then the chemical, which makes it hard to breath and see, was locked up. His report notes that there hasn't been a correlating increase in the severity of security incidents or threats to justify the increased use pepper spray. Sapers also called out what he termed a lack of monitoring and national oversight of how pepper spray is stored, weighed, inspected, assigned and controlled. CBC News; La Presse Canadienne (L'actualité)

The Number of Female Indigenous Prisoners in Canada Has Doubled in the Last Decade
The number of Indigenous people now represent more than a quarter of all inmates held in Canada's federal prisons, according to the new annual report from Canada's prison watchdog. And within the last decade, the number of female Indigenous inmates has doubled, while the population of male Indigenous inmates has increased by more than 50 percent. During that time, the federal inmate population increased by only 10 percent. "It's a shameful milestone in Canadian history," correctional investigator Howard Sapers told a press conference on Monday. His annual report, which also says Indigenous women represent 35 percent of inmates in federal prisons, serves to highlight his concerns about federal correctional facilities, which house offenders who have been sentenced to more than two years in prison... In addition to decrying the increase in Indigenous offenders, his report also sounds the alarm over a dramatic increase in guards using "inflammatory agents" such as pepper spray against inmates. The number of incidents involving the use of pepper spray against inmates has more than tripled since 2011, and more than one-third of those incidents involved inmates suffering from mental illnesses. Vice News

La Presse says Montreal police tracked journalist's iPhone for months
A Montreal journalist says he was furious when he learned that city police monitored his iPhone for months in order to find out who he was speaking with... The French-language newspaper reported it has learned at least 24 surveillance warrants were issued for Lagace's phone this year at the request of the police's special investigations unit. That section is responsible for looking into crime within the police force. Three of those warrants reportedly authorized police to get the phone numbers for all Lagace's incoming and outgoing texts and calls, while another allowed them to track the phone's location via its GPS chip. Lagace said police told him they obtained the court-issued warrants because they believed the target of one of their investigations was feeding him information. But he said the story in question was actually first reported on by a competitor, leading him to believe the investigation was actually a thinly veiled attempt to learn the identity of his sources within the police department... Reaction to La Presse's story was swift, with some unions and media organizations denouncing the police operation, and some opposition city councillors calling for Montreal's police chief to step aside while the matter is investigated. Canadian Press (Globe and Mail; CTV News; Herald News; Metro News); Montreal Gazette; Postmedia Network (Toronto Star)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fort McMurray fire first responders honoured in Alberta legislature ceremony
Premier Rachel Notley and her government paid tribute Monday to those who came to Alberta's aid and rescue during the spring's devastating Fort McMurray wildfire. Notley said the fire devastated the lives of thousands of people but failed to cripple their spirit or resolve. Individuals representing nine first-responder agencies were recognized in a ceremony in the rotunda of the Alberta legislature... One of the recipients, Wood Buffalo fire Chief Darby Allen, said people are strong, but are still struggling with the

memories and reminders of the devastation. Canadian Press (Times Colonist; Winnipeg Free Press); CBC News; Fort McMurray Today

Canada not ready for catastrophic effects of climate change, report warns
Canada is not prepared to handle the devastating and costly effects of increased flooding and extreme weather brought on by climate change, according to a new report released Monday. The report from the University of Waterloo's Intact Centre on Climate Adaptation found governments at all levels across the country need to take immediate action to make the country's infrastructure – highways, railways and water supply systems- more resilient or face increasingly catastrophic financial loses in the future. "The country as a whole is not prepared for climate change, extreme weather events, with a primary focus on flooding," said Blair Feltmate, head of the Intact Centre on Climate Adaptation. "There was no particular province that was disproportionately good or bad compared to the other." CHML Hamilton

Alberta legislation aims to reduce human-caused wildfires
The Alberta government tabled legislation Monday that aims to reduce the number of human-caused wildfires in the province. Over the past five years, about 70 per cent of the wildfires in Alberta have been linked to human activity. The province said Bill 24, the Forest and Prairie Protection Amendment Act, will also enhance firefighting operations. Global News

Hunter and stepson reported overdue
Search and rescue teams have been called out to look for a 55-year-old man and his stepson, reported overdue Sunday from a hunting trip northeast of Quesnel. Glen Brooker and the 10-year-old, whose name was not provided, were to have ton into the area of Stoney Lake or Narrow Lake on Sunday and did not return home that night as planned. Prince George Citizen; CBC News

Arctic survival tips from a search and rescue volunteer
With the sea ice beginning to form and more people heading out on the land, the Civil Air Search and Rescue Association (CASARA) wants to remind people about the skills, safety techniques and tools you need to ensure you survive if stranded in the wilderness. CASARA is a national volunteer organization funded by the Department of National Defence that provides air search assistance to the Royal Canadian Air Force and promotes flight safety. CBC News

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Ottawa terror suspect granted bail again after allegedly breaching conditions
An Ottawa terror suspect has been released from custody after he was charged with breaching some of his bail conditions while awaiting the outcome of his case. The RCMP arrested Tevis Gonyou-McLean in August on a terrorism peace bond for his alleged support of ISIL and was later granted bail on several conditions that included wearing a GPS monitoring device on his ankle and a ban on possessing any terrorist logos. On Oct. 25, the 24-year-old was arrested again after police allege he failed to report to the John Howard Society's bail supervisory program and reside at his pre-approved address, and that he damaged his ankle bracelet, thereby allegedly committing mischief. But his Ottawa lawyer, Biagio Del Greco, said the breaches were the result of a "miscommunication" and said the damage to the bracelet occurred while his client was in police custody and was unintentional. None of the breaches were related to alleged terrorist activity. Ottawa Citizen

Quebec hosts UNESCO conference on prevention of radicalization of young people
Quebec is hosting an important conference on the links between radicalization and the Internet. A UNESCO conference called "Youth and the Internet: Fighting Radicalization and Extremism" is taking place in Quebec City. It started Sunday night and continues until Tuesday. Global News

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Mammoth fine for importing woolly mammoth tusk
Border agents at the Ambassador Bridge fined two Canadians for under-reporting the value of antiques, which included a woolly mammoth tusk. Two Canadians returning from the U.S. in September brought along a haul of antiques, including the woolly mammoth tusk, according to Canada Border Services Agency. The two travellers reported the goods cost an estimated $760, but further estimates revealed the items were valued at $6,100. Border officials issued a $3,317 penalty for under-reporting the value. The items were eventually released to the owners. CBC News; Postmedia Network (Windsor Star)

Ottawa man gets 43-month sentence for forging immigration documents
An Ottawa man who forged documents to allow hundreds of immigrants to enter Canada has been sentenced to three-and-a-half years behind bars. Mohamed Farah Abdulle, 54, was sentenced Monday after being convicted last November on five charges relating to the immigration fraud scheme, according to a statement from the Canada Border Services Agency (CBSA). According to the CBSA, Abdulle had filed more than 170 fraudulent sponsorship applications for 528 people, all while collecting fees from the applicants for his services. CBC News

Border post in automated experiment
The border crossing at Morses Line is a tiny operation that's gone high tech to handle the traffic in slow periods. Described as a "sleepy border crossing" with few than 60 vehicles a day, there was a proposal at one point to close it down. Now the Canada Border Services Agency (CBSA) is testing new technology that could be the standard for border control at small and remote crossings across the country. But critics say the experiment is a threat to public safety. Radio Canada

John McCallum sets new base immigration target at 300,000 a year
The Liberal government is boosting the base number for immigrants to Canada to 300,000 to help drive economic growth as the country grapples with an aging demographic... McCallum said the new annual target will be set at 300,000. The target from 2011-2015 was 260,000 which increased to 300,000 in 2016 to account for the influx of Syrian refugees... More than half the 2016 total, 160,600, are in the economic category for skilled workers, business people and caregivers; 80,000 are in the family program for spouses, children, parents and grandparents; 55,800 are refugees and protected persons and another 3,600 are in the humanitarian category. CBC News

Law enforcement agencies around the world collaborate on international Darknet marketplace enforcement operation
A globally coordinated law enforcement action against the buyers and sellers of illicit drugs and other illegal activities using Darknet global marketplaces was conducted Oct. 22 to 28. "Operation Hyperion" was initiated by U.S. federal law enforcement, the Five Eyes Law Enforcement Group (Australia, Canada, New Zealand, the United Kingdom and the United States) and members of Europol, the European Union's law enforcement agency, as the first step in developing a more unified global law enforcement response to the growing usage of the Darknet by individuals seeking to buy and sell illicit drugs and other illegal goods and services... Operation Hyperion resulted in a number of law enforcement leads on cases related to the buying and selling of illicit drugs and other goods on the Darknet. This operation will also help law enforcement agencies continue to combat the trafficking of illicit goods and services on the Darknet through the identification of new smuggling networks and trends... International partners included Europol the United Kingdom's National Crime Agency; Australian Federal Police; New Zealand Police and New Zealand Customs Service; Canada's Royal Canadian Mounted Police, Canada Post and Canada Border Services Agency; The Netherlands; French Customs National Intelligence and Investigations Directorate; Finnish Customs; Swedish Police Authority and Swedish Customs; Ireland's

Garda National Drugs & Organised Crime Bureau; and Spain's Guardia Civil. U.S. Immigration and Customs Enforcement

Peace Bridge to close one lane for construction
As long as U.S. and Canada customs have the necessary staff available and suitable number of inspection lanes open, any traffic impacts related to the temporary closure of one lane on the Peace Bridge can be mitigated, according to the agency that owns and operates the international border crossing. The Peace Bridge will be reduced to two lanes between Nov. 15 and May 15 for an ongoing $100-million rehabilitation. Fort Erie Times

Liberals in denial about Monsef story
An opinion pieces states, "A file within the federal government has been opened to investigate Democratic Institutions Minister Maryam Monsef for citizenship fraud. And the Liberal government seems to be in denial about it. The Sun exclusively reported that a file was opened to investigate Monsef, who claims she only recently learned she was born in Iran, not Afghanistan. A number of complaints were received through a tip line created by Canada Border Service Agency (CBSA) and the Department of Immigration, Refugees and Citizenship Canada (IRCC), leading to an investigation. It remains unknown whether Monsef's proper birthplace information was included on her original refugee and citizenship application..." Postmedia Network (Toronto Sun)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Old Android malware still circulating, Apple patches Windows apps - Security news IT leaders need to know
This week's highlights also include a fake Microsoft security installer and 247 Oracle patches being issued. Apple has released Xcode 8.1 to address multiple security issues that could allow a remote attacker to be able to cause unexpected application termination or arbitrary code execution. iCloud for Windows 6.0.1 corrects two security flaws that could result in disclosure of user information or arbitrary code execution. Finally, the same two flaws are corrected in iTunes for Windows 12.5.2. National Post

LAW ENFORCEMENT / APPLICATION DE LA LOI

RCMP not to blame for death of suspect who shot Golden Mountie: Police watchdog
The suspect who led police on a manhunt after shooting a Mountie near Golden died from head trauma and RCMP action or inaction was not to blame, B.C.'s police watchdog says. The provincial Independent Investigations Office launched a probe to determine whether there was any connection between the officers' actions and the death of Sheldon Kyle Thunderblanket, 40. Investigators concluded "there is no causal connection between death of the male affected person and actions or inactions of police," according to a Independent Investigations Office media release. Info News

RCMP nab 10 men for prostitution-related offences in Moncton
The Codiac RCMP arrested 10 men, aged 25 to 80, for attempting to obtain sexual services in Moncton in two separate busts earlier in October. The RCMP carried out two police operations Oct. 14 and 27 in the area of Dufferin Street targeting individuals attempting to buy services from sex trade workers. CBC News; CTV News

'We are seniors, why you hit me and my wife?': Elderly couple speak out about RCMP arrest
The elderly couple caught on camera being violently arrested by Coquitlam RCMP last week is speaking out. The incident happened on the evening of Oct. 26 after police were called to a strata meeting that allegedly got out of control. The video, which was posted on YouTube, appears to show an officer dragging a man down a staircase while another officer arrests a woman, who appears to fall at one point... Myung Ju Lee and his wife, Kap Su Lee, told Global News they spent the night in the hospital after ending up with bruises, cuts and scrapes as a result of the incident. "[The police] walked up and did not say anything. Just walked up and grabbed us," Myung Ju Lee said. Lee claims the strata meeting was

not over and there had been no screaming or fighting when police entered and grabbed him and his wife… Lee believes the police officers involved should not only apologize but lose their jobs. Additionally the couple wants compensation for their physical and mental anguish due to the incident. The couple have given a statement to Coquitlam police and will be getting a lawyer. Global News

RCMP vehicle involved in serious crash
An RCMP vehicle was involved in a serious crash Monday afternoon at one of the city's most notorious intersections. Emergency crews were called to the corner of Kenaston and McGillivray Boulevard for what appeared to be a two-vehicle crash. A light standard was seen sitting atop the police cruiser in the southbound lane of Kenaston. Front and side airbags were deployed. A van ended up in the westbound lane of McGillivray. No word yet on injuries. The intersection was highlighted eariler this year as having the second highest number of collisions in the city with 2,298 crashes between 2005 and 2014. Winnipeg Free Press; CTV News; CBC News

La Presse says Montreal police tracked journalist's iPhone for months
A Montreal journalist says he was furious when he learned that city police monitored his iPhone for months in order to find out who he was speaking with… The French-language newspaper reported it has learned at least 24 surveillance warrants were issued for Lagace's phone this year at the request of the police's special investigations unit. That section is responsible for looking into crime within the police force. Three of those warrants reportedly authorized police to get the phone numbers for all Lagace's incoming and outgoing texts and calls, while another allowed them to track the phone's location via its GPS chip. Lagace said police told him they obtained the court-issued warrants because they believed the target of one of their investigations was feeding him information. But he said the story in question was actually first reported on by a competitor, leading him to believe the investigation was actually a thinly veiled attempt to learn the identity of his sources within the police department… Reaction to La Presse's story was swift, with some unions and media organizations denouncing the police operation, and some opposition city councillors calling for Montreal's police chief to step aside while the matter is investigated. Canadian Press (Globe and Mail; CTV News; Herald News; Metro News); Montreal Gazette; Postmedia Network (Toronto Star)

Broadcast Media / Médias télédiffusés :

CTV News discussed the monitoring of Patrick Lagace's emails and phone calls by the Montreal Police as well as reactions to the revelation by the SPVP, Montreal City Councilors, the Minister of Public Security of Quebec, and the general public (CTV News, 18:15 ET, 19:15 ET)

Le chef du SPVM n'exclut pas que d'autres journalistes aient été placés sous surveillance
Le chef de police Philippe Pichet a pris la parole à 16 h 30 au quartier général du SPVM pour réagir à l'onde de choc créée par la mise sous surveillance du téléphone cellulaire de Patrick Lagacé. Le chef du SPVM a déclaré qu'il n'était pas insensible à l'affaire. «Cette enquête visait un de nos policiers et non Patrick Lagacé. C'est une situation qui a été traitée avec des moyens exceptionnels. Quand j'ai appris qu'un mandat a été demandé, je me suis assuré que nous respections toutes les règles», a-t-il dit. «Nous avons suivi les règles et le juge a autorisé le mandat», a-t-il rappelé. «Le SPVM reconnaît la liberté d'expression.» Répondant à la question d'un journaliste, il a précisé qu'il ne pouvait dire si d'autres journalistes ont été placés sous surveillance. Des vérifications à ce sujet sont en cours… Le ministre québécois de la Sécurité publique, Martin Coiteux, s'est dit «renversé» par ces révélations. La Presse; Radio Canada; CTV News

We're spied on more often than you think, journalists groups say
Canadians may be used to hearing about police tapping journalists' phones in China, or tailing them down the street in Turkey. But in Montreal, Canada? Unfortunately, say organizations like Canadian Journalists for Free Expression, it is happening a lot more than we think. "It's something we've been suspecting for a long time – that when this kind of power is in the hands of the police they will abuse it," said Tom Henheffer, executive director of CJFE. "I used to be cautious about drawing parallels with Canada and dictatorships like Turkey, China, Russia or Egypt. But the difference has started to erode, especially when it comes to privacy rights"... Montreal Gazette

Les pratiques du SPVM inquiètent Edward Snowden
Le lanceur d'alerte Edward Snowden, qui a mis à jour les activités de surveillance de masse de la NSA aux États-Unis, s'inquiète des pratiques du SPVM qui a espionné le journaliste de *La Presse* Patrick Lagacé. Dans un message publié sur le réseau social Twitter, Edward Snowden qui a fui en Russie par crainte des représailles dénonce la surveillance des journalistes en prenant l'exemple du journaliste de *La Presse*. «Êtes-vous un journaliste ? Le fait que la police vous espionne pour identifier vos sources n'est pas hypothétique. Ça se passe aujourd'hui», a écrit l'homme. Son message est accompagné d'un lien vers un article du quotidien montréalais *The Gazette* sur la surveillance dont le chroniqueur a été la cible le printemps dernier. La Presse

Lagacé espionné: «inacceptable», «troublant», réagit la classe politique
Pour le chef péquiste Jean-François Lisée, l'espionnage du journaliste de La Presse, Patrick Lagacé par la police de Montréal est « inacceptable » et devrait « cesser immédiatement ». Les révélations de La Presse laissent le chef péquiste « complètement outré », a-t-il dit dans une entrevue à 98,5 ce matin. « Le travail du journaliste fait partie de la démocratie, lance sans détour, Lisée, lui-même ancien journaliste. C'est un genre de soupape pour que des informations qui devraient circuler, mais ne circulent pas, puissent arriver aux lecteurs, aux citoyens, et même aux élus ». « Qu'un journaliste ait été sous enquête, que son téléphone ait été vu, qu'il ait été géolocalisé alors que la Cour suprême disait récemment que cela devrait être réservé à des cas exceptionnels - et c'est encore trop - que l'Assemblée nationale ait unanimement réprouvé en septembre dernier la saisie de l'ordinateur du journaliste du Journal de Montréal Michael Nguyen, que la police continue de tenter d'avoir des sources du côté des journalistes, c'est inacceptable. Il faut mettre un holà à ça ». La Presse

Spying on Montreal reporter an attack on free press
An opinion piece states, "For the second time in two months, a journalist reporting on matters related to the justice system has found his own rights egregiously compromised. These affronts to freedom of the press are deeply troubling. Starting last January, Montreal police spied on La Presse columnist Patrick Lagacé through his cellphone, obtaining his call records and tracking his movements, as part of what police said was an internal probe of anti-gang squad officers later charged with fabricating evidence. This is an outrageous violation of Lagacé's privacy and an attack on his role as a journalist in a democratic society. He was never a target of the probe nor suspected of any wrongdoing. And he was never even given an opportunity to safeguard his contacts from police scrutiny. In September, Journal de Montréal reporter Michaël Nguyen had his computer seized by the Sûreté du Québec after reporting on two judges under investigation by the Conseil de la magistrature... Police must be held to account for these heavy-handed tactics. But the judges and justices of the peace who signed off the police warrants have much to answer for, too..." Postmedia Network (Montreal Gazette); Globe and Mail

RCMP mourns one of its own
Insp. Tony Perry was found dead Friday morning in Happy-Valley-Goose Bay. Perry, who is originally from Deer Lake, joined the RCMP in 1988 and served in Nova Scotia until July 2015, when he was transferred to Newfoundland and Labrador. Most recently, Perry worked as a negotiator between police, aboriginal leaders and protesters at the Muskrat Falls hydroelectric project site. Foul play is not suspected. Western Star

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Pepper spray use with little accountability concerns prison watchdog
Canada's prison watchdog is raising red flags about the "go-to" use of pepper spray in federal penitentiaries, which his office found has tripled in a five-year period with little accountability. In his annual report tabled in Parliament Monday, Correctional Investigator Howard Sapers said pepper spray was used in 60 per cent of the 1,833 use-of-force incidents in 2015-2016. "The link between institutional safety and the increasing use and reliance on inflammatory agents is tenuous at best," said Sapers. The correctional investigator partly blamed the increase on a policy change back in September 2010 that allowed correctional officers to carry pepper spray canisters on their belts. Before then the chemical, which makes it hard to breath and see, was locked up. His report notes that there hasn't been a correlating increase in the severity of security incidents or threats to justify the increased use pepper spray. Sapers also called out what he termed a lack of monitoring and national oversight of how pepper spray is stored, weighed, inspected, assigned and controlled. CBC News; La Presse Canadienne (L'actualité)

Broadcast Media / Médias télédiffusés :

CTV News' Power Play interviewed Correctional Investigator Howard Sapers on the Correctional Investigator's 2015-2016 Annual Report and the use of pepper spray in federal penitentiaries. Rough Transcript (2016-10-31)

The Number of Female Indigenous Prisoners in Canada Has Doubled in the Last Decade
The number of Indigenous people now represent more than a quarter of all inmates held in Canada's federal prisons, according to the new annual report from Canada's prison watchdog. And within the last decade, the number of female Indigenous inmates has doubled, while the population of male Indigenous inmates has increased by more than 50 percent. During that time, the federal inmate population increased by only 10 percent. "It's a shameful milestone in Canadian history," correctional investigator Howard Sapers told a press conference on Monday. His annual report, which also says Indigenous women represent 35 percent of inmates in federal prisons, serves to highlight his concerns about federal correctional facilities, which house offenders who have been sentenced to more than two years in prison... In addition to decrying the increase in Indigenous offenders, his report also sounds the alarm over a dramatic increase in guards using "inflammatory agents" such as pepper spray against inmates. The number of incidents involving the use of pepper spray against inmates has more than tripled since 2011, and more than one-third of those incidents involved inmates suffering from mental illnesses. Vice News

Ontario premier calls inmate's 52-month segregation 'extremely disturbing'
The treatment of an inmate held in segregation for four years is "extremely disturbing," Ontario Premier Kathleen Wynne said Monday, but she declined to call it torture... Federal correctional investigator Howard Sapers called Capay's case "troubling," and said he had never before heard of someone being kept in such conditions. There have been cases, however, in the federal system in which offenders are kept in segregation for years, he said. "Until we have a legislated cap, I'm very concerned that long-term segregation and segregation that could go on almost indefinitely is still possible," Sapers said in Ottawa. Canadian Press (CTV News)

Dangerous offender status sought for man
It's been a long time coming, but the office of Kingston's Crown attorney is applying to seek a dangerous offender designation for a 39-year-old sexual predator initially sent to prison in 2004 for drugging and raping three women in North Bay between 1999 and 2002. The decision follows Rene R. Bourdon's convictions in Kingston's Superior Court on two new counts of sexual assault in the Kingston area; eight violations of the long-term supervision order imposed on him 12 years ago at his original sentencing; and fraudulent personation in the service of a sex scheme of Rube Goldberg complexity... In the first nine months following his release in November 2005, however, his release was suspended four times for violating conditions of the LTSO and he was shunted between all three (at that time) Ontario federal halfway houses directly operated by Correctional Service Canada. Known as community correctional centres, they're the the only halfway houses in the system that can't refuse to accept high-risk offenders... The Whig

St. Lawrence Parks Commission would like to continue Kingston Penitentiary tours
The prison that was once off-limits to most people has just completed its first full tourist season. Public tours of Kingston Penitentiary brought in thousands of visitors and millions of dollars over the past 5 months — making it Kingston's top attraction. The final "sold-out" tours concluded this weekend. The question now — will the once-notorious maximum security prison re-open next year? CKWS Kingston

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Vancouver Coastal Health applies for 2 more supervised injection sites
Vancouver Coastal Health (VCH) has submitted applications to Health Canada to open two new supervised injection sites in Vancouver in the midst of an overdose crisis. The proposed supervised injection sites are located at the Downtown Eastside Mental Health and Substance Use Drop-In Centre (528 Powell Street) and the Heatley Integrated Health Centre (330 Heatley Street). "The evidence is clear that supervised consumption services reduce transmision of diseases and help to connect peopel to healthcare services," said B.C. Health Minister Terry Lake. "In the face of the current public health emergency, what is even more critical is the fact that more than three million injections have been done at Insite in the last 13 years and not one person has died of an overdose there." Insite, Canada's first supervised injection site, was opened in 2003 in Vancouver's Downtown Eastside. Metro News; CBC News

Vehicle seizures, extended zero tolerance as Saskatchewan tackles drunk driving
Proposed changes to impaired driving laws in Saskatchewan are being called a good first step by grieving families of people killed by drunk drivers. The changes include a three-day vehicle seizure for drivers who are charged for the first time with having a blood alcohol content over .04 and an extended a zero tolerance policy to all drivers under the age of 21. If passed, the new law would also extend mandatory ignition interlock durations for repeat drunk drivers and apply to those who refuse to provide a breath sample... The changes will take effect Jan. 1, if approved by the legislature. Canadian Press (Brandon Sun); Postmedia Network (Star Phoenix)

How North America Found Itself in the Grips of an Opioid Crisis
The story of today's prescription opioid overdose crisis didn't start this year, or ten years ago, or even 100 years ago. It starts with a plant—the opium poppy—that has been a part of human civilization for thousands of years... But how did we get here? The answer is a cautionary tale about the power of Big Pharma, the unintended consequences of government intervention, and the tenacity of drug markets. Vice News

Opioid overdose treatment kit requires training before use, but available soon
Government-funded kits announced this summer that will contain the antidote for the deadly drug Fentanyl and other opioid overdoses aren't on the streets yet... While there's no specific timeline, provincial officials are still promising a fall launch. The province announced funding for the Naloxone take-home kits in late August. According to the Department of Health, within days of that announcement, it struck a working group -- addictions experts, representatives of regional health authorities, government and the Aids Committee of Newfoundland and Labrador -- that has been meeting regularly. People who take the kit home have to be trained on its use and just last week, a train-the- trainer program got started. Telegram

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Medical marijuana industry budding in Lachute
Medical marijuana is a growing industry in Canada. Doctors are increasingly prescribing marijuana to treat everything from cancer to back pain. There are currently 36 licensed medical marijuana facilities in the country, including 21 in Ontario. Two new facilities are expected to be opening in Lachute, one as early as next spring. Quebec currently has only one licensed facility, owned and operated by Gatineau-based Hydropothecary. After the city began the consultation process to rezone a section of the city for specific use by medical marijuana facilities, Lachute Mayor Carl Péloquin told The Review it received dozens of inquiries from interested companies. "I thought that it would be good to be ready and to have the right zoning, since it's now considered an acceptable therapy," said Péloquin. Council initially looked at the possibility of rezoning an industrial sector on Cristini Boulevard, but rejected the plan after nearly a dozen of the existing industries objected. After evaluating their options, Péloquin said council chose to begin the consultation process to rezone the area surrounding the Régie Intermunicipale Argenteuil Deux-Montagnes garbage dump, which is located on Chemin des Sources. The Review

PUBLIC SERVICE / FONCTION PUBLIQUE

Government misses Halloween deadline to clear Phoenix backlog
Public Services and Procurement Canada has missed its promised Halloween deadline to clear the backlog of pay problems caused by the Phoenix pay system, as the cases of 22,000 public servants remain unresolved, the department's top bureaucrat says. Deputy minister Marie Lemay said the department couldn't meet the self-imposed Oct. 31 target because the remaining cases are older and much more complicated than the front end of the pile and require much more work than expected. Lemay said she is disappointed the deadline was missed but that the department did everything it could. Ottawa Citizen

OTHER / AUTRES

NIL

INTERNATIONAL

Dakota Access pipeline protests: UN group investigates human rights abuses
A United Nations group is investigating allegations of human rights abuses by North Dakota law enforcement against Native American protesters, with indigenous leaders testifying about "acts of war" they observed during mass arrests at an oil pipeline protest. A representative of the UN's permanent forum on indigenous issues, an advisory group, has been collecting testimony from Dakota Access pipeline protesters who have raised concerns about excessive force, unlawful arrests and mistreatment in jail where some activists have been held in cages. Guardian (UK)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

canadaCJFE
Today @MattDube and @RalphGoodale debated #SPVM @kick1972 and #VICE @BMakuch cases. @snowden #ProtectPressFreedom http://bit.ly/2fxQYup

https://twitter.com/VincentBP
Affaire Lagacé: le ministre fédéral Ralph Goodale prêt « à avoir une discussion sérieuse » sur les règles policières http://www.lapresse.ca/actualites/justice-et-affaires-criminelles/201610/31/01-5036264-affaire-lagace-goodale-pret-pour-une-discussion-serieuse-sur-les-regles-policieres.php ...

davidakin
"We take freedom of the press very, very, very seriously" @RalphGoodale says without condemning cops who spy on cops.

davidakin
And here's @RalphGoodale reading a statement on what happens when "journalism and investigations intercept".

rachaiello
"We take the freedom of the press in this country very, very seriously," Min. @RalphGoodale says just now in the #HoC #pressfreedom #cdnpoli

Colinfreeze
3. The #cdnpoli powers are important because @RalphGoodale is consulting Canadians on whether cops need more powers. https://www.publicsafety.gc.ca/cnt/rsrcs/pblc

RalphGoodale
Happy Halloween! Wishing everyone a fun and safe evening of trick or treating!

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

jonmeyer_980
#NathanEStewart report. Wildlife team monitoring pod of orcas en route to Balagny Psg, and humpback whale sightings. #Heiltsuk #bellabella

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Safety_Canada
Participating in our Twitter Chat on Nat'l Security Accountability on Thursday? Check this out #YourNatlSec http://ow.ly/4O86305HX89

Securite_Canada
Vous participez à notre conv. Twitter sur responsabilité en matière de sécurité nat. jeudi? Consultez #VotreSecNat http://ow.ly/F0b5305HXbn

NATIONAL SECURITY / SÉCURITÉ NATIONALE

OttawaCitizen
Ottawa terror suspect granted bail again after allegedly breaching conditions http://ow.ly/Dzzi305HWrT

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

MichelleZilio
2017 immigration total target remains unchanged from last year. 300,000 total: http://news.gc.ca/web/article-en.do?mthd=index&crtr.page=1&nid=1145319 … #cdnpoli #cdnimm

RosieBarton
Macallum: economic immigrants goes from 160,600 in 2016 to 172,500 in 2017. #hw

CYBER SECURITY / CYBERSÉCURITÉ

cyber_securite
Les enfants ne sont pas seuls à se déguiser à l'#Halloween! Sachez détecter la fraude : http://www.pensezcybersecurite.gc.ca/cnt/rsks/scms-frd/index-fr.aspx …

GetCyberSafe
How can #cybercrime affect Canada's critical infrastructure? Find out on our blog: https://www.getcybersafe.gc.ca/cnt/blg/pst-20161031-en.aspx … #CSAM

LAW ENFORCEMENT / APPLICATION DE LA LOI

RCMPAlberta
D/Commr. Ryan accepted a medallion on behalf of RCMP employees who assisted in the #YMMFire. http://rcmp.ca/-gSr

VGaudreau
Le chef du @SPVM n'exclut pas que d'autres journalistes aient été placés sous surveillance http://www.lapresse.ca/actualites/justice-et-affaires-criminelles/201610/31/01-5036220-le-chef-du-spvm-nexclut-pas-que-dautres-journalistes-aient-ete-places-sous-surveillance.php … @fpjq #fpjq @kick1972

Colinfreeze
Cops got warrants to spy on journalist "using the GPS chip in his iPhone & to obtain the IDs of everyone he has spoken and messaged with." https://twitter.com/CBCCanada/status/793157452321685505

Colinfreeze
7. CanLIi indicates real-time GPS tracking of iPhones still a novel power for #cdnpoli police.Dunno of any parallels https://www.canlii.org/en/#search/text=GPS%20and%20real-time%20and%20%20tracking …

georgiastraight
The irresistible allure of a Hells Angels funeral and the cost of the war on drugs http://ow.ly/u6yW305Hypw #HellsAngels #drugs

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

CTV_PowerPlay
Federal correctional Investigator Howard Sapers is here to share the findings of a new report. #cdnpoli #ctvpp

alisoncrawford5
Sapers points out that RCMP use of force and pepper has gone down just as correctional officers use it more often. #hw

alisoncrawford5
Sapers says police services account for their use of force and pepper spray and Correctional Service Canada must do the same. #hw

alisoncrawford5
Sapers says lack of oversight, insufficient video footage, little documentation, makes it hard to see if pepper spray is used appropriately

alisoncrawford5
Sapers says pepper spray was used in 54% of use of force incidents when offenders were harming themselves. He says hardly therapeutic.

alisoncrawford5
Sapers says correctional officers often not following the rules for checking inmates' health after using pepper spray. #hw

alisoncrawford5
Sapers says 40% of use of force incidents at CSC psychiatric hospitals involved pepper spray. #hw

l_stone
Sapers says he's never heard of a similar case to Adam Capay - an inmate held in acrylic glass cell under artificial light for 24 hrs a day

l_stone
Since March 2005, aboriginal inmate population increased by 52%. Sapers again recommends a deputy commish for indigenous corrections

alisoncrawford5
Sapers says the increase is linked to pepper spray now being on officers' belts and not locked in designated control posts. #hw

alisoncrawford5
MOre than 1/3 of all use of force incidents in fed prisons involved inmates with mental health issues identified by CSC #hw

l_stone
Security incidents involving pepper spray in federal prisons have tripled since 2011/12, new report from Correctional Investigator says

l_stone
Correctional Investigator Howard Sapers speaks now about his annual report - special focus on use of pepper spray

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

VICE
How North America found itself in the grips of an opioid crisis: http://bit.ly/2fo491J

PUBLIC SERVICE / FONCTION PUBLIQUE

AshleyBurkeCBC
Correction: $500,000 is the estimated operating cost for the gov't office that handles claims for workers' out-of-pocket expenses #Phoenix

CBCTheNational
Phoenix deadline arrives, but pay problems continue for thousands of public servants http://www.cbc.ca/1.3826399

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

Today's News / Actualités
October 31, 2016 / le 31 octobre 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 9:00 a.m. and 6:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 9h00 et 18h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Montreal Cops Have Tracked a Journalist's Cellphone for the Past Year
Montreal police, investigating the possibility of crooked cops on the force, obtained warrants to surveil a journalist's iPhone, and even obtained permission to use his GPS chip to track his whereabouts at all time. But the **federal minister of public safety, Ralph Goodale, stopped short of discouraging police forces from going to the courts to obtain judicial orders against journalists**. Asked directly by NDP Member of Parliament Matthew Dubé on Monday about whether he'll issue a directive to create more formal rules around how police deal with journalists, **Goodale would only say that *"we take the***

freedom of the press in this country very, very seriously." Dubé raised the question after on Monday after Montreal newspaper La Presse published details on surveillances warrants, at least 24 in total, obtained to surveil journalist Patrick Lagacé. The MP also referenced another case, where federal police are working to obtain chat records from a VICE journalist's cell phone, as evidence that action needs to be taken. Vice News

SPVM: le ministre Coiteux est surpris par une procédure contre un journaliste
Le ministre de la Sécurité publique, Martin Coiteux, a exprimé sa surprise, lundi, en apprenant que la police a surveillé les appels téléphoniques d'un journaliste. M. Coiteux a entamé des vérifications pour établir si les procédures ont été respectées par le Service de police de la ville de Montréal (SPVM). «J'ai été très surpris et c'est pour ça qu'on fait des vérifications», a-t-il dit. La ministre de la Justice, Stéphanie Vallée, effectuera également une évaluation des procédures qui ont mené un tribunal à accorder à plusieurs reprises un mandat au SPVM, cette année... À Ottawa, **le ministre de la Sécurité publique, Ralph Goodale, a affirmé que la situation est toujours délicate quand le journalisme et les enquêtes policières se rencontrent. *«Il s'agit d'un cas qui relève des compétences provinciales, mais la position fédérale est d'affirmer que la liberté de presse est une valeur canadienne fondamentale»,* a-t-il dit.** La Presse Canadienne (L'actualité)

Affaire Lagacé : Goodale prêt pour «une discussion sérieuse» sur les règles policières
À la lumière de l'affaire Patrick Lagacé, **le ministre fédéral de la Sécurité publique Ralph Goodale se dit *« certainement prêt à avoir une discussion de politique sérieuse »* et *« à entendre les représentations »* des médias sur la façon dont les forces policières devraient concilier leurs enquêtes avec la protection des sources journalistiques et la liberté de presse. Le ministre Goodale, qui n'a pas voulu commenter le cas de Patrick Lagacé mais qui se dit *« profondément préoccupé par ce genre de dossier »,* s'assurera prochainement auprès du commissaire de la GRC Bob Paulson que les directives fédérales en vigueur sont respectées dans les faits.** Depuis 2003, une directive ministérielle demande aux forces policières de porter une « attention spéciale » au statut des médias dans le cadre d'enquêtes sur la sécurité nationale. ***« Au regard de ce dossier au Québec, qui est sous juridiction provinciale, c'est une question qui doit être posée [à la GRC]. Je n'ai pas encore eu l'occasion de le faire [hier], mais je le ferai [prochainement]. C'est une question juste de demander [à la GRC] de s'assurer que la directive ministérielle qui requiert un très haut standard soit appliquée dans les faits »,* dit le ministre Goodale en entrevue à La Presse. Le ministre Goodale, qui croit que la liberté de presse est *« une valeur fondamentale »* au Canada, n'a pas voulu s'avancer à savoir si des changements législatifs sont nécessaires afin de protéger la liberté de presse dans le cadre d'enquêtes policières. *« Nous devons traiter de cet enjeu sérieusement et je suis certainement prêt à entendre les représentations [des médias et d'associations de journalistes comme la FPJQ] sur ce qui pourrait être un meilleur ensemble de règles »,* dit le ministre Goodale...** La Sûreté du Québec a saisi en septembre l'ordinateur d'un journaliste du Journal de Montréal à la demande du Conseil de la magistrature en rapport avec un dossier traité par le conseil. **Le ministre Goodale, qui n'a pas voulu commenter sur ces cas précis, fait valoir que *« les cas vont suivre leur cours pour voir s'ils respectent les critères de la Cour suprême »* en matière de protection du matériel et des sources journalistiques.** La Presse

Liberals rapped as $900M unspent by Indigenous Affairs among 'lapsed' funding for fiscal 2016
Like the Harper government before it, the Trudeau government left billions of dollars unspent on everything from national parks to veterans services to economic development grants during the 2015-16 fiscal year. The so-called "lapsed" funding for fiscal 2016 is $9.7 billion, according to the Public Accounts of Canada. All of those unspent funds were used to pay down the federal debt. ublic Safety Canada, which includes the RCMP, the Correctional Service of Canada, and Canada Border Services Agency, was authorized to spend $9.2 billion in fiscal 2016 but left unspent 11.6 per cent of that — about $1 billion. **Scott Bardsley, press secretary to Public Safety Minister Ralph Goodale,** said the lion's share of the lapse — about $700 million — was related to disaster relief for the provinces that, while booked by the federal government in 2016, was not paid out. National Post

TOP STORIES / MANCHETTES

Pepper spray use with little accountability concerns prison watchdog
Canada's prison watchdog is raising red flags about the "go-to" use of pepper spray in federal penitentiaries, which his office found has tripled in a five-year period with little accountability. In his annual report tabled in Parliament Monday, Correctional Investigator Howard Sapers said pepper spray was used in 60 per cent of the 1,833 use-of-force incidents in 2015-2016. "The link between institutional safety and the increasing use and reliance on inflammatory agents is tenuous at best," said Sapers. The correctional investigator partly blamed the increase on a policy change back in September 2010 that allowed correctional officers to carry pepper spray canisters on their belts. Before then the chemical, which makes it hard to breath and see, was locked up. His report notes that there hasn't been a correlating increase in the severity of security incidents or threats to justify the increased use pepper spray. Sapers also called out what he termed a lack of monitoring and national oversight of how pepper spray is stored, weighed, inspected, assigned and controlled. CBC News; La Presse Canadienne (L'actualité)

The Number of Female Indigenous Prisoners in Canada Has Doubled in the Last Decade
The number of Indigenous people now represent more than a quarter of all inmates held in Canada's federal prisons, according to the new annual report from Canada's prison watchdog. And within the last decade, the number of female Indigenous inmates has doubled, while the population of male Indigenous inmates has increased by more than 50 percent. During that time, the federal inmate population increased by only 10 percent. "It's a shameful milestone in Canadian history," correctional investigator Howard Sapers told a press conference on Monday. His annual report, which also says Indigenous women represent 35 percent of inmates in federal prisons, serves to highlight his concerns about federal correctional facilities, which house offenders who have been sentenced to more than two years in prison... In addition to decrying the increase in Indigenous offenders, his report also sounds the alarm over a dramatic increase in guards using "inflammatory agents" such as pepper spray against inmates. The number of incidents involving the use of pepper spray against inmates has more than tripled since 2011, and more than one-third of those incidents involved inmates suffering from mental illnesses. Vice News

La Presse says Montreal police tracked journalist's iPhone for months
A Montreal journalist says he was furious when he learned that city police monitored his iPhone for months in order to find out who he was speaking with... The French-language newspaper reported it has learned at least 24 surveillance warrants were issued for Lagace's phone this year at the request of the police's special investigations unit. That section is responsible for looking into crime within the police force. Three of those warrants reportedly authorized police to get the phone numbers for all Lagace's incoming and outgoing texts and calls, while another allowed them to track the phone's location via its GPS chip. Lagace said police told him they obtained the court-issued warrants because they believed the target of one of their investigations was feeding him information. But he said the story in question was actually first reported on by a competitor, leading him to believe the investigation was actually a thinly veiled attempt to learn the identity of his sources within the police department... Reaction to La Presse's story was swift, with some unions and media organizations denouncing the police operation, and some opposition city councillors calling for Montreal's police chief to step aside while the matter is investigated. Canadian Press (Globe and Mail; CTV News; Herald News; Metro News); Montreal Gazette; Postmedia Network (Toronto Star)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fort McMurray fire first responders honoured in Alberta legislature ceremony
Premier Rachel Notley and her government paid tribute Monday to those who came to Alberta's aid and rescue during the spring's devastating Fort McMurray wildfire. Notley said the fire devastated the lives of thousands of people but failed to cripple their spirit or resolve. Individuals representing nine first-responder agencies were recognized in a ceremony in the rotunda of the Alberta legislature... One of the recipients, Wood Buffalo fire Chief Darby Allen, said people are strong, but are still struggling with the

memories and reminders of the devastation. Canadian Press (Times Colonist; Winnipeg Free Press); CBC News; Fort McMurray Today

Canada not ready for catastrophic effects of climate change, report warns
Canada is not prepared to handle the devastating and costly effects of increased flooding and extreme weather brought on by climate change, according to a new report released Monday. The report from the University of Waterloo's Intact Centre on Climate Adaptation found governments at all levels across the country need to take immediate action to make the country's infrastructure – highways, railways and water supply systems- more resilient or face increasingly catastrophic financial loses in the future. "The country as a whole is not prepared for climate change, extreme weather events, with a primary focus on flooding," said Blair Feltmate, head of the Intact Centre on Climate Adaptation. "There was no particular province that was disproportionately good or bad compared to the other." CHML Hamilton

Alberta legislation aims to reduce human-caused wildfires
The Alberta government tabled legislation Monday that aims to reduce the number of human-caused wildfires in the province. Over the past five years, about 70 per cent of the wildfires in Alberta have been linked to human activity. The province said Bill 24, the Forest and Prairie Protection Amendment Act, will also enhance firefighting operations. Global News

Hunter and stepson reported overdue
Search and rescue teams have been called out to look for a 55-year-old man and his stepson, reported overdue Sunday from a hunting trip northeast of Quesnel. Glen Brooker and the 10-year-old, whose name was not provided, were to have ton into the area of Stoney Lake or Narrow Lake on Sunday and did not return home that night as planned. Prince George Citizen; CBC News

Arctic survival tips from a search and rescue volunteer
With the sea ice beginning to form and more people heading out on the land, the Civil Air Search and Rescue Association (CASARA) wants to remind people about the skills, safety techniques and tools you need to ensure you survive if stranded in the wilderness. CASARA is a national volunteer organization funded by the Department of National Defence that provides air search assistance to the Royal Canadian Air Force and promotes flight safety. CBC News

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Ottawa terror suspect granted bail again after allegedly breaching conditions
An Ottawa terror suspect has been released from custody after he was charged with breaching some of his bail conditions while awaiting the outcome of his case. The RCMP arrested Tevis Gonyou-McLean in August on a terrorism peace bond for his alleged support of ISIL and was later granted bail on several conditions that included wearing a GPS monitoring device on his ankle and a ban on possessing any terrorist logos. On Oct. 25, the 24-year-old was arrested again after police allege he failed to report to the John Howard Society's bail supervisory program and reside at his pre-approved address, and that he damaged his ankle bracelet, thereby allegedly committing mischief. But his Ottawa lawyer, Biagio Del Greco, said the breaches were the result of a "miscommunication" and said the damage to the bracelet occurred while his client was in police custody and was unintentional. None of the breaches were related to alleged terrorist activity. Ottawa Citizen

Quebec hosts UNESCO conference on prevention of radicalization of young people
Quebec is hosting an important conference on the links between radicalization and the Internet. A UNESCO conference called "Youth and the Internet: Fighting Radicalization and Extremism" is taking place in Quebec City. It started Sunday night and continues until Tuesday. Global News

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Mammoth fine for importing woolly mammoth tusk
Border agents at the Ambassador Bridge fined two Canadians for under-reporting the value of antiques, which included a woolly mammoth tusk. Two Canadians returning from the U.S. in September brought along a haul of antiques, including the woolly mammoth tusk, according to Canada Border Services Agency. The two travellers reported the goods cost an estimated $760, but further estimates revealed the items were valued at $6,100. Border officials issued a $3,317 penalty for under-reporting the value. The items were eventually released to the owners. CBC News; Postmedia Network (Windsor Star)

Ottawa man gets 43-month sentence for forging immigration documents
An Ottawa man who forged documents to allow hundreds of immigrants to enter Canada has been sentenced to three-and-a-half years behind bars. Mohamed Farah Abdulle, 54, was sentenced Monday after being convicted last November on five charges relating to the immigration fraud scheme, according to a statement from the Canada Border Services Agency (CBSA). According to the CBSA, Abdulle had filed more than 170 fraudulent sponsorship applications for 528 people, all while collecting fees from the applicants for his services. CBC News

Border post in automated experiment
The border crossing at Morses Line is a tiny operation that's gone high tech to handle the traffic in slow periods. Described as a "sleepy border crossing" with few than 60 vehicles a day, there was a proposal at one point to close it down. Now the Canada Border Services Agency (CBSA) is testing new technology that could be the standard for border control at small and remote crossings across the country. But critics say the experiment is a threat to public safety. Radio Canada

John McCallum sets new base immigration target at 300,000 a year
The Liberal government is boosting the base number for immigrants to Canada to 300,000 to help drive economic growth as the country grapples with an aging demographic... McCallum said the new annual target will be set at 300,000. The target from 2011-2015 was 260,000 which increased to 300,000 in 2016 to account for the influx of Syrian refugees... More than half the 2016 total, 160,600, are in the economic category for skilled workers, business people and caregivers; 80,000 are in the family program for spouses, children, parents and grandparents; 55,800 are refugees and protected persons and another 3,600 are in the humanitarian category. CBC News

Law enforcement agencies around the world collaborate on international Darknet marketplace enforcement operation
A globally coordinated law enforcement action against the buyers and sellers of illicit drugs and other illegal activities using Darknet global marketplaces was conducted Oct. 22 to 28. "Operation Hyperion" was initiated by U.S. federal law enforcement, the Five Eyes Law Enforcement Group (Australia, Canada, New Zealand, the United Kingdom and the United States) and members of Europol, the European Union's law enforcement agency, as the first step in developing a more unified global law enforcement response to the growing usage of the Darknet by individuals seeking to buy and sell illicit drugs and other illegal goods and services... Operation Hyperion resulted in a number of law enforcement leads on cases related to the buying and selling of illicit drugs and other goods on the Darknet. This operation will also help law enforcement agencies continue to combat the trafficking of illicit goods and services on the Darknet through the identification of new smuggling networks and trends... International partners included Europol the United Kingdom's National Crime Agency; Australian Federal Police; New Zealand Police and New Zealand Customs Service; Canada's Royal Canadian Mounted Police, Canada Post and Canada Border Services Agency; The Netherlands; French Customs National Intelligence and Investigations Directorate; Finnish Customs; Swedish Police Authority and Swedish Customs; Ireland's

Garda National Drugs & Organised Crime Bureau; and Spain's Guardia Civil. U.S. Immigration and Customs Enforcement

Peace Bridge to close one lane for construction
As long as U.S. and Canada customs have the necessary staff available and suitable number of inspection lanes open, any traffic impacts related to the temporary closure of one lane on the Peace Bridge can be mitigated, according to the agency that owns and operates the international border crossing. The Peace Bridge will be reduced to two lanes between Nov. 15 and May 15 for an ongoing $100-million rehabilitation. Fort Erie Times

Liberals in denial about Monsef story
An opinion pieces states, "A file within the federal government has been opened to investigate Democratic Institutions Minister Maryam Monsef for citizenship fraud. And the Liberal government seems to be in denial about it. The Sun exclusively reported that a file was opened to investigate Monsef, who claims she only recently learned she was born in Iran, not Afghanistan. A number of complaints were received through a tip line created by Canada Border Service Agency (CBSA) and the Department of Immigration, Refugees and Citizenship Canada (IRCC), leading to an investigation. It remains unknown whether Monsef's proper birthplace information was included on her original refugee and citizenship application..." Postmedia Network (Toronto Sun)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Old Android malware still circulating, Apple patches Windows apps - Security news IT leaders need to know
This week's highlights also include a fake Microsoft security installer and 247 Oracle patches being issued. Apple has released Xcode 8.1 to address multiple security issues that could allow a remote attacker to be able to cause unexpected application termination or arbitrary code execution. iCloud for Windows 6.0.1 corrects two security flaws that could result in disclosure of user information or arbitrary code execution. Finally, the same two flaws are corrected in iTunes for Windows 12.5.2. National Post

LAW ENFORCEMENT / APPLICATION DE LA LOI

RCMP not to blame for death of suspect who shot Golden Mountie: Police watchdog
The suspect who led police on a manhunt after shooting a Mountie near Golden died from head trauma and RCMP action or inaction was not to blame, B.C.'s police watchdog says. The provincial Independent Investigations Office launched a probe to determine whether there was any connection between the officers' actions and the death of Sheldon Kyle Thunderblanket, 40. Investigators concluded "there is no causal connection between death of the male affected person and actions or inactions of police," according to a Independent Investigations Office media release. Info News

RCMP nab 10 men for prostitution-related offences in Moncton
The Codiac RCMP arrested 10 men, aged 25 to 80, for attempting to obtain sexual services in Moncton in two separate busts earlier in October. The RCMP carried out two police operations Oct. 14 and 27 in the area of Dufferin Street targeting individuals attempting to buy services from sex trade workers. CBC News; CTV News

'We are seniors, why you hit me and my wife?': Elderly couple speak out about RCMP arrest
The elderly couple caught on camera being violently arrested by Coquitlam RCMP last week is speaking out. The incident happened on the evening of Oct. 26 after police were called to a strata meeting that allegedly got out of control. The video, which was posted on YouTube, appears to show an officer dragging a man down a staircase while another officer arrests a woman, who appears to fall at one point... Myung Ju Lee and his wife, Kap Su Lee, told Global News they spent the night in the hospital after ending up with bruises, cuts and scrapes as a result of the incident. "[The police] walked up and did not say anything. Just walked up and grabbed us," Myung Ju Lee said. Lee claims the strata meeting was

not over and there had been no screaming or fighting when police entered and grabbed him and his wife… Lee believes the police officers involved should not only apologize but lose their jobs. Additionally the couple wants compensation for their physical and mental anguish due to the incident. The couple have given a statement to Coquitlam police and will be getting a lawyer. Global News

RCMP vehicle involved in serious crash
An RCMP vehicle was involved in a serious crash Monday afternoon at one of the city's most notorious intersections. Emergency crews were called to the corner of Kenaston and McGillivray Boulevard for what appeared to be a two-vehicle crash. A light standard was seen sitting atop the police cruiser in the southbound lane of Kenaston. Front and side airbags were deployed. A van ended up in the westbound lane of McGillivray. No word yet on injuries. The intersection was highlighted eariler this year as having the second highest number of collisions in the city with 2,298 crashes between 2005 and 2014. Winnipeg Free Press; CTV News; CBC News

La Presse says Montreal police tracked journalist's iPhone for months
A Montreal journalist says he was furious when he learned that city police monitored his iPhone for months in order to find out who he was speaking with… The French-language newspaper reported it has learned at least 24 surveillance warrants were issued for Lagace's phone this year at the request of the police's special investigations unit. That section is responsible for looking into crime within the police force. Three of those warrants reportedly authorized police to get the phone numbers for all Lagace's incoming and outgoing texts and calls, while another allowed them to track the phone's location via its GPS chip. Lagace said police told him they obtained the court-issued warrants because they believed the target of one of their investigations was feeding him information. But he said the story in question was actually first reported on by a competitor, leading him to believe the investigation was actually a thinly veiled attempt to learn the identity of his sources within the police department… Reaction to La Presse's story was swift, with some unions and media organizations denouncing the police operation, and some opposition city councillors calling for Montreal's police chief to step aside while the matter is investigated. Canadian Press (Globe and Mail; CTV News; Herald News; Metro News); Montreal Gazette; Postmedia Network (Toronto Star)

Broadcast Media / Médias télédiffusés :

CTV News discussed the monitoring of Patrick Lagace's emails and phone calls by the Montreal Police as well as reactions to the revelation by the SPVP, Montreal City Councilors, the Minister of Public Security of Quebec, and the general public (CTV News, 18:15 ET, 19:15 ET)

Le chef du SPVM n'exclut pas que d'autres journalistes aient été placés sous surveillance
Le chef de police Philippe Pichet a pris la parole à 16 h 30 au quartier général du SPVM pour réagir à l'onde de choc créée par la mise sous surveillance du téléphone cellulaire de Patrick Lagacé. Le chef du SPVM a déclaré qu'il n'était pas insensible à l'affaire. «Cette enquête visait un de nos policiers et non Patrick Lagacé. C'est une situation qui a été traitée avec des moyens exceptionnels. Quand j'ai appris qu'un mandat a été demandé, je me suis assuré que nous respections toutes les règles», a-t-il dit. «Nous avons suivi les règles et le juge a autorisé le mandat», a-t-il rappelé. «Le SPVM reconnaît la liberté d'expression.» Répondant à la question d'un journaliste, il a précisé qu'il ne pouvait dire si d'autres journalistes ont été placés sous surveillance. Des vérifications à ce sujet sont en cours… Le ministre québécois de la Sécurité publique, Martin Coiteux, s'est dit «renversé» par ces révélations. La Presse; Radio Canada; CTV News

We're spied on more often than you think, journalists groups say
Canadians may be used to hearing about police tapping journalists' phones in China, or tailing them down the street in Turkey. But in Montreal, Canada? Unfortunately, say organizations like Canadian Journalists for Free Expression, it is happening a lot more than we think. "It's something we've been suspecting for a long time – that when this kind of power is in the hands of the police they will abuse it," said Tom Henheffer, executive director of CJFE. "I used to be cautious about drawing parallels with Canada and dictatorships like Turkey, China, Russia or Egypt. But the difference has started to erode, especially when it comes to privacy rights"... Montreal Gazette

Les pratiques du SPVM inquiètent Edward Snowden
Le lanceur d'alerte Edward Snowden, qui a mis à jour les activités de surveillance de masse de la NSA aux États-Unis, s'inquiète des pratiques du SPVM qui a espionné le journaliste de *La Presse* Patrick Lagacé. Dans un message publié sur le réseau social Twitter, Edward Snowden qui a fui en Russie par crainte des représailles dénonce la surveillance des journalistes en prenant l'exemple du journaliste de *La Presse*. «Êtes-vous un journaliste ? Le fait que la police vous espionne pour identifier vos sources n'est pas hypothétique. Ça se passe aujourd'hui», a écrit l'homme. Son message est accompagné d'un lien vers un article du quotidien montréalais *The Gazette* sur la surveillance dont le chroniqueur a été la cible le printemps dernier. La Presse

Lagacé espionné: «inacceptable», «troublant», réagit la classe politique
Pour le chef péquiste Jean-François Lisée, l'espionnage du journaliste de La Presse, Patrick Lagacé par la police de Montréal est « inacceptable » et devrait « cesser immédiatement ». Les révélations de La Presse laissent le chef péquiste « complètement outré », a-t-il dit dans une entrevue à 98,5 ce matin. « Le travail du journaliste fait partie de la démocratie, lance sans détour, Lisée, lui-même ancien journaliste. C'est un genre de soupape pour que des informations qui devraient circuler, mais ne circulent pas, puissent arriver aux lecteurs, aux citoyens, et même aux élus ». « Qu'un journaliste ait été sous enquête, que son téléphone ait été vu, qu'il ait été géolocalisé alors que la Cour suprême disait récemment que cela devrait être réservé à des cas exceptionnels - et c'est encore trop - que l'Assemblée nationale ait unanimement réprouvé en septembre dernier la saisie de l'ordinateur du journaliste du Journal de Montréal Michael Nguyen, que la police continue de tenter d'avoir des sources du côté des journalistes, c'est inacceptable. Il faut mettre un holà à ça ». La Presse

Spying on Montreal reporter an attack on free press
An opinion piece states, "For the second time in two months, a journalist reporting on matters related to the justice system has found his own rights egregiously compromised. These affronts to freedom of the press are deeply troubling. Starting last January, Montreal police spied on La Presse columnist Patrick Lagacé through his cellphone, obtaining his call records and tracking his movements, as part of what police said was an internal probe of anti-gang squad officers later charged with fabricating evidence. This is an outrageous violation of Lagacé's privacy and an attack on his role as a journalist in a democratic society. He was never a target of the probe nor suspected of any wrongdoing. And he was never even given an opportunity to safeguard his contacts from police scrutiny. In September, Journal de Montréal reporter Michaël Nguyen had his computer seized by the Sûreté du Québec after reporting on two judges under investigation by the Conseil de la magistrature... Police must be held to account for these heavy-handed tactics. But the judges and justices of the peace who signed off the police warrants have much to answer for, too..." Postmedia Network (Montreal Gazette); Globe and Mail

RCMP mourns one of its own
Insp. Tony Perry was found dead Friday morning in Happy-Valley-Goose Bay. Perry, who is originally from Deer Lake, joined the RCMP in 1988 and served in Nova Scotia until July 2015, when he was transferred to Newfoundland and Labrador. Most recently, Perry worked as a negotiator between police, aboriginal leaders and protesters at the Muskrat Falls hydroelectric project site. Foul play is not suspected. Western Star

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Pepper spray use with little accountability concerns prison watchdog
Canada's prison watchdog is raising red flags about the "go-to" use of pepper spray in federal penitentiaries, which his office found has tripled in a five-year period with little accountability. In his annual report tabled in Parliament Monday, Correctional Investigator Howard Sapers said pepper spray was used in 60 per cent of the 1,833 use-of-force incidents in 2015-2016. "The link between institutional safety and the increasing use and reliance on inflammatory agents is tenuous at best," said Sapers. The correctional investigator partly blamed the increase on a policy change back in September 2010 that allowed correctional officers to carry pepper spray canisters on their belts. Before then the chemical, which makes it hard to breath and see, was locked up. His report notes that there hasn't been a correlating increase in the severity of security incidents or threats to justify the increased use pepper spray. Sapers also called out what he termed a lack of monitoring and national oversight of how pepper spray is stored, weighed, inspected, assigned and controlled. CBC News; La Presse Canadienne (L'actualité)

Broadcast Media / Médias télédiffusés :

CTV News' Power Play interviewed Correctional Investigator Howard Sapers on the Correctional Investigator's 2015-2016 Annual Report and the use of pepper spray in federal penitentiaries. Rough Transcript (2016-10-31)

The Number of Female Indigenous Prisoners in Canada Has Doubled in the Last Decade
The number of Indigenous people now represent more than a quarter of all inmates held in Canada's federal prisons, according to the new annual report from Canada's prison watchdog. And within the last decade, the number of female Indigenous inmates has doubled, while the population of male Indigenous inmates has increased by more than 50 percent. During that time, the federal inmate population increased by only 10 percent. "It's a shameful milestone in Canadian history," correctional investigator Howard Sapers told a press conference on Monday. His annual report, which also says Indigenous women represent 35 percent of inmates in federal prisons, serves to highlight his concerns about federal correctional facilities, which house offenders who have been sentenced to more than two years in prison... In addition to decrying the increase in Indigenous offenders, his report also sounds the alarm over a dramatic increase in guards using "inflammatory agents" such as pepper spray against inmates. The number of incidents involving the use of pepper spray against inmates has more than tripled since 2011, and more than one-third of those incidents involved inmates suffering from mental illnesses. Vice News

Ontario premier calls inmate's 52-month segregation 'extremely disturbing'
The treatment of an inmate held in segregation for four years is "extremely disturbing," Ontario Premier Kathleen Wynne said Monday, but she declined to call it torture... Federal correctional investigator Howard Sapers called Capay's case "troubling," and said he had never before heard of someone being kept in such conditions. There have been cases, however, in the federal system in which offenders are kept in segregation for years, he said. "Until we have a legislated cap, I'm very concerned that long-term segregation and segregation that could go on almost indefinitely is still possible," Sapers said in Ottawa. Canadian Press (CTV News)

Dangerous offender status sought for man
It's been a long time coming, but the office of Kingston's Crown attorney is applying to seek a dangerous offender designation for a 39-year-old sexual predator initially sent to prison in 2004 for drugging and raping three women in North Bay between 1999 and 2002. The decision follows Rene R. Bourdon's convictions in Kingston's Superior Court on two new counts of sexual assault in the Kingston area; eight violations of the long-term supervision order imposed on him 12 years ago at his original sentencing; and fraudulent personation in the service of a sex scheme of Rube Goldberg complexity... In the first nine months following his release in November 2005, however, his release was suspended four times for violating conditions of the LTSO and he was shunted between all three (at that time) Ontario federal halfway houses directly operated by Correctional Service Canada. Known as community correctional centres, they're the the only halfway houses in the system that can't refuse to accept high-risk offenders... The Whig

St. Lawrence Parks Commission would like to continue Kingston Penitentiary tours
The prison that was once off-limits to most people has just completed its first full tourist season. Public tours of Kingston Penitentiary brought in thousands of visitors and millions of dollars over the past 5 months — making it Kingston's top attraction. The final "sold-out" tours concluded this weekend. The question now — will the once-notorious maximum security prison re-open next year? CKWS Kingston

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Vancouver Coastal Health applies for 2 more supervised injection sites
Vancouver Coastal Health (VCH) has submitted applications to Health Canada to open two new supervised injection sites in Vancouver in the midst of an overdose crisis. The proposed supervised injection sites are located at the Downtown Eastside Mental Health and Substance Use Drop-In Centre (528 Powell Street) and the Heatley Integrated Health Centre (330 Heatley Street). "The evidence is clear that supervised consumption services reduce transmision of diseases and help to connect peopel to healthcare services," said B.C. Health Minister Terry Lake. "In the face of the current public health emergency, what is even more critical is the fact that more than three million injections have been done at Insite in the last 13 years and not one person has died of an overdose there." Insite, Canada's first supervised injection site, was opened in 2003 in Vancouver's Downtown Eastside. Metro News; CBC News

Vehicle seizures, extended zero tolerance as Saskatchewan tackles drunk driving
Proposed changes to impaired driving laws in Saskatchewan are being called a good first step by grieving families of people killed by drunk drivers. The changes include a three-day vehicle seizure for drivers who are charged for the first time with having a blood alcohol content over .04 and an extended a zero tolerance policy to all drivers under the age of 21. If passed, the new law would also extend mandatory ignition interlock durations for repeat drunk drivers and apply to those who refuse to provide a breath sample... The changes will take effect Jan. 1, if approved by the legislature. Canadian Press (Brandon Sun); Postmedia Network (Star Phoenix)

How North America Found Itself in the Grips of an Opioid Crisis
The story of today's prescription opioid overdose crisis didn't start this year, or ten years ago, or even 100 years ago. It starts with a plant—the opium poppy—that has been a part of human civilization for thousands of years... But how did we get here? The answer is a cautionary tale about the power of Big Pharma, the unintended consequences of government intervention, and the tenacity of drug markets. Vice News

Opioid overdose treatment kit requires training before use, but available soon
Government-funded kits announced this summer that will contain the antidote for the deadly drug Fentanyl and other opioid overdoses aren't on the streets yet... While there's no specific timeline, provincial officials are still promising a fall launch. The province announced funding for the Naloxone take-home kits in late August. According to the Department of Health, within days of that announcement, it struck a working group -- addictions experts, representatives of regional health authorities, government and the Aids Committee of Newfoundland and Labrador -- that has been meeting regularly. People who take the kit home have to be trained on its use and just last week, a train-the- trainer program got started. Telegram

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Medical marijuana industry budding in Lachute
Medical marijuana is a growing industry in Canada. Doctors are increasingly prescribing marijuana to treat everything from cancer to back pain. There are currently 36 licensed medical marijuana facilities in the country, including 21 in Ontario. Two new facilities are expected to be opening in Lachute, one as early as next spring. Quebec currently has only one licensed facility, owned and operated by Gatineau-based Hydropothecary. After the city began the consultation process to rezone a section of the city for specific use by medical marijuana facilities, Lachute Mayor Carl Péloquin told The Review it received dozens of inquiries from interested companies. "I thought that it would be good to be ready and to have the right zoning, since it's now considered an acceptable therapy," said Péloquin. Council initially looked at the possibility of rezoning an industrial sector on Cristini Boulevard, but rejected the plan after nearly a dozen of the existing industries objected. After evaluating their options, Péloquin said council chose to begin the consultation process to rezone the area surrounding the Régie Intermunicipale Argenteuil Deux-Montagnes garbage dump, which is located on Chemin des Sources. The Review

PUBLIC SERVICE / FONCTION PUBLIQUE

Government misses Halloween deadline to clear Phoenix backlog
Public Services and Procurement Canada has missed its promised Halloween deadline to clear the backlog of pay problems caused by the Phoenix pay system, as the cases of 22,000 public servants remain unresolved, the department's top bureaucrat says. Deputy minister Marie Lemay said the department couldn't meet the self-imposed Oct. 31 target because the remaining cases are older and much more complicated than the front end of the pile and require much more work than expected. Lemay said she is disappointed the deadline was missed but that the department did everything it could. Ottawa Citizen

OTHER / AUTRES

NIL

INTERNATIONAL

Dakota Access pipeline protests: UN group investigates human rights abuses
A United Nations group is investigating allegations of human rights abuses by North Dakota law enforcement against Native American protesters, with indigenous leaders testifying about "acts of war" they observed during mass arrests at an oil pipeline protest. A representative of the UN's permanent forum on indigenous issues, an advisory group, has been collecting testimony from Dakota Access pipeline protesters who have raised concerns about excessive force, unlawful arrests and mistreatment in jail where some activists have been held in cages. Guardian (UK)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

canadaCJFE
Today @MattDube and @RalphGoodale debated #SPVM @kick1972 and #VICE @BMakuch cases. @snowden #ProtectPressFreedom http://bit.ly/2fxQYup

https://twitter.com/VincentBP
Affaire Lagacé: le ministre fédéral Ralph Goodale prêt « à avoir une discussion sérieuse » sur les règles policières http://www.lapresse.ca/actualites/justice-et-affaires-criminelles/201610/31/01-5036264-affaire-lagace-goodale-pret-pour-une-discussion-serieuse-sur-les-regles-policieres.php ...

davidakin
"We take freedom of the press very, very, very seriously" @RalphGoodale says without condemning cops who spy on cops.

davidakin
And here's @RalphGoodale reading a statement on what happens when "journalism and investigations intercept".

rachaiello
"We take the freedom of the press in this country very, very seriously," Min. @RalphGoodale says just now in the #HoC #pressfreedom #cdnpoli

Colinfreeze
3. The #cdnpoli powers are important because @RalphGoodale is consulting Canadians on whether cops need more powers. https://www.publicsafety.gc.ca/cnt/rsrcs/pblc

RalphGoodale
Happy Halloween! Wishing everyone a fun and safe evening of trick or treating!

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

jonmeyer_980
#NathanEStewart report. Wildlife team monitoring pod of orcas en route to Balagny Psg, and humpback whale sightings. #Heiltsuk #bellabella

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Safety_Canada
Participating in our Twitter Chat on Nat'l Security Accountability on Thursday? Check this out #YourNatlSec http://ow.ly/4O86305HX89

Securite_Canada
Vous participez à notre conv. Twitter sur responsabilité en matière de sécurité nat. jeudi? Consultez #VotreSecNat http://ow.ly/F0b5305HXbn

NATIONAL SECURITY / SÉCURITÉ NATIONALE

OttawaCitizen
Ottawa terror suspect granted bail again after allegedly breaching conditions http://ow.ly/Dzzi305HWrT

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

MichelleZilio
2017 immigration total target remains unchanged from last year. 300,000 total: http://news.gc.ca/web/article-en.do?mthd=index&crtr.page=1&nid=1145319 … #cdnpoli #cdnimm

RosieBarton
Macallum: economic immigrants goes from 160,600 in 2016 to 172,500 in 2017. #hw

CYBER SECURITY / CYBERSÉCURITÉ

cyber_securite
Les enfants ne sont pas seuls à se déguiser à l'#Halloween! Sachez détecter la fraude : http://www.pensezcybersecurite.gc.ca/cnt/rsks/scms-frd/index-fr.aspx …

GetCyberSafe
How can #cybercrime affect Canada's critical infrastructure? Find out on our blog: https://www.getcybersafe.gc.ca/cnt/blg/pst-20161031-en.aspx … #CSAM

LAW ENFORCEMENT / APPLICATION DE LA LOI

RCMPAlberta
D/Commr. Ryan accepted a medallion on behalf of RCMP employees who assisted in the #YMMFire. http://rcmp.ca/-gSr

VGaudreau
Le chef du @SPVM n'exclut pas que d'autres journalistes aient été placés sous surveillance http://www.lapresse.ca/actualites/justice-et-affaires-criminelles/201610/31/01-5036220-le-chef-du-spvm-nexclut-pas-que-dautres-journalistes-aient-ete-places-sous-surveillance.php … @fpjq #fpjq @kick1972

Colinfreeze
Cops got warrants to spy on journalist "using the GPS chip in his iPhone & to obtain the IDs of everyone he has spoken and messaged with." https://twitter.com/CBCCanada/status/793157452321685505

Colinfreeze
7. CanLIi indicates real-time GPS tracking of iPhones still a novel power for #cdnpoli police.Dunno of any parallels https://www.canlii.org/en/#search/text=GPS%20and%20real-time%20and%20%20tracking …

georgiastraight
The irresistible allure of a Hells Angels funeral and the cost of the war on drugs http://ow.ly/u6yW305Hypw #HellsAngels #drugs

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

CTV_PowerPlay
Federal correctional Investigator Howard Sapers is here to share the findings of a new report. #cdnpoli #ctvpp

alisoncrawford5
Sapers points out that RCMP use of force and pepper has gone down just as correctional officers use it more often. #hw

alisoncrawford5
Sapers says police services account for their use of force and pepper spray and Correctional Service Canada must do the same. #hw

alisoncrawford5
Sapers says lack of oversight, insufficient video footage, little documentation, makes it hard to see if pepper spray is used appropriately

alisoncrawford5
Sapers says pepper spray was used in 54% of use of force incidents when offenders were harming themselves. He says hardly therapeutic.

alisoncrawford5
Sapers says correctional officers often not following the rules for checking inmates' health after using pepper spray. #hw

alisoncrawford5
Sapers says 40% of use of force incidents at CSC psychiatric hospitals involved pepper spray. #hw

l_stone
Sapers says he's never heard of a similar case to Adam Capay - an inmate held in acrylic glass cell under artificial light for 24 hrs a day

l_stone
Since March 2005, aboriginal inmate population increased by 52%. Sapers again recommends a deputy commish for indigenous corrections

alisoncrawford5
Sapers says the increase is linked to pepper spray now being on officers' belts and not locked in designated control posts. #hw

alisoncrawford5
MOre than 1/3 of all use of force incidents in fed prisons involved inmates with mental health issues identified by CSC #hw

l_stone
Security incidents involving pepper spray in federal prisons have tripled since 2011/12, new report from Correctional Investigator says

l_stone
Correctional Investigator Howard Sapers speaks now about his annual report - special focus on use of pepper spray

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

VICE
How North America found itself in the grips of an opioid crisis: http://bit.ly/2fo491J

PUBLIC SERVICE / FONCTION PUBLIQUE

AshleyBurkeCBC
Correction: $500,000 is the estimated operating cost for the gov't office that handles claims for workers' out-of-pocket expenses #Phoenix

CBCTheNational
Phoenix deadline arrives, but pay problems continue for thousands of public servants http://www.cbc.ca/1.3826399

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

Today's News / Actualités
November 2, 2016 / le 2 novembre 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Surveillance de journalistes : mutisme à la GRC et au SCRS
Alors que la SQ et la Ville de Montréal ont confirmé avoir mis des journalistes sous surveillance, la GRC et le SCRS, les deux corps policiers fédéraux, ne veulent pas confirmer s'ils ont déjà adopté de telles pratiques, et le cas échéant à quelle fréquence. La GRC précise seulement que «les cas où des enquêtes de la GRC concernant des journalistes ont eu lieu sont extrêmement rares». Le commissaire de la GRC Bob Paulson a dit mercredi «ne pas être au courant que nous avons des enquêtes actives ou de la surveillance à l'égard de journalistes», mais la GRC n'a pas voulu confirmer si des journalistes ont été

surveillés dans le cadre de ses enquêtes.... Tout en précisant «reconnaître» et «respecter [...] l'importance de la liberté et de l'indépendance de la presse», la Gendarmerie royale du Canada (GRC) a indiqué ne pas pouvoir commenter «l'existence d'enquêtes en cours» ou «discuter des détails opérationnels» d'enquêtes passées. La GRC n'a pas précisé à *La Presse* si elle effectuait, comme l'a fait la Sûreté du Québec cette semaine, un examen de ses enquêtes pour déterminer si des journalistes ont été mis sous surveillance... Le Service canadien de renseignement de sécurité (SCRS) n'a pas répondu aux questions de *La Presse* à savoir si l'organisme fédéral responsable des enquêtes de sécurité nationale : 1) surveille actuellement des journalistes, 2) en a surveillé par le passé, 3) mène actuellement des démarches pour répondre à ces questions et a l'intention de rendre public le résultat de ces démarches. De son côté, le gouvernement Trudeau n'a pas l'intention de demander à la GRC et au SCRS de divulguer de telles informations, estimant qu'il n'était «pas approprié de commenter sur les questions opérationnelles». ***«Bob Paulson, commissaire de la GRC, a confirmé qu'aucun journaliste ne fait actuellement l'objet d'une surveillance par la GRC. Le ministre Goodale examine la Directive ministérielle sur les enquêtes dans les secteurs sensibles existante afin de s'assurer que les plus grands soins sont pris lorsque des enquêtes criminelles et du journalisme se recoupent et que la valeur canadienne fondamentale de la liberté de presse est protégée. Il est toujours ouvert à recevoir des représentations sur ce qu'il y a d'autre à faire pour protéger les libertés fondamentales de la presse»,* indique Scott Bardsley, attaché de presse du ministre fédéral de la Sécurité publique Ralph Goodale.** La Presse

Senator André Pratte urges stronger protection for reporters, sources
Independent senator and former journalist Andre Pratte wants the Liberal government to look seriously at beefing up protection for reporters and their sources. Pratte says if the government shows no interest, he'll pursue the idea himself. It is "quite worrisome" that Montreal police obtained warrants to monitor one of his former colleagues, La Presse columnist Patrick Lagace, Pratte said Wednesday in an interview... **Public Safety Minister Ralph Goodale says the Supreme Court of Canada has already explicitly laid out the test that must be satisfied when police investigations intersect with media freedoms...** Despite his apparent reluctance to revisit the existing regime, **Goodale left the door open a crack*. "If there are those in the federation of journalists or others who have recommendations to make about how this can be more abundantly emphasized, I would certainly be glad to receive their recommendations,"* he said Tuesday. Pratte said he would contact the Liberal government for a direct answer about whether it will consider a new law.** Canadian Press (Globe and Mail; Metro News; Toronto Star)

Deltell wonders if he was monitored in Lagacé surveillance case
Conservative finance critic and former television journalist Gerard Deltell said he's "shocked" by revelations that police were monitoring La Presse journalist Patrick Lagacé's iPhone and thinks there's merit in starting a discussion on whether the laws protecting journalists and their sources are sufficient... But there don't seem to be immediate signs of cabinet interest in revisiting the laws. Public Safety Minister Ralph Goodale said yesterday the Supreme Court has already, in a "very clear ruling," laid out the conditions for how to proceed when police investigations run up against freedom of the press. The NDP's line of attack has been to pressure the federal government to say how many journalists are now being monitored**. Goodale said today that question has to be answered by the RCMP, and that Commissioner Bob Paulson's answer was "no." *"There are no such investigations to the best of his knowledge and he would certainly know,"* Goodale said**. Yesterday, Paulson told reporters he's "not aware that we have any ongoing investigations or surveillance activity against journalists." The RCMP also said it wouldn't provide details for "security reasons." iPolitics

Trudeau promet de «faire ce qui est nécessaire» pour la liberté de la presse
Le premier ministre Justin Trudeau promet que son gouvernement « va faire ce qui est nécessaire » pour défendre la liberté de la presse, a-t-il indiqué ce matin en rapport avec l'affaire Patrick Lagacé, dont le téléphone portable a été surveillé pendant six mois par le Service de police de la Ville de Montréal. « La préoccupation que nous avons tous par rapport à la protection de la liberté d'expression, la liberté de la presse, est soulignée par ce qui vient juste de se passer. On va regarder attentivement les conversations qui vont avoir lieu entre l'hôtel de ville de Montréal et les Services de police de Montréal, mais certainement, comme on a dit plusieurs fois, ce gouvernement est à la défense de la liberté de la presse

et on va faire ce qui est nécessaire pour l'encadrer s'il y a d'autres étapes nécessaires », a dit le premier ministre Trudeau à l'entrée du caucus libéral à la Chambre des communes. Le gouvernement Trudeau a annoncé mardi entreprendre un « examen » de la directive ministérielle de 2003 demandant aux forces policières de porter une « attention spéciale » au statut des médias dans le cadre d'enquêtes sur la sécurité nationale. Le cabinet du **ministre Goodale** n'était pas en mesure d'indiquer si cet « examen » comprendrait des consultations publiques... Le Nouveau Parti démocratique demande une enquête publique sur la question, tandis que les conservateurs veulent que le **ministre Goodale** fasse un examen de la situation et fasse s'expliquer en comité parlementaire... Le **ministre Goodale** n'a pas voulu indiquer mardi, en réponse à une question du chef néo-démocrate Thomas Mulcair à la Chambre des communes, si la Gendarmerie royale du Canada (GRC) ou le Service canadien du renseignement de sécurité (SCRS) espionnent actuellement des journalistes. Le commissaire de la GRC Bob Paulson a indiqué mardi « ne pas être au courant que nous avons des enquêtes actives ou de la surveillance à l'égard de journalistes ». **Le cabinet du ministre Goodale estime qu'il *« n'est pas convenable que le ministre formule des commentaires sur les enquêtes en cours ».*** La GRC est actuellement devant les tribunaux afin d'obtenir du matériel journalistique d'un journaliste de VICE au sujet d'un présumé terroriste. En 2007 et en 2008, la GRC avait aussi autorisé la filature du journaliste de La Presse Joël-Denis Bellavance. ***« C'était un cas clair où les règles en vigueur n'ont pas été suivies [par la GRC] »,* disait le ministre Goodale en entrevue plus tôt cette semaine.** La Presse

La protection des sources journalistiques rebondit jusqu'à Ottawa
Alors que Justin Trudeau promet de faire le «nécessaire» pour défendre la liberté de presse, Thomas Mulcair demande la tenue d'une enquête fédérale... Le chef sortant du NPD, Thomas Mulcair, n'est pour sa part pas rassuré par la situation et exige la tenue d'une enquête au niveau fédéral pour s'assurer que les journalistes ne fassent pas l'objet d'une surveillance similaire de la part de la GRC. «Au Canada, en ce moment, il y a combien de journalistes qui sont surveillés soit par la GRC, soit par le SCRS? M. Goodale connaît la réponse. Il a refusé de répondre hier (mardi) et il n'a certainement pas répondu qu'il n'y en avait pas, donc il y en a. Alors moi, je m'attends à ce que Justin Trudeau tire ça au clair. C'est son obligation», a-t-il suggéré. **Le ministre fédéral de la Sécurité publique, Ralph Goodale, a indiqué qu'une directive ministérielle datant de 2003, visant à protéger certains secteurs incluant les médias ferait l'objet d'une révision. *«Ce que j'ai entrepris, c'est de m'assurer que toutes les directives émises par le ministre de la Sécurité publique répondent aux buts auxquels elles devaient répondre»,* a-t-il fait valoir. Le ministre a ajouté que le commissaire de la GRC, Bob Paulson, avait indiqué mardi ne pas être au courant de cas de journalistes qui feraient actuellement l'objet d'une telle surveillance.** Agence QMI (Journal de Quebec; Journal de Montreal)

TOP STORIES / MANCHETTES

La SQ confirme que les appels téléphoniques de six journalistes ont été ciblés
La Sûreté du Québec a confirmé, mercredi, qu'elle a enquêté sur les activités de six journalistes il y a trois ans. Le capitaine Guy Lapointe a affirmé que l'enquête portait sur la révélation de contenu d'écoutes électroniques. M. Lapointe a expliqué que la SQ a déclenché cette enquête à la suite d'allégations que des journalistes ou d'autres personnes avaient divulgué de telles informations. Le directeur général de la SQ, Martin Prud'homme, en poste depuis deux ans, a obtenu ces informations concernant un seul dossier au cours des dernières 20 années, a indiqué le porte-parole. Selon M. Lapointe, la SQ a obtenu une ordonnance en 2013 pour consulter les registres d'appels entrants et sortants de six journalistes. Cette procédure ne prévoyait aucune écoute électronique ni surveillance par géolocalisation des personnes visées, que la SQ n'a pas voulu identifier, mercredi. Par ailleurs, M. Prud'homme a réclamé mercredi au ministère de la Sécurité publique qu'une enquête soit effectuée par «un tiers indépendant» afin d'examiner le recours à cette méthode dans le cas de journalistes. M. Lapointe n'a pas précisé si ce mandat devrait être confié au Bureau des enquêtes indépendantes, comme le réclame le Parti québécois depuis des révélations qui concernent la police montréalaise cette semaine... Les journalistes de Radio-Canada Marie-Maude Denis, Isabelle Richer et Alain Gravel sont parmi les cibles de la SQ, tout comme Denis Lessard, de La Presse, et Éric Thibault, du Journal de Montréal. La Presse Canadienne (Le Soleil); Postmedia Network (National Post); Agence QMI (Journal de Québec; Journal de Montréal); Radio

Canada; La Presse; CBC News; Canadian Press (Metro News; Times Colonist; Winnipeg Free Press); Montreal Gazette

Immigration detainee hunger strike in Ontario jail goes into third week
A group of immigration detainees at the Central East Correctional Centre (CECC) in Lindsay, Ontario, have been on a hunger strike for over two weeks to protest Canada's immigration detention system, says a migrants' rights advocacy group. Eighteen immigration detainees at the maximum security provincial prison located about 125 km northeast of Toronto began refusing meals on Oct. 17 to demand legislative changes to federal immigration rules that allow Canadian authorities to detain certain immigrants for an indefinite period, said Macdonald Scott, an immigration consultant with the Toronto law firm Carranza LLP. On Wednesday, only four detainees were able to continue the protest, the third such hunger strike by immigration detainees this year, Scott said. "They are fighting for the same demands, the main one being the presumptive period, that they be released after 90 days if they are not deported," Scott said... The detainees are also asking for a one-on-one meeting with federal **Public Safety Minister Ralph Goodale** to discuss the issue with him, he said. RCI

RCMP were afraid to let officers testify at inquest of Nunavut man shot by police
New details emerged into how a 30-year-old man was shot by RCMP at his own home as a coroner's inquest got underway in Igloolik, Nunavut, Tuesday — including the fact the RCMP was afraid to let its officers testify in person. On March 20, 2012, two RCMP officers went to the home of Felix Taqqaugaq after getting a call from someone in the community who became concerned after hearing Taqqaugaq ranting on the community's local radio station. Taqqaugaq had schizophrenia and was being treated for mental health issues, according to the coroner's facts. On the night he died, the officers met with him briefly on his porch before Taqqaugaq went inside, returned with a knife, and was shot three times. This week's inquest, led by Nunavut's chief coroner Padma Suramala, will shed more light on the events surrounding his death and the subsequent investigation by the Ottawa Police Service. On Tuesday, the coroner's jury was selected, but it's still not clear how exactly the process will unfold, and how exactly the officers involved will take part. CBC News

Why Adam Capay has spent 1,560 days in solitary
Renu Mandhane spent part of her day on Oct. 7 at the Indigenous friendship centre located on the outskirts of Thunder Bay, Ont. Mandhane, 39, is chief commissioner of the Ontario Human Rights Commission (OHCR), the 55-year-old body charged with preventing discrimination and advancing human rights in Ontario. Her office had organized the meeting with Indigenous leaders and community members to talk about discrimination and racial profiling. After the meeting was over, Mandhane organized an impromptu tour of the Thunder Bay Jail, a 170-bed facility built in 1926. "It's a s–thole," says Mike Lundy, a union president and a correctional officer at the jail... According to Ontario's Correctional Services, inmates are placed in administrative segregation when they are in need of protection, pose a threat to the health and safety of themselves or others, or are alleged to have committed a serious misconduct. "In Canada, we do not practise solitary confinement," a Public Safety Canada official, Kimberley Lavoie, told a UN meeting in Geneva on Oct. 25, a week after Mandhane revealed Capay's plight... Yet as Kimberley Savoie reinforced to the UN, Canada is adamant it doesn't practise solitary confinement. "Please note that the term 'solitary confinement' is not accurate or applicable within the Canadian penitentiary system," says Correctional Services Canada spokesperson Avely Serin. Canada does, however, practise "administrative segregation." "It is the separation, when specific legal requirements are met, of an inmate from other inmates," explains Serin. The difference between the two is often lost on government... Capay's case speaks to another troubling trend in Canadian prisons: Indigenous offenders serve much harder time than anyone else... "There is a group in Canada that keeps mysteriously dying,'" says University of Toronto sociology professor Sherene Razack. Many of these deaths occur because officials "will not touch, examine, or closely monitor Indigenous people in their care," Razack says. "This indifference kills." Adam Capay's treatment has drawn condemnation from all corners—including the very people responsible for his care. Maclean's

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

B.C. announces first step in province-wide earthquake warning system
Earthquake technology saves lives. Japan has it, the U.S is working on it, and now B.C. is beginning the process to get it in place — a province-wide earthquake early warning system. The province of B.C. has issued a formal request for expressions of interest on an earthquake early warning and seismic monitoring program. It's the first step to gain a better understanding of what sensors and networks are already in place, and what groups are interested in — and have the capacity to implement — the program. CBC News

Windsor floods cause close to $108 million in insured damage
Flooding, which impacted the Windsor at the end of September, has resulted in almost $108 million in damages, according to the Insurance Bureau of Canada. "Flood events are happening across Canada with more frequency and with greater severity," said Kim Donaldson, the bureau's vice-president in Ontario. "It is important that Canadians understand their insurance policies and that they know what's covered before bad weather strikes." Over 6,000 home, auto, and business claims were filed with insurers following the flood, the bureau said in a statement released Wednesday morning. Postmedia Network (Windsor Star)

L'état des brise-glaces de la Garde côtière compromet le commerce sur le Saint-Laurent
Le géant Rio Tinto et d'autres grands joueurs de l'économie demandent l'intervention d'Ottawa pour prévenir une crise. Des centaines de millions de dollars sont en jeu. Et la situation ne peut que s'aggraver révèle une enquête de Radio-Canada. Quelque 120 navires par année franchissent le Saint-Laurent avant d'emprunter le Saguenay pour alimenter en matières premières les alumineries de Rio Tinto. Or, plusieurs sont déjà restés prisonniers des glaces pour une simple raison : le manque de disponibilité de brise-glaces de la Garde côtière canadienne (GCC). Tout un couloir commercial stratégique deviendra vulnérable au cours des prochains mois. Radio Canada

Cost of storm-surge barrier for False Creek dampens enthusiasm
The City of Vancouver's idea to build a storm-surge barrier in False Creek to protect against future flooding could come with a price tag of as much as $800 million, city staff told councillors Wednesday. In anticipation of rising sea levels over the next century, staff have come up with a range of options to protect low-lying areas of the city. But the estimated costs of the options are so significant that the mayor asked staff to examine the idea of legal action against major carbon-emitters, including companies in the oil and gas industry. Province

Search underway for missing hunting guide
Police in the Bay St. George area of Newfoundland are searching for a missing hunting guide who was separated from his party on Tuesday. RCMP were called at 2:15 p.m. about a man lost in moose management area 11, near the community of Jeffrey's. The guide was separated from his hunting party on Tuesday afternoon and hasn't been seen or heard from since... The Barachois Brook Search and Rescue Team are working to find the man. RCMP are also trying to get a helicopter to do an air search. CBC News; Gulf News; VOCM

Albertans bring Christmas cheer by the truckload to Fort McMurray
Christmas has come early to Fort McMurray, in boxes, as a truckload of donated Christmas decorations arrived at Shell Place Tuesday for distribution to residents affected by the wildfire. Municipal employees and volunteers unloaded the truck when it arrived yesterday afternoon, laying out the boxes of ornaments in the Diamond Ballroom at Shell Place. The province-wide donation campaign was organized by High River residents Helga and Terry Lempriere, whose house was badly damaged in the 2013 High River flood. Fort McMurray Today

Camp and catering firm blames poor results on slow recovery from Fort McMurray fire
A company that operates workcamps for the oilsands industry in northern Alberta says demand for its services has been weaker than expected over the summer in the wake of the Fort McMurray wildfire. CBC News

Bill aims to reduce human element from wildfires

Debate continues in the Alberta Legislature on major amendments proposed to the Forest and Prairie Protection Act that, among other things, will substantially increase penalties to those who cause forest fires. Bill 24, co-sponsored by Banff-Cochrane MLA Cam Westhead, calls for increasing fines to a maximum of $50,000 for individuals responsible for wildfires and up to $500,000 for corporations found responsible for the same. Both offences currently carry a maximum penalty of $5,000. The bill also gives clarifies processes, role and responsibilities of the Agriculture and Forestry ministry and forestry officials in making decisions that aim to reduce the threat of wildfire and stop action that interferes with firefighting. Cochrane Times

Red Cross brings mobile disaster response unit to Courtenay
It may only look like a truck and trailer, but what is inside a new Canadian Red Cross mobile unit can significantly help a community in a time of need. This week, one of four mobile units made its way across the Island, and stopped in Courtenay Tuesday at the Red Cross office to bring awareness to what the unit can offer if a disaster - flood, fire, earthquake or other - should strike... There will be four units across B.C. and the Yukon, and Harvey said he hopes to see one on Vancouver Island soon. Comox Valley Record

State of agricultural disaster declared in Brazeau County
A state of agricultural disaster has been declared in Brazeau County because of extremely wet conditions. County council unanimously voted for the move during Tuesday night's regular meeting and will notify provincial and federal government officials to ask for the establishment of a disaster recovery program. "These extremely wet conditions over the past few months have resulted in very low crop yields across Brazeau County," Reeve Bart Guyon said in a release. Postmedia Network (Edmonton Journal)

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

La SQ confirme que les appels téléphoniques de six journalistes ont été ciblés
La Sûreté du Québec a confirmé, mercredi, qu'elle a enquêté sur les activités de six journalistes il y a trois ans. Le capitaine Guy Lapointe a affirmé que l'enquête portait sur la révélation de contenu d'écoutes électroniques. M. Lapointe a expliqué que la SQ a déclenché cette enquête à la suite d'allégations que des journalistes ou d'autres personnes avaient divulgué de telles informations. Le directeur général de la SQ, Martin Prud'homme, en poste depuis deux ans, a obtenu ces informations concernant un seul dossier au cours des dernières 20 années, a indiqué le porte-parole. Selon M. Lapointe, la SQ a obtenu une ordonnance en 2013 pour consulter les registres d'appels entrants et sortants de six journalistes. Cette procédure ne prévoyait aucune écoute électronique ni surveillance par géolocalisation des personnes visées, que la SQ n'a pas voulu identifier, mercredi. Par ailleurs, M. Prud'homme a réclamé mercredi au ministère de la Sécurité publique qu'une enquête soit effectuée par «un tiers indépendant» afin d'examiner le recours à cette méthode dans le cas de journalistes. M. Lapointe n'a pas précisé si ce mandat devrait être confié au Bureau des enquêtes indépendantes, comme le réclame le Parti québécois depuis des révélations qui concernent la police montréalaise cette semaine... Les journalistes de Radio-Canada Marie-Maude Denis, Isabelle Richer et Alain Gravel sont parmi les cibles de la SQ, tout comme Denis Lessard, de La Presse, et Éric Thibault, du Journal de Montréal. La Presse Canadienne (Le Soleil); Postmedia Network (National Post); Agence QMI (Journal de Québec; Journal de Montréal); Radio Canada; La Presse; CBC News; Canadian Press (Metro News; Times Colonist; Winnipeg Free Press); Montreal Gazette

Journalistes épiés par la police : « une pratique qui n'appartient pas au Québec », dit Amir Khadir
« Ce genre de pratique appartient à des pays que je n'ose même pas nommer », a ajouté le député de Mercier de Québec solidaire. Plus tôt on apprenait que six journalistes avaient été ciblés en 2013 par des

mandats permettant aux policiers de la SQ d'obtenir le registre des appels entrants et sortants de leurs téléphones. Radio Canada

After Patrick Lagacé, other Montreal journalists worry they were spied on, too
Following revelations Montreal police obtained warrants to spy on a La Presse columnist, other Montreal journalists are raising concerns they may also have been tracked by law enforcement authorities. Monic Néron, a court reporter with the news station 98.5 FM, believes she may have been the target of investigators, as well. Néron said a source told her police have been looking at their own officers' phone records to find out who's been leaking information to the media... In her case, she said police probably didn't need a warrant, since cell phones issued to police officers are likely the property of their employer. CBC News

Le SPVQ a «d'autres chats à fouetter»
Le chef de police de Québec, Michel Desgagné, affirme que son service n'a jamais lancé une enquête visant la surveillance de journalistes. «Dans les cinq dernières années, il n'y a jamais eu d'enquête de ce type», a dit M. Desgagné. Il indique d'ailleurs que la réponse du maire Labeaume mardi sur le sujet provenait directement de lui. Plus encore, il affirme ne jamais avoir mené d'enquête interne sur des policiers de son service soupçonnés de donner de l'information aux journalistes. «On a d'autres chats à fouetter», a-t-il ajouté. Par contre, le directeur, qui prendra sa retraite le 31 décembre prochain, après 40 ans de service, dont cinq comme chef, avoue qu'il y a une préoccupation en ce sens, notamment en ce qui a trait aux enquêtes criminelles. «Il y a une préoccupation sur le serment de discrétion de nos collègues et on doit faire des rappels.» Agence QMI (TVA Nouvelles)

Edward Snowden talks surveillance at McGill University
McGill University will play host to whistleblower Edward Snowden tonight as many continue to question the tactics used by Montreal police after it was revealed they obtained warrants to spy on a journalist. Snowden, a former C.I.A. computer technician and contractor at the U.S. National Security Agency, will appear via video link to speak about surveillance in Canada. CBC News; Global News

The real faces of ISIS
Sally Armstrong talks to several ISIS militants about why they joined one of the world's most feared terror groups. (Video) Maclean's

It was judges who let police spy on a journalist
An opinion piece states, "You've probably heard of the Lagacé affair in recent days, about how Montreal police obtained warrants to spy on La Presse columnist Patrick Lagacé's cell phone for the apparent purpose of identifying the sources of leaks from the department... But while police have received most of the attention and criticism in connection with the Lagacé affair, they did not act alone. In fact, a more important role was played by the justices of the peace who gave the police the warrants that allowed them to spy on Lagacé's telephone, even though he was not suspected of involvement in any crime. As Pichet said, by seeking the warrants, the police followed the rules. Whether the justices of the peace did, too, in granting the warrants may be up to higher courts to decide. But this case is not the only one in which the actions of Quebec judges have threatened freedom of the press... So, the problem isn't with the police alone. It's also with the judges, or maybe with the rules under which the police and the judges operate. That's why the measures announced on Tuesday by the Couillard government in quick response to the Lagacé affair are a step in the right direction, but may not go far enough. One of the measures was an immediate order to police that they treat journalists the same as lawyers, judges and National Assembly members, by getting permission from the prosecutors' directorate before asking a judge for a warrant affecting them. Another is the formation of a committee including representatives of the police, the judges and the media to study the situation and, by next spring, make public recommendations that could include changes in provincial legislation. But prosecutors may be reluctant to refuse warrants to the police with whom they work closely and on whose co-operation they rely. And provincial legislation alone may not be enough to protect the watchdogs of public institutions and their sources. Changes in federal legislation may also be necessary." Postmedia Network (Montreal Gazette)

These Studies Shouldn't Be Used To Avoid The Issue Of Racial Profiling
An opinion piece states, "… A recent study, conducted by, the Canadian Network for Research on Terrorism, Security and Society, for the account of Public Safety Canada, claimed that "religious extremism has become the top motive for Canadian terrorism, replacing environmentalism." It is disturbing to know that such a study will be used by the government to write its own report about threats facing Canada. The study, not yet published but obtained by the National Post through access to information, found that between 2010 and 2015, 29 per cent of terrorist incidents were religiously motivated, while seven per cent were categorized as "anarchist," and three per cent were "supremacist." Meanwhile, we are surprised to know that the motivation for 61 per cent of the violent incidents examined are unknown. How reliable and serious could this study be if it identify three main motives for terrorist incidents and then leave more than half of the incidents with "no motives."…" Huffington Post

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Immigration detainee hunger strike in Ontario jail goes into third week
A group of immigration detainees at the Central East Correctional Centre (CECC) in Lindsay, Ontario, have been on a hunger strike for over two weeks to protest Canada's immigration detention system, says a migrants' rights advocacy group. Eighteen immigration detainees at the maximum security provincial prison located about 125 km northeast of Toronto began refusing meals on Oct. 17 to demand legislative changes to federal immigration rules that allow Canadian authorities to detain certain immigrants for an indefinite period, said Macdonald Scott, an immigration consultant with the Toronto law firm Carranza LLP. On Wednesday, only four detainees were able to continue the protest, the third such hunger strike by immigration detainees this year, Scott said. "They are fighting for the same demands, the main one being the presumptive period, that they be released after 90 days if they are not deported," Scott said… The detainees are also asking for a one-on-one meeting with federal **Public Safety Minister Ralph Goodale** to discuss the issue with him, he said. RCI

Drones, So Useful in War, May Be Too Costly for Border Duty
Cameras on drones stare down at the Canadian border from as high as 28,000 feet, scanning vast stretches of mountains, rivers and forests for potential terrorists and drug smugglers. The drones are intended to compensate for the Department of Homeland Security's lack of personnel and other surveillance equipment to adequately patrol the longest international border in the world. Equipped with high-tech cameras and radar, and capable of staying in the air much longer than planes flown by humans, the drones fill a critical gap in border security, officials with Homeland Security say. While the bulk of the department's drones are flown on the more troubled American border with Mexico, the ones here are used to surveil remote parts of the 5,500-mile border with Canada that are too risky for ground access or normal aircraft. New York Times

Richmond-based immigration fraudsters face sentencing
Three Richmond women appeared before a provincial court judge Friday for a sentencing hearing related to their involvement in a large-scale, Richmond-based immigration scam that has already sent Xu "Sunny" Wang to prison for seven years. The Richmond News understands that the nearly 1,200 clients Wang and the women — Ming Kun "Makkie" Wu, Jin "Fanny" Ma, Wen "Vvian" Jiang — assisted are now under investigation by Immigration, Refugees and Citizenship Canada (IRCC) to determine the validity of their residency and citzenship… IRCC spokesperson Nancy Caron would not explicitly confirm the 1,200 clients are under investigation… Caron also credits "large-scale fraud investigations led by our RCMP and Canada Border Services Agency (CBSA) partners. "These investigations led to criminal convictions of several immigration consultants. Notices of intent to revoke citizenship were sent to their clients who had provided fraudulent documents to suggest that they were living in Canada when they were living abroad," said Caron. But despite successes, a May 2016 report by Canada's Auditor General determined the federal government has not been adequately detecting and preventing citizenship fraud in part because the immigration department, along with the RCMP and CBSA, have failed to adequately share information. Richmond News

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Drone-hacking cybersecurity boot camp launched in UK
Budding cyberspies will learn how to hack into drones and crack codes at a new cybersecurity boot camp backed by the government. Matt Hancock, the minister for digital and culture, said students would gain the skills needed to "fight cyber-attacks" and help keep the UK safe. The 10-week course has been "certified" by UK spy agency GCHQ. But some security experts raised questions about the need for the course and the intent behind it. BBC News

Why Windows hack is being blamed on Russia-linked group
Microsoft's Windows chief has accused a notorious group of hackers - previously linked to Russia - of making use of an unpatched flaw in its operating system. Terry Myerson said Strontium was exploiting the bug to infect PCs in order to get access to potentially sensitive data. Strontium is also known as APT28 and Fancy Bear, and has previously been blamed for attacking a French TV network and the US Democratic Party. Microsoft says it is working on a fix. It intends to release the patch next week. BBC News

LAW ENFORCEMENT / APPLICATION DE LA LOI

RCMP were afraid to let officers testify at inquest of Nunavut man shot by police
New details emerged into how a 30-year-old man was shot by RCMP at his own home as a coroner's inquest got underway in Igloolik, Nunavut, Tuesday — including the fact the RCMP was afraid to let its officers testify in person. On March 20, 2012, two RCMP officers went to the home of Felix Taqqaugaq after getting a call from someone in the community who became concerned after hearing Taqqaugaq ranting on the community's local radio station. Taqqaugaq had schizophrenia and was being treated for mental health issues, according to the coroner's facts. On the night he died, the officers met with him briefly on his porch before Taqqaugaq went inside, returned with a knife, and was shot three times. This week's inquest, led by Nunavut's chief coroner Padma Suramala, will shed more light on the events surrounding his death and the subsequent investigation by the Ottawa Police Service. On Tuesday, the coroner's jury was selected, but it's still not clear how exactly the process will unfold, and how exactly the officers involved will take part. CBC News

RCMP now involved in Elections Yukon investigation in Whitehorse Centre
Elections Yukon said Monday it is investigating accusations of electoral shenanigans in two Whitehorse-area ridings. The RCMP are investigating claims that Tamara Goeppel, the Liberal candidate in Whitehorse Centre, violated the Elections Act by misusing proxy ballots. In a statement, Elections Yukon said “it appears that an offence, or offences under the Elections Act, have occurred.” Yukon News

Arrest made as RCMP investigate suspicious death in Kerrobert
RCMP have arrested a 56-year-old man in connection to a suspicious sudden death in Kerrobert early Wednesday morning. Police found a man dead after being called to a home in the community around 5 a.m. Officers believe his death is suspicious. Police have not revealed the victim's identity. CKOM; CBC News

Raid on Calgary home yields Alberta's fourth-largest fentanyl seizure
Police say they seized more than 3,700 fentanyl pills when executing search warrants in the Calgary communities of Killarney and Hillhurst in late October. The larger seizure involved 2,771 pills taken on Oct. 28 from a vehicle parked at a home in the southwest community of Killarney that was identified as "a potential fentanyl stash site" based on an earlier investigation in Lethbridge. That marked the fourth-largest seizure of fentanyl in Alberta's history, according to police. Police said the home was also being used as a cocaine conversion lab and officers seized 23 grams of cocaine along with 135 grams of a suspected buffing agent from the residence... Meanwhile, on Oct. 26, officers searched an apartment in the Hillhurst area and seized 943 fentanyl pills... The seizures were coordinated by the Alberta Law Enforcement Response Teams, or ALERT, a group that targets organized crime. and includes members

of the Calgary Police Service, Edmonton Police Service, Lethbridge Police Service, Medicine Hat Police Service, Alberta Sheriffs and RCMP. CBC News

Officer had a 'funny feeling' after encounter with a shaken Matthew Tucker
Two Oromocto RCMP officers told a murder trial in Saint John Wednesday of their strange encounter with Matthew Tucker on Nov. 9, 2014, the day before his mother Dorothy Tucker disappeared. The two officers were in separate cruisers late that morning when they stopped to assist a man, who was waving at them from a car. Const. Valerie Caron told the court the man, later identified as Matthew Tucker, was shaking and appeared nervous. He complained of seeing a "creature," a white head with no hair, she said. CBC News

Calgary police force needs new complaint process, Coun. Diane Colley-Urquhart says
Coun. Diane Colley-Urquhart stepped up her push Wednesday to reform the culture of Calgary's police force, one day after its chief and Mayor Naheed Nenshi gave assurances that change is coming. Last week, Colley-Urquhart, a member of the police commission, said several female police members of the Calgary Police Service (CPS) had come to her directly alleging they had been bullied and harassed while on the job, but felt that making formal complaints would hurt their careers. CBC News; Postmedia Network (Calgary Sun; Calgary Herald)

Surrey Mountie accused of child luring to appear in court Nov. 30
Surrey RCMP Constable Dario Devic is expected to appear in Surrey provincial court on Nov. 30 on a charge of child luring. Devic was arrested on Sept. 9 after Creep Catcher Surrey, a citizen group that aims to weed out "potential predators" and "blast" them in social media, did a sting outside a local mall. The Now

Local RCMP Veterans Association donate to Hospice Simcoe
A special entourage trouped into Hospice Simcoe on Wednesday with a gift for the palliative care organization. Members of the Georgian Bay division of the RCMP Veterans Association, two of them decked out in scarlet blazers, presented Hospice Simcoe executive director Sandra Dunham with a cheque for $7,000. The money came from the division's annual golf tournament in September, as well as the RCMP Musical Ride held during this year's Barrie Fair at the Essa Agriplex where Mountie hats were sold. Barrie Examiner

Auxiliary cop versatility
The City of Kelowna is seeking three levels of auxiliary cops. The three-tiered system preferred by council would allow auxiliaries to obtain specialized training and experience for specific requirements. In January, the federal government suspended the auxiliary constable program across the country, pending a full review. That decision took the civilian volunteers off the streets, where they had previously worked alongside regular RCMP members and assisted with traffic control for special events. "When the policy changed, it had a huge affect when you see the number of volunteers hours that are put in," said Coun. Brad Sieben. "It affects, financially, the functioning of the city." Castanet

RCMP humiliation: Sit on his knee and hike up your skirt
An opinion piece states, “Another drip falls in the continuing water torture of RCMP Commissioner Bob Paulson, who likely thought a public apology and a $100-million taxpayer settlement of two class-action harassment suits by female officers would shut down the tap. So much for wishful thinking. The added drip, and there are more, come to me in emails from individual women in the RCMP — both officers and civilians — outlining their alleged stories of physical and emotion abuse in the alpha-male dominated federal police force. All fear personal bankruptcy from pursuing their litigation, because the RCMP’s lawyers, paid for by the taxpayers, can play the long game of dragging the cases out. They also fear backlash from within, so much so that many have changed their unlisted numbers multiple times because harassment phone calls never failed to stop. And, even when they think they’ve won, they lose…”
Postmedia Network (Calgary Sun; Winnipeg Sun; Ottawa Sun; Edmonton Sun)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Why Adam Capay has spent 1,560 days in solitary
Renu Mandhane spent part of her day on Oct. 7 at the Indigenous friendship centre located on the outskirts of Thunder Bay, Ont. Mandhane, 39, is chief commissioner of the Ontario Human Rights Commission (OHCR), the 55-year-old body charged with preventing discrimination and advancing human rights in Ontario. Her office had organized the meeting with Indigenous leaders and community members to talk about discrimination and racial profiling. After the meeting was over, Mandhane organized an impromptu tour of the Thunder Bay Jail, a 170-bed facility built in 1926. "It's a s–thole," says Mike Lundy, a union president and a correctional officer at the jail... According to Ontario's Correctional Services, inmates are placed in administrative segregation when they are in need of protection, pose a threat to the health and safety of themselves or others, or are alleged to have committed a serious misconduct. "In Canada, we do not practise solitary confinement," a Public Safety Canada official, Kimberley Lavoie, told a UN meeting in Geneva on Oct. 25, a week after Mandhane revealed Capay's plight... Yet as Kimberley Savoie reinforced to the UN, Canada is adamant it doesn't practise solitary confinement. "Please note that the term 'solitary confinement' is not accurate or applicable within the Canadian penitentiary system," says Correctional Services Canada spokesperson Avely Serin. Canada does, however, practise "administrative segregation." "It is the separation, when specific legal requirements are met, of an inmate from other inmates," explains Serin. The difference between the two is often lost on government... Capay's case speaks to another troubling trend in Canadian prisons: Indigenous offenders serve much harder time than anyone else... "There is a group in Canada that keeps mysteriously dying,'" says University of Toronto sociology professor Sherene Razack. Many of these deaths occur because officials "will not touch, examine, or closely monitor Indigenous people in their care," Razack says. "This indifference kills." Adam Capay's treatment has drawn condemnation from all corners—including the very people responsible for his care. Maclean's

Former Oshawa politician Robert Lutczyk, jailed for kidnapping and weapons offences, denied parole
A bid for release by Robert Lutczyk, the former Oshawa councillor convicted last year of kidnapping and weapons offences, has been denied by the Parole Board of Canada. The board rejected Lutczyk's applications for both day and full parole following a video conference at Warkworth Penitentiary on Monday, Oct. 31. Lutczyk pleaded guilty last December and was sentenced in February to eight years and four months in federal custody. In a written decision released following the hearing, parole board members cited what they perceive as a failure on Lutczyk's part to take responsibility for his offences and the effect they had. Durham Region

Remembrance services across the area
The Orillia area salutes those who have given so much to the nation over the next 10 days. There are a number of Remembrance Day services slated throughout the region, beginning Friday in Brechin where the village holds its parade service. The parade will form at 10:30 a.m. at Brechin Public School with the Correctional Service Canada pipe band marching with veterans, other officials and local school children to the Brechin Legion for a Remembrance service and wreath-laying ceremony. Orillia Packet

Prime Minister Justin Trudeau appoints six new Quebec senators
Prime Minister Justin Trudeau has named six new senators from Quebec, including a doctor, an environmental scientist and a mayor. They include:.. Marc Gold, a former law professor who has held roles in the Jewish community and served on boards including the Parole Board of Canada, the Montreal Symphony Orchestra and Centraide. CTV News; CBC News

Union says cutting 14 deputy sheriff jobs in Saskatchewan will jeopardize safety
The union representing deputy sheriffs says 14 jobs have been cut in Saskatoon, Regina, Prince Albert, North Battleford and Weyburn. The Saskatchewan Government and General Employees' Union says losing the deputy sheriffs will jeopardize public safety. They screen people entering a courthouse, operate detention areas, escort prisoners inside the courthouse, provide courtroom security and transport prisoners by vehicle. They carry firearms. Union president Bob Bymoen says it's his understanding that the work will be contracted out to commissionaires who don't have the same level of training and are not

armed. Bymoen says government's mismanagement of public funds is to blame for the job cuts. Canadian Press (StarPhoenix; Leader Post)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Young man charged in deadly stabbing at Abbotsford high school
One day after a man walked into an Abbotsford high school and stabbed two students, killing one of them, charges have been approved against a suspect. Gabriel Brandon Klein, a young man in his early 20s, has been charged with murder and aggravated assault in connection with the attack, which shocked the Fraser Valley community. CTV News

Schools superintendent says Abbotsford, B.C. stabbing was 'random act'
The superintendent of schools in Abbotsford, B.C., says evidence suggests the man alleged to have killed one female student and injured another didn't know his victims. Kevin Godden says investigators believe the attack was a "random act of violence." "What I can tell you is that he is not a student of this school now." very school in the district will have all but one of its exterior doors locked during the school day out of an abundance of caution, Godden told reporter Wednesday. He said the Abbotsford Police Department has closed the high school where the two young women were stabbed to maintain the integrity of the investigation and a decision would be made later on Wednesday about when the school would reopen. Canadian Press (CTV News)

Liquid fentanyl found in Hamilton — believed to be 1st appearance in Canada
Police investigators in Hamilton announced today that they have seized what is believed to be the country's first stash of liquid fentanyl. The incredibly powerful prescription opioid is usually found on the street in pill, powder or patch form, but this new discovery is another marker in a growing opioid crisis across the country. CBC News

RCMP volunteers putting eyes on high crime areas in Kelowna
For the last two months local RCMP have been using specially trained volunteers to help go through hours of video surveillance footage and scout out problem areas in the city. The Auxiliary Constable Program is a nationally supported network of citizens who help local law enforcement with various tasks like public outreach. Since August, however, Kelowna has been using some of its 55 Auxiliary Constables in a very different way. In a report to council this week, Police Services Manager Stacey Jackson says the Auxiliary Constable Video Review Team has helped with one of the most time-intensive aspects of evidence gathering and investigation. Info News

Fentanyl-impaired driver convicted in Yellowknife
A woman in Yellowknife has been found guilty of driving while impaired by drugs including fentanyl — the first fentanyl-related impaired driving conviction in the N.W.T., say RCMP. Police arrested the driver, whose name they aren't releasing, in April. CBC News

Saanich Police will be equipped with overdose treatment
Saanich Police plans to purchase devices that would allow officers to administer a medication against the potentially deadly effects of illicit opioid overdoses. Acting Sgt. Jereme Leslie of the Saanich Police said the department anticipates "purchasing naloxone (hydrochloride) for our first line responders in the near future, once policy and training initiatives have been decided." Saanich News

Fentanyl crisis: Richmond to hold community forum on overdose prevention
Richmond will host a public forum this month on the impact of the North American drug-overdose crisis in the community. Parents, doctors, first-responders and educators will meet with the goal of helping community members understand the opioid-overdose epidemic and the lethal impact of the synthetic opioid fentanyl, according to a release. Province

New Gatineau crime map portal displays crime trends

Gatineau residents are now able to check out crime in their neighbourhoods and across the West Quebec city on the Gatineau police's new crime map portal. The portal, updated daily, lists seven offences: Break-ins, arson, mischief (for example, vandalism and graffiti), robberies, thefts from vehicles, thefts of vehicles and physical assault. The map will show incidents broken down daily, every 31 days and year to date. Deputy police chief Luc Beaudoin said in a release that the portal is part of the department's crime prevention strategy "because we believe people informed on certain crimes ... are able to take preventive measures" to protect themselves and their neighbours. Ottawa Citizen

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Fanshawe College's Woodstock campus kicks off traveling Faceless Dolls exhibit to bring greater awareness to staggering number of missing and murdered indiginous women in Canada
It's not just a statistic. Fanshawe College is launching an artistic endeavour to bring awareness to the fact that at least 1,200 indigenous women have gone missing or been murdered in Canada over the past few decades. The Faceless Dolls Exhibit, a student-made instalment, started its journey at the Woodstock Fanshawe campus last week. Students and staff gathered to echo a project started by the Native Women's Association of Canada, creating dolls out of felt and fabric to represent each one of those 1,200 missing or murdered women. Postmedia Network (London Free Press)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

How Taxing Weed in Canada Could Backfire
Next spring, the Liberal government is expected to introduce legislation to legalize marijuana for recreational use. Depending on how fast the legislation moves through parliament, legal weed sales could begin as early as 2018 and Canada would become the second country after Uruguay to legalize cannabis at a federal level. But with legalization comes hard questions about the amount of taxation necessary for that dank kush. Rachel Browne talks to us about the possible profits and consequences Canada could be seeing in the coming years once legalization becomes a reality. Vice News

One man in custody after police and bailiff shut down Ottawa pot shop
One of Ottawa's 17 illegal pot shops has been forcibly closed, but not by the drug squad. A bailiff arrived at the CannaGreen dispensary on Roydon Place Wednesday afternoon to enforce an eviction order. The shop had continued operating after an eviction notice was posted on the door Tuesday and the locks were changed. Ottawa police were on hand to help bailiff Doug Specht. A man inside the store was led out in handcuffs. Police said a man was arrested for trespassing, but no charges have been laid. Ottawa Citizen

Fatal car crashes triple among drivers high on marijuana after legalization in Colorado; double in Washington state
Prime Minister Justin Trudeau's plan to legalize marijuana should take into account "sobering" U.S. experiences where the first states to legalize the drug have seen big increases in fatal car crashes among cannabis-impaired drivers, according to a B.C. doctors' group. Washington State and Colorado started taxing and regulating cannabis in 2012 and the Council on Health Promotion, a section of Doctors of B.C., said vehicle fatality statistics, post-legalization, are "sobering." Postmedia Network (Edmonton Journal)

PUBLIC SERVICE / FONCTION PUBLIQUE

Federal pay backlog chopped in Phoenix system, but still slow going
Ottawa says it has winnowed down the backlog of federal salary problems related to the controversial Phoenix payment software to 22,000 from about 82,000 and is plowing ahead with eliminating the list. However, it won't give a deadline. IT World Canada

Ottawa's Phoenix nightmare rises in the House; all 338 MPs owe pension overpayments
Canada's 338 MPs, including Prime Minister Justin Trudeau and the entire cabinet are being forced to make retroactive payments to their pension plans after being hit by the same technical glitches in the new federal pay system that affected more than 80,000 federal civil servants this year. A notice to MPs sent last week from House of Commons chief human resources officer Pierre Parent pointed out that the maligned Phoenix pay system is the reason proper pension-plan deductions were not made between May and September of this year. The average MP will have to repay about $640, and cabinet ministers owe about $250. The actual amounts depend on an individual MP's specific pay situation, including tax deductions and payment amounts. The overpayments are being corrected during three pay periods, which began last month and continue through December. Winnipeg Free Press

OTHER / AUTRES

Royal Military College of Canada to be reviewed after suspected suicides, misconduct
Senior Canadian Armed Forces commanders have ordered a complete review of the Royal Military College of Canada following a number of suspected suicides and allegations of sexual misconduct at the prestigious institution in Kingston, Ont. The rare move highlights the growing concern among top brass about the way the 140-year-old college — where future generations of military officers are groomed — is being run... An eight-member team comprised of current and former military officers has been convened to look at all aspects of the college, from the institution's climate and culture to its academic programs and infrastructure. CBC News

Sajjan's Africa trip could be logistics planning for peacekeeping mission
Defence Minister Harjit Sajjan's trip to Mali and Senegal next week could be a sign the government is trying to nail down logistics for a possible peacekeeping mission in Mali, two peace operation experts suggest. iPolitics

All federal government operations to run on green power by 2025: environment minister
The federal Liberals are promising to run all government operations on renewable energy within a decade, Environment Minister Catherine McKenna said Wednesday. Speaking in Calgary to the Canadian Wind Energy Association, McKenna said the switch for all government operations is to be complete by 2025. CBC News

INTERNATIONAL

2 Iowa police officers killed; suspect in custody
A suspect in Wednesday morning's apparent ambush killings of two Iowa police officers was taken into custody hours later, after he flagged down a natural resources officer a county away from where the killings occurred, police said. CNN

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

canadaCJFE
Tuesday @ThomasMulcair debated @RalphGoodale on #PressFreedom in Canada. #SPVM @BMakuch @kick1972 @JustinBrakeNL protectpressfreedom.ca

Tonda MacCharles
Goodale said the ministerial directives apply to both #RCMP & #CSIS surveillance of journos & other potentially sensitive targets.

Tonda MacCharles
Goodale has rescinded only one ministerial directive so far, re firearms classification. (Not directive re use of info gleaned by torture)

Tonda MacCharles
Goodale opposes political approval for such warrants, says a "dangerous slope"- you don't want any politicians overseeing of journos.

Tonda MacCharles
Goodale: ministerial dirctvs under review require approvals for surveillance of "sensitive" sectors eg journos, academics, trade unions.

Tonda MacCharles
@RalphGoodale in scrum quotes #RCMP Comm Paulson that no journos under surveillance "to his knowledge & he'd know."

michael_byers
Press freedom under threat in Canada, reports the New York Times http://nyti.ms/2eblN1u #canpoli @LP_Affaires @DenisCoderre @RalphGoodale

CTV_PowerPlay
ICYMI: Saskatchewan @PremierBradWall penned open letter to Minister Goodale protesting a nat'l carbon tax http://goo.gl/kZyemx #cdnpoli https://t.co/GWilcT34qP

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Snowden
Oh, Canada... http://montrealgazette.com/news/local-news/police-surveillance-scandal-montreal-to-study-spying-issue-behind-closed-doors ...

ryhicks
.@CoiteuxMartin says the Public Security Ministry will investigate the latest revelations that the SQ spied on journalists in 2013 #polqc

Mathieu_Dion
Journalistes surveillés par la SQ: "Ce serait le seul cas", dit Martin Coiteux de la Sécurité publique. Enquête sur ce cas. #assnat #polqc

tvanouvelles
Martin Coiteux annonce qu'une enquête administrative sur la surveillance de journalistes par la SQ sera effectuée par son ministère

PatriceRoyTJ
Journalistes épiés : «C'est une crise comme on en a rarement vu ici. C'est important d'agir vite» -Michel Cormier

PatriceRoyTJ
Journalistes sous surveillance - «Je n'aurais jamais autorisé cela. Je n'ai jamais été informé de cela.» -Stéphane Bergeron

tvanouvelles
Surveillance de journalistes par la SQ - Le chef du corps policier «irrité» par ce qui a été mis à jour

felixseguin
Espionnage des journalistes, voici ce que les policiers du @spvm viennent de recevoir de leur syndicat.

FPJQ
6 journalistes épiés par la SQ: La FPJQ réitère le besoin urgent d'une enquête publique sur la surveillance des journalistes au Québec

RadioCanadaInfo

Les appels de Marie-Maude Denis, Isabelle Richer et Alain Gravel surveillés par la SQ http://rc.ca/MZIFTg

Global_Montreal
Whistleblower Edward @Snowden to speak at @McGillU https://t.co/tNa3epjE8j

gravela_rc
À mon tour d'avoir la confirmation comme quoi j'ai été visé par des mandats de cour pour obtenir le registre de mes appels par la SQ.

mmdenisrc
Je viens d'apprendre que mes appels entrant et sortant ont été espionnés par la Sûreté du Québec en 2013.

IsabelleRicher
Surréaliste... La SQ a espionné mon cellulaire à la suite d'une plainte formulée par Michel Arsenault en 2013

CBC_Hayward
.@IsabelleRicher and @mmdenisrc are on air right now, expressing their shock at being spied on by Quebec police.

LAW ENFORCEMENT / APPLICATION DE LA LOI

620 CKRM
RCMP investigating "suspicious death" in Kerrobert. More at http://bit.ly/2e2NWOq #sask

StewartBellNP
Quebec narcotics distributor detained in international crackdown on Darknet drug dealers. http://www.rcmp.gc.ca/en/news/2016/1/the-rcmp-and-law-enforcement-agencies-the-world-collaborate-international-darknet ...

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Justin Ling
Have you checked out @vicecanada's week-long series looking at Canada opioid crisis yet? http://www.vice.com/en_ca/series/relapse-facing-canadas-opioid-crisis ...

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

vicecanada
How taxing weed in Canada could backfire. http://bit.ly/2faI7hA

OttawaCitizen
Updated: One man in custody after police and bailiff shut down Ottawa pot shop http://ow.ly/6iC9305Nd1I

OTHER / AUTRES

CBCPolitics
All federal government operations to run on green power by 2025: environment minister http://ift.tt/2eoHAr0

CTVVancouver
#Breaking: Gabriel Brandon Klein, born 1995, charged with murder and aggravated assault in stabbing at Abbotsford high school.

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

Today's News / Actualités
November 3, 2016 / le 3 novembre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

MINISTER / MINISTRE

Broadcast Media / Médias télédiffusés :

Au Canada en ce moment, il y a combien de journalistes qui sont surveillés, soit par la GRC, soit par le SCRS? **M. Goodale** connaît la réponse mais il a refusé de répondre hier. (RDI, 3 :08ET)

TOP STORIES / MANCHETTES

Fort McMurray's next 6 priorities in wildfire recovery

The May wildfire that ripped through Fort McMurray was so devastating it not only razed communities but also hit the Canadian economy. The fire devoured more than 2,400 homes and forced more than 88,000 people to leave for over a month. The wildfire, which is still smoldering but no longer a risk, raged uncontrollably for six weeks and consumed 589,552 hectares of forest — an area larger than Prince Edward Island. Six months later, Fort McMurray's municipal and community leaders are reflecting on what the region's priorities should be over the next six months of recovery. CBC News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Fort McMurray's next 6 priorities in wildfire recovery
The May wildfire that ripped through Fort McMurray was so devastating it not only razed communities but also hit the Canadian economy. The fire devoured more than 2,400 homes and forced more than 88,000 people to leave for over a month. The wildfire, which is still smoldering but no longer a risk, raged uncontrollably for six weeks and consumed 589,552 hectares of forest — an area larger than Prince Edward Island. Six months later, Fort McMurray's municipal and community leaders are reflecting on what the region's priorities should be over the next six months of recovery. CBC News

Hydro seeks millions for emergency repairs
Newfoundland and Labrador Hydro is asking the Public Utilities Board (PUB) for more than $17 million in emergency funding for two major and unexpected repair jobs. In the first of two applications for extra money, the power company is requesting $4.6 million to fix damage to access roads in central Newfoundland caused by rain from Hurricane Matthew last month (…) The second Hydro application is for $12.9 million to repair faulty welds in the Bay d'Espoir penstock. The penstock is a sort of sluice that feeds water into power generation stations. The bad welding has caused two cracks in the structure, which means it can't be used again until it's fixed. CBC News

Canadian army interested in old nuke that may have been found off Haida Gwaii
Sean Smyrichinsky recently spent several hours diving for sea cucumbers off Pitt Island, near Haida Gwaii. He didn't find any. But he decided to hop on his underwater scooter for one last look before calling it a day. Flying around underwater, he spotted something unusual on the ocean floor. "I found this big thing underwater, huge, never seen anything like it before," Smyrichinsky related from Cortes Island (…)"That bomb" was a nuclear device that was dumped or exploded off the B.C. coast on Feb. 13, 1950, when an American B-36 bomber crashed while en route from Alaska to Texas. It was packed with lead – not plutonium – and TNT. Five crew members died but 12 were rescued after they parachuted onto Princess Royal Island, about 200 km south of Prince Rupert. They were forced to abandon the plane after ice built up on its wings and three of its six engines caught fire. None of the stories at the time of the crash detailed the payload the bomber had been carrying. But eventually it was discovered that the bomber's mission was to simulate a nuclear attack on San Francisco, and the plane had been carrying a Mark IV nuclear weapon. Postmedia (National Post, Vancouver Sun, Vancouver Province)

Canadian military sends surveillance aircraft to Arctic to investigate mysterious pinging sounds
The Canadian Forces has sent a surveillance aircraft to the Arctic to investigate a pinging sound that appears to be coming from the ocean floor, but the military is no closer to solving the mystery of what could be making the noise. The government of Nunavut asked Ottawa to investigate the sounds, prompting the decision to send a CP-140 Aurora aircraft to conduct surveillance of Fury and Hecla Strait, northwest of the hamlet of Igloolik. Descriptions of the noises range from pings to beeps or a hum. They have been reported by hunters in the region, who worry they are driving away animals. Paul Quassa, a member of Nunavut's legislative assembly, told lawmakers last month the sounds are coming from the sea floor. "The sound that has been heard in the area seems to be emitted from the seabed and underwater," Quassa said in an Oct. 25 statement. "Our constituents as well as hunters and boaters have reported that the area in question is almost devoid of sea mammals and that hunting has been poor in the area for quite some time." According to Department of National Defence spokesman Dan Le Bouthillier, the Aurora's crew "performed various multi-sensor searches in the area, including an acoustic search for 1.5 hours, without detecting any acoustic anomalies. The crew did not detect any surface or subsurface contacts." Postmedia (National Post, Ottawa Citizen); Motherboard

Sulphuric acid 'mist' reported in city's Wallace Emerson neighbourhood
Police are asking residents in the area of Bloor Street and Lansdowne Avenue to stay indoors and keep their windows closed due to a reported sulphuric acid "mist" in the air. Toronto Fire Services told CP24 that chemicals, including sulphuric acid, were reportedly mixed together at a building on Wade Avenue and the combination caused a type of mist to fill the air. The mist, Fire Capt. Michael Westwood said, can cause irritation to the nose, eyes and throat. The building where the incident occurred has been evacuated and a hazmat team is on scene. Streets in the area are blocked off and residents have been asked to stay indoors. No injuries have been reported. A TTC bus is in the area sheltering approximately 40 people. Westwood said a company is coming to remove the substance from the scene. CP24; Canadian Press (Globe and Mail); Toronto Star

Ottawa exigera l'installation d'enregistreurs audio-vidéo dans les locomotives
Le ministre fédéral des Transports a annoncé jeudi qu'Ottawa exigera dorénavant l'installation d'enregistreurs audio-vidéo dans les locomotives, comme le recommandait le Bureau de la sécurité des transports. Marc Garneau a indiqué que ces appareils serviront aux enquêtes sur les accidents comme celui de Lac-Mégantic, qui a fait 47 morts à l'été de 2013. Le ministre a aussi promis que l'examen de la Loi sur la sécurité ferroviaire sera terminé en 2017 plutôt qu'en 2018, afin de renforcer plus rapidement la sécurité dans les chemins de fer. M. Garneau était à Montréal, jeudi matin, pour présenter sa stratégie «Transports 2030», fruit de consultations que le nouveau ministre a menées depuis six mois. La Presse Canadienne (La Presse)

Search for missing Codroy Valley hunting guide into 2nd day
A ground search will continue Thursday for a 49-year-old man who became separated from his hunting group Tuesday afternoon on Newfoundland's west coast. RCMP said a helicopter search continued until midnight Wednesday, and will be back in the air Thursday, weather permitting. Barachois Ground Search and Rescue, a Joint Rescue Co-ordination Centre helicopter and RCMP assisted in the search, which began shortly after the man was reported missing at 1 p.m. Wednesday. CBC News

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Edward Snowden Calls Police Spying on Quebec Journalists a 'Threat to Democracy'
In a speech to 600 people at McGill University in Montreal on Wednesday night, Edward Snowden described police spying on Quebec journalists a "threat to the traditional model of our democracy." Though it had been announced months ago, the timing of Snowden's conference was strangely appropriate. The event took place just hours after *La Presse* revealed the Sûreté du Québec (SQ), which is the provincial police force, had put at least six prominent journalists under surveillance. Two days earlier, the same Montreal daily had broken the story that its own star columnist, Patrick Lagacé, had been spied on by the Montreal police force (SPVM). Appearing live from Russia, where he's been living in exile since exposing top secret information about US intelligence and surveillance programs, Snowden did not mince words when discussing the behaviour of Quebec police. (…) Snowden reiterated that citizens should be leery of authoritarian measures defended by governments that argue their very survival is under threat from terrorists. "There's no real evidence this is actually the case, but the politics of this fear have reshaped the way our laws are getting passed." Canada's Bill C-51, whose adoption in 2015 generated reams of criticism from legal experts and ordinary citizens worried about how it would erode Canadians' privacy and individual rights, was one such example, he said. During the election, Prime Minister Justin Trudeau promised to amend the law, most notably by scrapping some "problematic elements" like the overly vague proscription against terrorist propaganda and by "guaranteeing that all

actions undertaken by the Canadian Security Intelligence Service are consistent with Canada's Charter of rights and freedoms." Motherboard

Journalistes espionnés: Québec crée une commission d'enquête
Le gouvernement Couillard déclenche une commission d'enquête sur l'espionnage de journalistes par la police compte tenu de la « gravité » de la situation. Les nouvelles révélations voulant que la Sûreté du Québec ait, comme la SPVM, procédé à la surveillance électronique de journalistes « sont à ce point sérieuses » que Québec juge nécessaire de poser « un geste supplémentaire » pour faire « toute la lumière, de façon transparente » sur cette affaire, ont expliqué les ministres Stéphanie Vallée (Justice) et Martin Coiteux (Sécurité publique) en conférence de presse jeudi à l'Assemblée nationale. Plus tôt cette semaine, le gouvernement a annoncé la création d'un comité d'experts présidé par un juge et au sein duquel siégeront des représentants des corps de police et des médias. Or « le mandat confié au groupe d'experts sera conféré en vertu de la loi sur les commissions d'enquête », a annoncé Mme Vallée. Les commissaires auront ainsi le pouvoir de contraindre des personnes à témoigner. Leurs audiences pourront être publiques, selon le souhait des commissaires. Mais pour le premier ministre Philippe Couillard, il est évident qu'elles le seront. La Presse; Canadian Press (Daily Courier, iPolitics, Castanet); Agence QMI (Canoe); Presse canadienne (Journal Métro)

Stéphane Bergeron se retire de ses fonctions de porte-parole du PQ à la sécurité publique
Le député péquiste Stéphane Bergeron a annoncé qu'il se retire de ses fonctions de porte-parole à la sécurité publique après la révélation que des journalistes ont été surveillés par la Sûreté du Québec alors qu'il était ministre. M. Bergeron a pris cette décision parce qu'il craint de nuire au travail de sa formation politique à l'Assemblée nationale. Mercredi, M. Bergeron s'est défendu d'avoir demandé que des journalistes soient ciblés pour connaître l'origine de fuites de renseignements policiers dans les médias, en 2013, alors qu'il était ministre de la Sécurité publique. M. Bergeron a cependant reconnu qu'il avait contacté le directeur général de la SQ, Mario Laprise, à la suite d'une « conjonction » de faits, dont une lettre de l'ex-président de la Fédération des travailleurs du Québec, Michel Arsenault, se plaignant de fuites concernant des écoutes électroniques qui l'ont visé. Presse canadienne (Le Devoir); TVA Nouvelles; Radio-Canada

Coderre underwhelms with response to revelations of police spying
An opinion piece state, "Montreal Mayor Denis Coderre's response to revelations that police, with the approval of mainly one Quebec court judge, electronically monitored journalists was, in a word, unacceptable. While the Quebec government's response was encouraging, the mayor simply pronounced search engine-optimized keywords that imply "concern" for democracy, while simultaneously reiterating his support for a police chief whom he had recently nominated. "What you see is what you get," with the former Liberal MP, a "common sense" politician who is "close to the people" and can "walk and chew gum at the same time." He was elected mayor of Montreal three years ago this month and before his win, I warned that Coderre would be a bland "tofu mayor," adaptable and inoffensive. Coderre has expanded his bank of catch-phrases and remains bland, philosophically, but has become emboldened with power, seemingly incapable of backing down from any of his positions, no matter how ridiculous or wrongheaded. One of Quebec's most prominent journalists, La Presse columnist Patrick Lagacé, had his phone monitored by Montreal police (SPVM) as part of an investigation into officers who went on to be charged with falsifying evidence, it was revealed this week. Lagacé has been critical of the SPVM in recent years and was continuing to develop new stories based on sources within the department." National Post

Les journalistes dans l'œil de la cybersurveillance
Denis Lessard, Alain Gravel, Marie-Maude Denis, Isabelle Richer et Éric Thibault sont parmi les six journalistes ayant fait l'objet d'une surveillance confirmée par la SQ. Patrick Lagacé, lui, a été surveillé par le SPVM. Deux enquêtes qui se sont déroulées avant et après l'adoption du projet de loi C-51. La nouvelle a eu l'effet d'une bombe dans le milieu journalistique québécois cette semaine. On a ainsi appris qu'au total, sept journalistes ont été l'objet de surveillance de la part de deux corps policiers, la Sûreté du Québec et le Service de Police de la Ville de Montréal. Alors que ces révélations se sont effectuées au compte goûte depuis dimanche de façon antéchronologique, nous vous proposons ici un compte-rendu de ces deux histoires, en portant une attention particulière sur la nature de ces surveillances. L'adoption

du controversé projet de loi C-51 pourrait-elle avoir influencé la façon d'agir des forces de l'ordre? Branchez-vous

Feds forbid construction of new embassies on Sussex Drive
The federal government is forbidding the construction of new embassies on Ottawa's Sussex Drive following a stark RCMP assessment of the potential for "violent events" in the high-profile neighbourhood. Countries with diplomatic missions already located on the well-known boulevard include the United States, France, Kuwait, Saudi Arabia and South Africa. It is also home to Rideau Hall, where the Governor General lives, as well as the prime minister's residence at 24 Sussex. Justin Trudeau and his family are living in a house on the Rideau Hall grounds while federal officials consider badly needed renovations to the traditional address of Canada's leader. Foreign Affairs Minister Stephane Dion was advised of the ban on new embassies in January by Daniel Jean, then his deputy minister, records released under the Access to Information Act show. Jean has since been named national security adviser to the prime minister. "A recently concluded RCMP security assessment advises against any additional foreign embassies being located along Sussex Drive," says Jean's memo to Dion, obtained by The Canadian Press. "As a result, the department will no longer be approving requests by diplomatic missions to acquire land in the affected zone." Canadian Press (Daily Commercial News)

Broadcast Media / Médias télédiffusés :

CBC News aired the live conference with Prime Minister Justin Trudeau, who commented on freedom of the press from police surveillance. Rough Transcript

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Federal immigration policy 'a little disappointing' says ISANS
The federal government's new immigration strategy focuses too much on economic immigration and not enough on helping refugees, according to the director of operations for the Immigrant Services Association of Nova Scotia. The changes to Canada's immigration program will see the federal government increase the number of privately sponsored refugees to 16,000 in 2017, while the number of government sponsored refugees is being rolled back to 7,500. "It's just a little disappointing that the federal government's responsibility - those numbers are smaller than actually we thought they would be," said Gerry Mills director of operations for ISANS. Privately sponsored refugees arrive in Canada with financial help from community groups who pay for their travel and help them with housing, clothing and other basic needs. Government sponsored refugees have all of that taken care of by the federal government, said Mills. This year about 20,000 people were brought into the country as government-assisted refugees, in 2015 nearly 10,000 refugees were sponsored by the federal government. CBC News

The Detroit-Windsor Tunnel is how old?
They don't call us the Motor City for nothing. Yes, we're the home of the Big 3, everyone knows that. But, you probably didn't know (or maybe I'm the only one who didn't know?) that we're also home to the U.S.'s first vehicular tunnel that connects two countries. The Detroit-Windsor Tunnel, which runs underwater and takes drivers back and forth between Michigan and Ontario, turns 86 years old today. It's the second busiest crossing between the U.S. and Canada in the country, following Matty Moroun's Ambassador Bridge. Of course, it's not the country's first underwater tunnel. In fact, it's the third. The Holland Tunnel that connects New Jersey and Manhattan and the Posey Tube in California beat us out for that title. Detroit Metro Times; ClickOnDetroit

Canada: The Bri-Chem Trilogy: Federal Court Affirms Tribunal
On November 16, 2015, we described important substantive and procedural issues that would be addressed by the Federal Court of Appeal (FCA) in an appeal from a decision of the Canadian International Trade Tribunal (CITT). Almost a full year later, on October 21, 2106, the FCA affirmed the decisions of the CITT both in respect of the substantive customs issue, whether or not an importer may claim duty neutral relief under NAFTA more than one year from the date of accounting when its zero-

rated tariff classification is re-determined by the Canada Border Services Agency (CBSA) as a positive duty-rated tariff classification, and the procedural issue, the nature and application of the doctrine of precedent in the context of appeals from determinations of the President of the CBSA heard and decided by the CITT. The FCA deferred to the expertise of the CITT, particularly given its expertise and the fact-infused nature of the matters before it. Mondaq

China carfentanil trade thrives as seizures top 400 in U.S.
Seizures of the deadly chemical carfentanil have exploded across the United States, with more than 400 cases documented in eight states since July alone, The Associated Press has found. Fueled by a thriving trade out of China, the weapons-grade chemical is suspected in hundreds of drug overdoses in the U.S. and Canada. An AP investigation last month showed how easily carfentanil can be purchased online from China. Of the 12 companies that initially offered to export carfentanil around the world, just three have stopped since the report was released. Nine continue to offer carfentanil for sale, no questions asked, and the AP identified four additional companies willing to sell the drug, some of which claimed to have U.S. addresses. Asked for comment, most denied they'd ever made the offers. Jilin Tely Import and Export Co. initially boasted in an email that carfentanil was one of its "hot sales product (...) But it is not controlled in China, the top source of fentanyl-related compounds that end up in the U.S., Canada and Mexico, according to the U.S. Drug Enforcement Administration. "It's a loophole that needs to be closed because even small quantities can have a terrible lethal effect," said Andrew Weber, who served as U.S. assistant secretary of defence for nuclear, chemical and biological defence programs from 2009 to 2014. "Terrorists could acquire it commercially as we have seen drug dealers doing." Associated Press (CTV News, Global News)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Domain search tool aims to foil phishing
In the race to be the most imaginative, so far attackers are outwitting defenders. Take, for example, the ability to craft and find look-alike domain names. Somehow, no matter how creative security teams get thinking about and storing alternatives for blacklists, criminals are able to spoof brand, product, or organization names faster. That can give them an edge in phishing attacks, where emails often include phoney but real-looking links gullible employees fall for. To give security teams a better chance DomainTools, which has domain name discovery and profiling system, has created a new cloud-based service called PhishEye. which automates searching for registered lookalike domains, including those deliberately created with typos and misspellings. IT World Canada

Your WiFi-connected thermostat can take down the whole Internet. We need new regulations.
Late last month, popular websites like Twitter, Pinterest, Reddit and PayPal went down for most of a day. The distributed denial-of-service attack that caused the outages, and the vulnerabilities that made the attack possible, was as much a failure of market and policy as it was of technology. If we want to secure our increasingly computerized and connected world, we need more government involvement in the security of the “Internet of Things” and increased regulation of what are now critical and life-threatening technologies. It’s no longer a question of if, it’s a question of when. Washington Post

LAW ENFORCEMENT / APPLICATION DE LA LOI

200 fentanyl pills seized in Saskatoon drug bust
Police said they have seized fentanyl pills and charged three people following a drug bust in Saskatoon. The bust happened after members of the Saskatoon integrated drug enforcement team spotted what they believed to be a drug transaction in the area of Taylor Street and St. George Avenue on Wednesday afternoon. Police arrested two men and said they seized 100 fentanyl pills and over $1,500 in cash. A home in the 100-block of Girgulis Crescent was then searched, where police said they seized an additional 100 fentanyl pills. Two men, 20 and 22, are facing charges of possession for the purpose of trafficking. The 22-year-old man is also facing charges of trafficking fentanyl and possession of the

proceeds of crime. An 18-year-old woman is also charged with possession for the purpose of trafficking. Global News

RCMP release photo of homeless man charged in high school murder
Homicide investigators have released a photo of the 21-year-old man charged in the stabbing death of an Abbotsford high school student in hopes the public will come forward with information. Staff Sgt. Jennifer Pound says the photo of Gabriel Klein was captured on closed-circuit surveillance just hours before a deadly attack at Abbotsford Senior Secondary. Thirteen-year-old Letisha Reimer was killed after being attacked by a barefoot intruder in the school's atrium. Her 14-year-old friend, who cannot be named because of a publication ban, was seriously injured and remains in hospital. CTV News

LGBTQ Canadians Sue Government for Decades-Long Witch Hunt
In a Canadian military interrogation room in 1990, strapped to a polygraph machine and sensing unseen observers behind a two-way mirror, 21-year-old Canadian sailor Todd Ross finally broke down in tears and said out loud what he'd been unable to say even to himself: He was gay. The military gave Ross an ultimatum: accept an honourable discharge or perform "general duties"—grunt work—for the rest of his career. (...) According to government records, the RCMP spent decades following World War II investigating, surveilling, and questioning suspected gay and lesbian public servants, including members of the military, about their sexual orientation. At one point, the RCMP amassed a list of 9,000 people deemed suspect and subject to investigation. The Canadian government would often employ a device that would measure sweat and sexual reaction to certain words, phrases, and images—dubbed internally as the 'fruit machine'—to vet suspected LGBTQ government employees. The project was created through a government grant at the Carleton University Psychology Department. Vice News

Edmonton judge stays sex charge over unexplained loss of evidence by RCMP
An Edmonton judge has tossed out a sexual assault charge against an Edson-area man as a result of the "unexplained" loss by the RCMP of an audio-recorded statement from the alleged victim. In a ruling released this week, Court of Queen's Bench Justice Denny Thomas issued a judicial stay of the 2015 sexual assault charge against the 21-year-old accused man. "Balancing the societal interest of having a full trial on the merits of this charge before a jury and the right of the accused to make full answer and defence, I conclude that this is one of those 'clearest of cases' where a stay should be granted to respect the rights of the accused," said Thomas in his written decision, The man had sought a stay of the charge, arguing the "unexplained" loss of key evidence by the Mounties was so prejudicial to his right to make full answer and defence that he would not get a fair trial. The Crown had conceded that the loss of the complainant's audio statement meant the prosecution had not met their disclosure obligation and it was therefore a breach of the accused's Charter rights, but had argued there was other evidence available to the defence which would have mitigated the prejudice to him. Edmonton Journal

Alberta vehicle theft suspect arrested after leading police on low-speed skid steer chase
Police have arrested a suspect in connection with a string of thefts of trucks, trailers and construction equipment east of Edmonton. The arrest came after a man driving a construction vehicle led Vegreville RCMP on a low-speed chase. It all began last Saturday around 4:45 p.m., when Mounties got a call about a suspicious man who had just parked a truck and trailer in a field southwest of Mundare. Police did a check and discovered the truck and trailer had been stolen from a business in the Nisku industrial park south of Edmonton. The person who called police then said the man who had dropped off the truck was leaving the scene in a John Deere skid steer, which was later determined also to have been stolen. RCMP found a man driving the skid steer on Range Road 17-0 and attempted to arrest him. The man fled in the equipment which, according to John Deere's website, has a maximum travel speed of about 20 kilometres per hour. Police said at one point during the low-speed pursuit, the driver attempted to ram a police vehicle. Global News

Ten drug dealers in dial-a-dope network allegedly operated by Mohamed Abdi Yusuf caught in Brooks, Alberta bust
Seven suspected drug dealers have been arrested and warrants have been issued for three others as ALERT (Alberta Law Enforcement Response Teams) shut down a drug trafficking network operating in Brooks, Alberta. ALERT's Medicine Hat organized crime team conducted the investigation in response to

community concerns related to cocaine trafficking. ALERT worked hand-in-hand with RCMP Brooks and Medicine Hat Police Service on the three-month investigation. ALERT alleges that the group was operating as a dial-a-dope network with Mohamed Abdi Yusuf, 40, as the suspected ringleader. The group played a significant role in cocaine trafficking within Brooks and the project implicated the suppliers and street-level dealers. A total of 10 men are facing 20 drug-related charges. "This dial-a-dope group presented a challenge for uniformed members to investigate. However, by virtue of the partnership with ALERT and their specialized skill sets and resources, we were able to deliver a coordinated response and provide a safer community," said Sgt. Raimo Loo, RCMP Brooks. Indo-Canadian Voice

Needles found in chocolate bars
Sewing needles were found in two large-sized chocolate bars collected by Cochrane youth while trick-or-treating, Oct. 31. Cochrane RCMP are investigating the incident and in the meantime are asking people to step forward if they have been the victim of the tampering of candy during the annual Halloween costume dash for candy. According to the Cochrane RCMP, the complainant had been checking their children's Halloween candy and found a sewing needle in a large O'Henry bar and another sewing needle in a large Kit Kat bar. They had been trick-or-treating on the west side of Gleneagles. The exact location of where the bars were received is still under investigation and if there are any other incidents with tampered candy the RCMP are strongly encouraging it to be reported to help narrow down where this could have taken place at. Cochrane Times

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Advocates urge Liberal government to reduce number of women in prison
Alia Pierini says she still suffers from anxiety as a result of the time she spent in solitary confinement. The 31-year-old from Chilliwack, B.C., says she panics when she ventures out in public alone — traumatized from the effects of having been held periodically in a segregation cell, a place she calls a "cage not meant for a human." Pierini, who served 44 months for drug and assault charges, was on hand at a news conference today where prisoners' rights advocates called on the Liberal government to take steps to reduce the number of women behind bars. Kim Pate, the longtime activist newly recommended for the Senate by Prime Minister Justin Trudeau, says she was "heartened" to see Justice Minister Jody Wilson-Raybould given a mandate to restrict the use of solitary confinement and improve the treatment of prisoners with mental illness. That would mean implementing recommendations from the inquest into the death of Ashley Smith, an emotionally disturbed 19-year-old who died behind bars in 2007 after tying a strip of cloth around her neck. Guards who were ordered not to intervene stood watch outside her cell. Pate says three years after the release of that report, she wants to see action in those areas as quickly as possible. Canadian Press (Chronicle-Herald)

Un jeune Terre-Neuvien craint de voir son père, l'assassin de sa mère, réapparaître chez lui
Un jeune homme de Stephenville, à T.-N.-L., affirme qu'il vit dans la hantise de voir son père, condamné pour le meurtre de sa mère lorsqu'il n'avait que 4 ans, revenir dans la province lorsqu'il obtiendra sa pleine libération. Dale Ogden a obtenu une libération conditionnelle de jour après avoir purgé 16 ans d'une peine de prison à vie pour le meurtre non prémédité de sa femme, Judy Ogden, en 1997. Il se trouve dans une maison de transition de l'île de Vancouver après avoir obtenu sa libération du pénitencier William Head en septembre. Son fils, Daniel Benoit, 22 ans, estime qu'il aurait dû rester en prison. Il a décidé de prendre la parole publiquement parce qu'il souhaite lancer un débat national au sujet des peines pour meurtre qui sont trop légères au Canada, à son avis. Depuis septembre, il craint de voir apparaître Dale Ogden à tout moment sur le pas de sa porte. Il fait pression sur Service correctionnel du Canada pour obtenir une photo récente de lui, pour être en mesure de le reconnaître. Il a également déposé une demande de « séparation géographique » pour empêcher Ogden de revenir à Terre-Neuve-et-Labrador. Ses demandes sont restées lettre morte. Service correctionnel Canada explique que les règles en matière de protection de la vie privée l'empêchent de rendre publiques les photos d'un contrevenant ou des renseignements précis concernant ses allées et venues. Daniel Benoit croit que la sécurité de sa famille devrait primer. Il en a aussi contre un certain laxisme du Service correctionnel du Canada lors d'un incident à la fin septembre. L'agence l'a prévenu le 30 septembre qu'un mandat d'arrêt avait été lancé contre son père parce qu'il était introuvable. L'appel a déclenché une panique dans la

maisonnée de Daniel Benoit, qui croyait que Dale Ogden s'était mis en route pour Terre-Neuve. Ogden a rapidement été retrouvé, mais les Benoit en ont seulement été prévenus 24 heures plus tard. Radio-Canada

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NIL

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Amnesty International calls for more police in Fort St. John, northeast B.C.
Resource development contributes to crime, putting Indigenous women and girls most at risk, Amnesty says. A new report from Amnesty International says police in northeast B.C. are not equipped to deal with the high rates of crime in the region, particularly when it comes to violence against Indigenous women and girls. The report also calls on RCMP to increase Indigenous cultural knowledge for its officers, and renews Amnesty's demand for the Site C dam project to be stopped. The report titled Out of Sight, Out of Mind provides an overview of the ways in which resource development in B.C.'s Peace River region — including fracking, coal mining and hydroelectric dams — affect vulnerable populations. "There is a downside to the scale of resource development in the northeast and the people who live there," said Craig Benjamin, who helped prepare the report for Amnesty. "Particularly, Indigenous women and girls are bearing a very heavy burden for hosting these products in their region." CBC News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Legal pot could boost economy
An editorial piece states, "It's possible, even likely, that at some point next year, Ontarians will be able to search store shelves for 'purple haze', 'blue dream' and 'kosher kush' marijuana alongside their VQA merlots, sauvignon blancs and moscatos. Work is well underway to lay the foundation for marijuana legalization in this country, with legislation expected in the spring. Pot advocates have long argued legalization could give our economy a lift. A new report suggests that lift could surpass anyone's wildest prophecy. A study produced by the Deloitte firm – titled Recreational Marijuana: Insights and Opportunities – suggests a legal marijuana industry in Canada could be worth an incredible $22.6 billion – more than the sales of wine, spirits and beer combined. Deloitte's research values the recreational retail market for weed at between $5 billion and $8.7 billion annually. Tack on between $12.7 billion and $22.6 billion for the ancillary market (growers, specialty product makers, testing labs and security) and you have what Deloitte calls "a bold new landscape" for businesses and governments. But that's not all." Simcoe

Canada's Budget Office Estimates Cannabis Market Worth Hundreds of Millions During Flagship Year
According to Canada's Parliamentary Budget Office, sales tax revenues from legal cannabis could be between $356 million and $959 million once the drug is legalized nationwide, as is expected this spring. The figures are based on legal per gram prices between $7.48 and $9.34 with only federal and provincial sales tax applied. Parliamentary Budget Officer Jean-Denis Fréchette notes that the office expects the revenues to, eventually, climb into the billions of dollars and that the new sector will create both new revenues and expenses for the government. "Different products, such as edibles and concentrates, may require entirely different approaches to taxation," the report states. "These variations, along with others, each have different implications for market incentives and fiscal revenues." The PBO projects that in 2018 — the likely first year of legal sales — Canadians will consume between 378 and 1,017 metric tons of cannabis and that the legal market will be largely driven by individuals who consume the drug daily or

weekly. The office suggests that between 3.4 million and 6 million Canadians will consume cannabis at least once after it is legalized nationally. Ganjapreneur (2016-11-02)

Medical marijuana group one step closer to business
As Canadians reacted to news that Shoppers Drug Mart is exploring the possibility of selling medical marijuana in the near future, an independent retailer is finalizing the last steps in opening a medical marijuana dispencery within the Camrose area. Grant Gillott, the chief executive officer of htKa group — the acronym stands for honour, truth, knowledge and action — made a presentation to the Rotary Club of Camrose Oct. 17, discussing what the plans are heading forward. htKa have purchased a 66 acre lot outside the city limits, which Gillott said will leave lots of room for expansion as the market allows. "We see that as something that's almost inevitable," said Gillott. "We didn't want to get into a small site with a single building and try to do expansion and then have to go back through the application process." To reach the stage of owning land, htKa had to become certified with Health Canada in a five step process. The third step was to go through security clearance, that Gillott said took 22 months before they reached an 11 month review process, that they are currently finishing up. Now Gillott is ready to move forward, break ground and be licensed, and he hopes to be ready to go within the next 18 months. While many Canadians are still skeptical about the legalization of medical marijuana, Gillott said there are bussiness opportunities as as legal companies start moving forward. Camrose Canadian

PUBLIC SERVICE / FONCTION PUBLIQUE

Auditor General flags 'unacceptable' Phoenix pay glitches, PS pension costs
Auditor General Michael Ferguson turned the spotlight on the pay problems of Canada's public servants and the risks of the growing liabilities of their pension plans with the present low interest rates in his latest audit observations on the federal government's books. Ferguson, who audits the government's financial statements, gave the 2016 Public Accounts a clean audit, but he flagged the delays and errors of the Phoenix pay system as "unacceptable" and praised the government for re-examining the assumptions in determining pension liabilities in the face of prolonged low interest rates. Ferguson uses these notes or observations in his audit opinion to highlight issues for MPs to watch. Ferguson, along with senior bureaucrats from Treasury Board and Finance appear at the Commons public accounts committee Thursday to discuss the Public Accounts. On pensions, Ferguson's 2014 report urged the government to re-examine the design of the three defined-benefit plans for Canada's public servants, military and RCMP to ensure it can manage risks that could affect the long-term affordability and "sustainability" of the plans (…) Ferguson said he will be watching the impact of Phoenix in his upcoming audit of the 2017 financial statements. He is also undertaking a major investigation into Phoenix and the whole pay transformation project — at the request of Public Services Minister Judy Foote — to find out how the project went off the rails. It's unclear when that report will be completed. Ottawa Citizen

OTHER / AUTRES

Ottawa bringing in Air Passenger Bill of Rights: Garneau
The federal government will develop an air passenger bill of rights to better protect travellers, Transport Minister Marc Garneau told the Montreal Chamber of Commerce Thursday. (…) Canada's airport security screening is also under scrutiny. On Thursday, Garneau said Canadian travellers wait too long for security checks compared to their European counterparts. "Long lineups at screening checkpoints should be the exception but that is not the case," attendees were told. "Too many Canadians are waiting too long." Ottawa will develop international competitive targets aimed at ensuring Canadian airports keep up with other major hubs, Garneau said, like Germany and France. Meanwhile, the country's security agency, CATSA, will see its governance structure go under the microscope, while considering "new methods and new technologies." "We want achieve tangible improvements to the traveling experience," Garneau said. iPolitics; Toronto Star; Postmedia Network (National Post, Calgary Sun, Edmonton Sun, Toronto Sun, Ottawa Sun, Winnipeg Sun)

Liberals commit almost $350 million for Latvia mission to deter Russian aggression
The Trudeau government has set aside $348.6 million over the next three years for the deployment of a Canadian battle group in the Baltic States and ongoing air and sea patrols to counter the threat of Russian aggression on Europe's eastern flank. The Liberals have also renewed funding to support security forces and development assistance in Afghanistan until 2021. How much of the $465 million will be spent to prop up Afghan army and police units and how much has been earmarked for relief and capacity building is not clear. CBC News

INTERNATIONAL

Turkey's Erdogan says Germany has become 'haven for terrorists'
Turkish President Tayyip Erdogan said on Thursday Germany had become a haven for terrorists and would be "judged by history", accusing it of failing to root out supporters of a U.S.-based cleric Ankara blames for July's failed military coup. Erdogan said Germany had long harbored militants from the Kurdistan Workers Party (PKK), which has waged a three-decade insurgency for Kurdish autonomy, and far-leftists from the DHKP-C, which has carried out armed attacks in Turkey. Reuters; Deutsche Welle

Iraqi troops inside ISIS-held Mosul for first time since 2014
Iraqi forces have entered ISIS-held Mosul for the first time in more than two years, the Iraqi Defense Ministry said, in an operation to free the key city from the militant group's control. Iraqi Ministry of Defense spokesman Brig. Gen. Tahsin Ibrahim told CNN that units of the 9th Armored Division had entered the city, adding that troops had stormed the neighborhood of al Intisar in the east. CNN; Associated Press (CBC News)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

Tonda MacCharles
Trudeau says he's jealous that @RalphGoodale "gets to play" in the whole field of spies and intelligence agencies. Yep.

Tonda MacCharles
@RalphGoodale goes on "emergency preparedness".. ties it to Fort Mac forest fire, strength, courage of first responders &ppl, camaraderie.

Julie Van Dusen
Ralph Goodale has served under 2 Trudeau's - he recalls fires in Fort Mcmurray dealing with the "beast" #cdnpoli #hw

OpenMedia
Join the online conversation tonight and tell @RalphGoodale that Cdns want privacy reforms: http://ow.ly/y7eU305OEhH #YourNatlSec

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Canadian Red Cross
Six months ago, wildfires swept through #Alberta. Today, we thank every volunteer, donor, & Canadian who opened their hearts & homes.

Canadian Red Cross
Be ready for anything! An Emergency Preparedness Kit takes only minutes to assemble but could save you a lifetime.

Briar Stewart
Beautiful sunrise this morning in Prospect heights as rebuilding is underway #ymm #cbc @CBCNews

Glenn McGillivray
#FortMcMurray's next 6 priorities in #wildfire recovery

CBC Newfoundland
UPDATED | Searcher says helicopter 'only way in'

CBC News
From @briarstewart: In Fort McMurray rebuilding has begun, but the recovery continues http://www.cbc.ca/1.3834125 #ymmfire

UVic Anthropology
Canadian army interested in lost nuke that may have been found off west coast https://www.google.ca/amp/vancouversun.com/news/local-news/canadian-army-interested-in-old-nuke-that-may-have-been-found-off-haida-gwaii/amp?client=safari … @wellerstein

Vancouver Sun
Canadian army interested in old nuke that may have been found off Haida Gwaii

David Pugliese
Canadian military sends surveillance aircraft to Arctic to investigate mysterious pinging sounds http://natpo.st/2fl0lSG via @nationalpost

CP24
Toronto police reporting sulphuric acid spill in area of Bloor/ Lansdowne. Police asking residents to stay indoors, close doors and windows.

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

BC Civil Liberties
National security green paper is a whitewash - Azeezah Kanji http://on.thestar.com/2eiwxfS via @TorontoStar #cdnpoli #c51

BC Civil Liberties
National security review must acknowledge Canadian government's shortcomings http://bit.ly/2fqyHyO via @stevenzzhou @CBCNews #c51 #cdnpoli

Craig Forcese
Our brief today to the Commons privacy committee, re: reform of C-51's Security of Canada Information Sharing Act, http://craigforcese.squarespace.com/national-security-law-blog/2016/9/27/background-resources-bill-c-22-national-security-intelligenc.html …

NATIONAL SECURITY / SÉCURITÉ NATIONALE

CBC News Alerts
PM says he contacted CSIS, RCMP after learning of Quebec police surveillance of reporters; says nothing similar happening at federal level.

Tonda MacCharles
Trudeau: free press essential to democracy. "Concerned" & contacted RCMP, CSIS-no journo surveillance at fed level.

CBC – The Current
Where do we draw the line between freedom of the press and police surveillance? @Henheffer Listen here:

La Presse
DERNIÈRE HEURE: Espionnage des journalistes: Québec institue une commission d'enquête publique. #polqc

Radio-Canada
Surveillance des journalistes : le comité d'experts aura les pouvoirs d'une commission d'enquête annonce Québec http://ici.radio-canada.ca/breve/73179/surveillance-des-journalistes-le-comite-d-experts- ...

Raquel Fletcher
There will be a public inquiry into police spying on journalists, but Ministers Coiteux & Vallee don't know how far back it will go #polqc

Magazine L'actualité
«L'affaire #Lagacé représente une menace pour notre modèle traditionnel de #démocratie.» #polqc #Snowden #media http://www.lactualite.com/actualites/la-videoconference-de-snowden-a-ete-retardee-par-des-grevistes-a-montreal/ …

Edward Snowden
Oh, Canada... http://montrealgazette.com/news/local-news/police-surveillance-scandal-montreal-to-study-spying-issue-behind-closed-doors …

Motherboard
Edward Snowden calls police spying on Quebec journalists a "threat to democracy" http://bit.ly/2eDjJBW

CSIS Canada
Come meet Fed Gov recruiters at the Ottawa Shaw Centre, November 17, 2016 #secureyourcareer https://www.canada.ca/en/services/policing/career-fair.html …

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Rachel Browne
Chinese carfentanil business thrives at the cost of North American lives: http://globalnews.ca/news/3043678/chinese-trade-of-deadly-opioid-carfentanil-thrives-at-the-cost-of-north-american-lives/ … via @AP

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Kaspersky Lab
Unpatched #vulnerability on http://Wix.com puts millions of sites at risk via @threatpost https://kas.pr/T3rY #smb #smallbiz

LAW ENFORCEMENT / APPLICATION DE LA LOI

VICE Canada
Liquid fentanyl has been discovered in Canada for the first time: http://bit.ly/2fgzYWJ

CP24
Hamilton police discover liquid fentanyl during drug raid http://www.cp24.com/news/hamilton-police-discover-liquid-fentanyl-during-drug-raid-1.3144506 …

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

CP24
None of alleged trial errors raised by Rafferty on appeal occurred: Appeal Court http://cp24.to/u1Bm3yh

John Howard Society
Lauren Heuser: A dark age in our prisons: Time to end 'the dark ages of penal justice' http://natpo.st/2feXd1P via @fullcomment

John Howard Society
By the Numbers: The Complex Web of the #Reintegration of Formerly Incarcerated Persons in Ontario

John Howard Society
HOT OFF THE PRESS!!! @uofg & #JohnHowardSociety RELEASE REPORT CALLING FOR REAL CHANGE TO REINTEGRATION IN ONTARIO http://johnhoward.on.ca/wp-content/uploads/2016/11/JHSO-Press-Release-Effective-Reintegration-Final.pdf …

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Rachel Notley
Preventing family violence is every Albertan's responsibility. Learn more, including signs of abuse, at: http://www.endfamilyviolence.alberta.ca #ABFVPM

APTN
Does Thunder Bay police investigate Indigenous ppl in a discrminatory way? A review by @OIPRD_BDIEP hopes 2 find out https://goo.gl/zMZgon

Nicholas Keung
Canada chided for treatment of black people by UN group http://on.thestar.com/2flbo5L @TorontoStar

NCCM
These studies shouldn't be used to avoid the issue of racial profiling .@MoniaMazigh http://www.huffingtonpost.ca/monia-mazigh/racial-profiling-terrorism_b_12768662.html … via @HuffPostCanada #cdnpoli

VICE Canada
A young woman recounts her fentanyl addiction and painful recovery: http://bit.ly/2flj0n3

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

AmnestyCanada
Tune in @ 1 p.m. when we will be streaming our "Out of Sight, Out of Mind" report launch from Facebook live #mmiw >> http://amn.st/60128EUaa

PUBLIC SERVICE / FONCTION PUBLIQUE

Alison Crawford
Top executives at federal IT agency Shared Services Canada get $1.5 million in bonuses

Ottawa Citizen
Auditor General flags 'unacceptable' Phoenix pay glitches and public service pension costs http://ow.ly/nKKt305OXpJ

INTERNATIONAL

Phil Gurski
Muslim "crowds" attack Hindu temples and homes in Bangladesh

CNN International
Iraqi forces have entered ISIS-held Mosul for the first time in more than two years, the Iraqi Defense Ministry says http://cnn.it/2fhPstP

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

Today's News / Actualités
November 4, 2016 / le 4 novembre 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Civilian watchdog defends CSIS and embattled director over 'metadata'
Michel Coulombe, Canada's top spy, is in deep trouble with the courts and his political boss, **Public Safety Minister Ralph Goodale**, over revelations CSIS kept a decade's worth of data on Canadians who are no threat to national security. But Pierre Blais, head of the civilian watchdog agency over CSIS, says Coulombe "acted in good faith" and should not lose his job over the affair. "He's doing a good job. And that's a difficult issue, that we have to act as big girls and big boys and we look at this and we should do the best for the future," said Pierre Blais, chair of the Security Intelligence Review Committee

(SIRC)... Still, the judge said CSIS breached its ***"duty of candour"*** when it failed to reveal what it was up to. **Goodale said** Friday he first learned of it was two weeks ago when an unredacted copy of the pending judgment reached his desk. Asked point blank if he still has confidence in Coulombe, **the Public Safety Minister** would say only that he has made his expectations to the director abundantly clear. ***"A serious error has been made. (Coulombe) maintains that in his view, and in the view of the advice he got from the Department of Justice over the course of the last number of years, that the course of conduct by CSIS was within the parameters of law,"*** **Goodale told** reporters. ***"The court has now said very clearly and unequivocally that it was not. This situation needs to be remedied. It has to be remedied quickly . . . CSIS must be forthcoming and candid with the court. That will happen."*** Blais says Coulombe, who rose through the ranks of CSIS to become its head, should not resign or be fired, and expressed total confidence that he "is a very efficient person and he will make the correction that has to be done for the future no question about that." Asked if he was concerned CSIS had lied by omission to the courts, Blais said "lying, it's a very strong word." "As far as I'm concerned — I cannot say that; they never lied to the judge. They maybe (didn't) put everything that should have been presented to the judge," but he repeated "I'm sure that everybody's acting in good faith." A former chief justice of the Federal Court of Appeal who heard national security cases before taking the top job at SIRC, Blais was also once a Progressive Conservative solicitor general and justice minister, and said: "It's not that black and white all the time, particularly in this area. . . . It's never black and white, it's always grey, and we try to make sure that we do the best job possible in respecting the law." University of Ottawa law professor Craig Forcese said the debate over the scope of CSIS powers to collect and retain metadata "is one of these technical lawyerly discussions" but the Federal Court's findings about the spy agency's failure to be open and transparent are "very concerning" if not "astonishing" given that SIRC had recommended it disclose its activities to the court... **Goodale** left open the possibility of changing CSIS's governing legislation to allow new types of investigative techniques, noting the ruling said the CSIS Act could benefit from an update... **But Goodale was adamant** Friday that innocent people should not have their information tracked and stored by Canada's spies. ***"That's a fundamental principle of Canadian privacy,"*** **Goodale said.** Toronto Star

CSIS illegal data storage 'gross abuse of power': NDP

Revelations that Canada's spy agency has been illegally storing data not directly related to threats against national security for at least a decade continued to reverberate on Parliament Hill Friday. NDP justice critic Randall Garrison and public safety critic Matthew Dubé held a morning press conference to condemn the government for not revealing the behaviour, and to stress the need for committee of parliamentarians empowered to get to the bottom of such practices. "I think it reveals a gross abuse of power by Canada's spy agency," said Garrison. "This case makes clear the need for strong oversight of Canada's security agencies ... The bill which is before Parliament, Bill C-22, just simply doesn't do the job."... ***"A strong and timely remedial plan is required to assure the Federal Court about the issue of candour,"*** **said Public Safety Minister Ralph Goodale** in a press conference Friday morning, **stressing** the case shows the Security Intelligence Review Committee did its job by flagging this issue and bringing it to the Federal Court's attention. ***"I will discuss with the executive management of the service how they plan to respond to this judgment in full consultation with the Department of Justice,"*** **Goodale said** when asked specifically whether anyone might be fired over the metadata program. iPolitics

Former Ontario privacy commissioner wants CSIS metadata deleted

Information illegally held by Canada's spy agency over the course of a decade should be deleted from CSIS servers, according to Ontario's former information and privacy commissioner. Ann Cavoukian said metadata – the information included in a communication, such as a telephone number or email address – never should have been gathered because it included details on Canadians who didn't pose a security threat. "The Act is now more than 35 years old," said Jacques Shore, former director of research and investigation for the Security Intelligence Review Committee (SIRC), who now works as partner with Gowling WLG. "Clearly with new technologies, we have to address it." **Public Safety Minister Ralph Goodale said Friday he** was taking the finding ***"very seriously"*** and following up with CSIS top brass. ***"(CSIS) has confirmed to me that it is taking immediate steps to address the court's decision,"*** **Goodale said.** ***"It has blocked all access to, and analysis of, any associated data while it considers its next steps to comply."*** CTV News

Canada's spy agency may be hobbled by ruling on data collection

Canada's spy agency will not be able conduct normal operations until it assesses the effects of a court ruling that curtailed its ability to gather data and could make it less useful to key allies, say sources and officials. A federal court judge on Thursday said the Canadian Security Intelligence Service (CSIS) had secretly operated a data analysis center for 10 years and illegally retained electronic information from people in Canada who were not linked to particular security threats... CSIS could now also have trouble working with its allies in the so-called Five Eyes intelligence-sharing network, which also includes Britain, the United States, Australia and New Zealand, said a leading security expert. "The implications are major because the new constraints are now part of every warrant going forward," Christian Leuprecht, politics professor at the Royal Military College of Canada... If CSIS finds its ability to act is crimped it could in theory turn to the Royal Canadian Mounted Police, which shares responsibility for national security. Two sources with knowledge of the matter say relations between the agencies have deteriorated. Counterintelligence was originally handled by the RCMP's security service, but this was disbanded after a scandal and folded into the new CSIS in 1984 along with a new generation of civilian employees, a move that generated friction... CSIS officials said they retained the data in question because of its value. **Public Safety Minister Ralph Goodale**, who publicly criticized CSIS on Friday, **said** all intelligence and security agencies had to follow the law. Both agencies ultimately report to **Goodale**, **who said** CSIS director Michel Coulombe understood the need for immediate action in the wake of the court ruling. ***"A serious error has been made ... this situation needs to be remedied, it has to be remedied quickly," Goodale told reporters***. **He declined** to answer directly when asked whether he still had confidence in Coulombe, who has been in his position since May 2013. Reuters

What you need to know about the CSIS metadata ruling

A Federal Court judge's ruling this week that CSIS has been illegally storing Canadians' communications data for more than a decade has shed new light on the agency's secretive data analysis program. In his redacted ruling, Justice Simon Noël found the domestic spy agency held on to what it calls "associated data," vast amounts of data about private electronic communications obtained under warrant, long after it had decided the information was not related to a security threat... This practice, Noël wrote, goes beyond CSIS's limited mandate, which restricts its activities to those that are "strictly necessary for the purpose of protecting the security of Canada."... "We've heard the court loud and clear," Robert Frater, chief general counsel for the Department of Justice, who attended the press conference with Coulombe, said. "We are taking steps to improve our practices and we will meet that standard." Who knew about this operation? CSIS told the court that it had informed Stockwell Day, who was serving minister of public safety, about the associated data collection program. But Day refuted that claim in an interview with CBC News Network's Power & Politics. "If he is suggesting, or anybody, that they thought they told me something inappropriate was going on, yeah, I would suggest they did not." The current **public safety minister, Ralph Goodale**, **said Friday** the Security Intelligence Review Committee (SIRC) initially flagged possible problems with the collection and storage of associated data in a report tabled earlier this year. **Goodale said he** only became aware of the full extent of the problem recently, when Noël filed a preliminary report ***"a couple of weeks ago." "I took the immediate step of informing SIRC of the issue and asking SIRC to intervene in the situation to supervise the management of the data and to make sure that there was full compliance with the federal court's judgment," Goodale told*** reporters. CSIS does not need a warrant to review Revenue Canada files... **Goodale said** the Federal Court ruling is ***"timely"*** as it comes in the midst of the government's public consultations over the future of national security. **He has** already promised to launch a parliamentary oversight committee of CSIS, a promise the Liberals made after it tacitly endorsed parts of the controversial Bill C-51... Daniel Therrien, the country's privacy commissioner, told CBC News Friday that CSIS has already reached out to his agency to propose next steps. "At this point I can tell you that we welcome discussions on changes to CSIS policies required by the judgement. We also welcome a proposal from CSIS to meet to discuss their Privacy Impact Assessment for the Operational Data Analysis Centre and how it should be updated following the Court's decision." CBC News

A timeline of events in the case of CSIS's illegal data analysis

A timeline of events in the case of the Canadian Security Intelligence Service's illegal data analysis: 2005: A CSIS task force recommends the spy service retain all data collected from investigations and warrants in order to exploit that information in ongoing and future investigations through a technological program.

April 2006: CSIS sets up the Operational Data Analysis Centre (ODAC), a powerful program that processes metadata — the data trails associated with calls and messages, but not the actual content — to glean otherwise unknowable insights... January 2016: **Public Safety Minister Ralph Goodale tables** the 2014-15 annual report of the Security Intelligence Review Committee, the watchdog over CSIS. In reading it, Federal Court Justice Simon Noel understands for the first time that the service is retaining information collected through judicial warrants about people who were not actual targets of investigations. Noel directs CSIS to provide information at coming hearings concerning CSIS retention and use of metadata gathered through warrants. October 2016: In his ruling, Noel says CSIS violated the law by keeping potentially revealing metadata about people who were not under investigation over a 10-year period. **Goodale** receives a preliminary copy of the highly critical ruling. **He** immediately asks the intelligence review committee to supervise management of the data and ensure full compliance with the judgment. November 2016: A redacted version of the ruling is made public. CSIS says it has halted all access to, and analysis of, the data in question while it thoroughly reviews the court decision. **Goodale says** he expects CSIS to follow the court ruling. Canadian Press (Winnipeg Free Press, Metro News)

Commission d'enquête: Legault veut un examen de tous les corps policiers
Le chef de la Coalition avenir Québec, François Legault, estime que «tous les corps policiers du Québec» doivent être soumis à l'examen de la commission d'enquête chargée de se pencher sur la surveillance de journalistes. De passage à Montréal, vendredi, le chef caquiste a également réclamé que cette commission scrute attentivement la question de la nomination des directeurs de services policiers et les relations entre policiers et dirigeants politiques. «C'est un drôle de hasard que les deux derniers premiers ministres - ou première ministre - du Québec, dès leur arrivée, aient changé le directeur général de la SQ», a-t-il fait valoir. «Que M. (Stéphane) Bergeron (ancien ministre de la Sécurité publique) sente qu'il a le droit d'appeler le DG de la SQ pour demander ce qui se passe avec son ami Michel Arsenault de la FTQ, écoutez, c'est troublant. (...) Il y a beaucoup trop de proximité entre les chefs de police et les dirigeants politiques», a-t-il ajouté... Vendredi, aux Communes, **le ministre fédéral de la Sécurité publique, Ralph Goodale**, a reconnu que les révélations de la semaine au Québec sont ***«très inquiétantes»***, mais interrogé sur les gestes passés de la GRC et du SCRS, **il a clairement indiqué qu'il** n'avait pas l'intention d'aller fouiller dans les placards de ses organisations de sécurité. ***«La question porte sur ce qui se passe maintenant et nous pouvons offrir l'assurance que ce genre d'activité n'a pas lieu. Je ne sais rien sur les événements qui se sont produits lorsque nous (le Parti libéral du Canada) ne formions pas le gouvernement»,*** **a-t-il dit.** Presse Canadienne (La Presse, L'Actualité, Journal Métro)

Federal security review to examine CSIS powers in the digital age: Goodale
A federal review of national security will consider whether Canada's spy service should be able to sift through the kind of personal data it kept illegally for years, says **Public Safety Minister Ralph Goodale. Goodale** said Friday the notion that the Canadian Security Intelligence Service should avoid stashing away information about innocent people is a ***"fundamental principle of Canadian privacy."*** But the minister appeared to leave the door open to one day giving CSIS the legal authority to keep and analyze electronic data about individuals who do not pose a security threat. ***"I want to hear the professional advice on both sides,"*** **Goodale told** a news conference in the foyer of the House of Commons. ***"I'm not pre-empting the consultation."*** A Federal Court judge says CSIS violated the law by keeping potentially revealing electronic data about people who were not targets of investigation over a 10-year period...**Goodale said he** became aware of the ***"full scope of the issue"*** when the court judgment was made available to him in preliminary form a couple of weeks ago. **He said he** took the immediate step of informing the Security Intelligence Review Committee, the watchdog over CSIS, and asked the review committee to supervise management of the data and ensure full compliance with the judgment. Coulombe ***"understands my expectations here,"*** **Goodale added.** ***"A serious error has been made. This situation needs to be remedied. It has to be remedied quickly."*** The NDP said Friday the revelations underscore the need for stronger parliamentary oversight... **Goodale flatly** rejected the criticism, **saying** the committee would have extraordinary authority to look at classified information. Canadian Press (Chronicle-Herald, Metro News, Mississauga.com, Prince George Citizen)

Feds to appoint border crossing adviser
The federal government is set to appoint a special ministerial representative to look at border crossing issues faced by First Nations. In a joint letter written in response to a Senate committee study, Indigenous Affairs Minister Carolyn Bennett, Immigration Minister John McCallum and **Public Safety Minister Ralph Goodale** say the adviser and First Nations will discuss significant and complex challenges. It also says the resolution of these issues will require a "horizontal approach" involving several departments and agencies. The ministers say the results of the engagement between the representative and First Nations will shape the work of an interdepartmental committee of senior officials. The Senate committee on aboriginal peoples outlined border crossing issues in its June report. The committee said some First Nations believe they should have the right to freely cross the Canada-U.S. border, based on the 1794 Jay Treaty between Britain and the U.S. Canadian Press (Inside Ottawa Valley, CBC News); Presse Canadienne (Journal Métro)

Policing concerns in rural Saskatchewan prompt meeting of ministers - 'Public safety continues to be our challenge,' says Minister of Justice Gord Wyant
Saskatchewan's minister of justice says he went to the federal minister responsible for the RCMP over rural policing concerns. Gord Wyant said he and **Minister of Public Safety Ralph Goodale** agreed to have further meetings to discuss adequate RCMP deployment and resources allocated to this matter. "Public safety continues to be our challenge," said Wyant, adding that comments and concerns from the public prompted the meeting with the Saskatchewan MP. "We need to make sure that not only is the proper protection there, but people feel they are being protected," said Wyant. He said **Goodale is doing a review of vacancy management**. "I think that was a big concern that was expressed in rural Saskatchewan," said Wyant. **CBC has reached out to Goodale for comment.** CBC News; Radio-Canada

5 things to know about the CSIS metadata ruling
In a scathing ruling released Thursday, a Federal Court judge said the Canadian Security Intelligence Service illegally held on to potentially revealing electronic data about people over a 10-year timeframe. We break down the ramifications of the major decision and what it means for the future of Canada's spy agency: What do we know? Justice Simon Noel said CSIS held on to metadata that was not directly linked to threats to Canadian security... How has the government reacted? **Public Safety Minister Ralph Goodale said** the government won't appeal the decision and said he will follow up with CSIS top brass about the ruling. **He** added that ***"Canadians need to have confidence"*** about all federal departments and agencies. CTV News

MISE À JOUR : Canada - le renseignement rappelé à l'ordre pour abus de collecte de données
Le gouvernement canadien a rappelé à l'ordre vendredi le Service canadien du renseignement de sécurité (SCRS) reconnu coupable par un tribunal d'avoir mené une collecte "excessive" de données des citoyens, sans lien avec une menace précise à la sécurité nationale. ***"Le SCRS et toutes les agences de renseignement et de sécurité du gouvernement du Canada doivent respecter la loi"***, a **tonné le ministre de la Sécurité publique, Ralph Goodale**, après un jugement dévastateur rendu public jeudi par un tribunal fédéral***. "Le respect de la vie privée est très clairement une valeur canadienne fondamentale. Le respect de nos droits et libertés et de la justice est absolument fondamental"***, **a-t-il déclaré** lors d'une conférence de presse. La Cour fédérale a conclu que le SCRS avait violé son devoir d'être "franc" à son égard pour ne pas lui avoir dévoilé l'existence d'un programme qui, de 2006 à 2015, a permis de collecter et de conserver des métadonnées de tierces personnes, telles des numéros de téléphones et des adresses de courriel, sans que les personnes en question ne posent une quelconque menace à la sécurité nationale. ***"Le juge a conclu que la quantité d'informations collectées était excessive et injustifiée"***, **a rappelé M. Goodale** en réitérant que le gouvernement ne comptait pas faire appel de la décision. Michel Coulombe, directeur du SCRS, a indiqué jeudi que son organisme avait "déjà pris des mesures immédiates" comme la suspension de "tout accès aux données" obtenues en dehors des mandats ainsi que leur analyse... En vertu d'un projet de loi à l'examen au Parlement, ***"un nouveau comité parlementaire aura toute l'autorité pour examiner le travail de toutes nos agences de renseignement et de sécurité, non seulement du SCRS mais de toutes les autres aussi"***, **a dit M. Goodale.** Ce comité aura aussi le pouvoir d'examiner "les opérations en cours" de ces agences, a-t-il promis. Agence France-Presse (L'Orient le Jour)

UPDATE: Canadian Court Rules Spy Agency Illegally Kept Data Unrelated to Threats
A Canadian court issued a strong rebuke to the country's intelligence agency in a ruling released Thursday, saying the Canadian Security Intelligence Service broke the law by holding on to data that wasn't directly related to security threats... The issue of data collection has come under greater scrutiny since former U.S. National Security Agency contractor Edward Snowden revealed that agency was conducting surveillance of U.S. citizens... **Canada Public Safety Minister Ralph Goodale said** in a statement that the government doesn't intend to appeal the court's decision. **Speaking in Ottawa** early Friday, **Mr. Goodale said he** would follow up with the agency's executive management on its failure to inform the court of its actions. ***"CSIS must be forthcoming and candid with the court," he said. "That will happen." Mr. Goodale said*** a government-mandated watchdog, known as the Security Intelligence Review Committee, has also been tasked with supervising CSIS to ensure the data flagged by the court is dealt with properly. **The minister said he** first became aware of the issue through a report by the watchdog that was made public in January, but only learned the full scope of the CSIS program from the court's judgment. Wall Street Journal

Where is the review of intelligence analysis in CSIS?
An opinion piece by Stephanie Carvin, assistant professor of international relations at the Norman Paterson School of International Affairs at Carleton University and a former national security analyst with the federal government, states, "In a week dominated by headlines alleging the FBI meddling in the U.S. presidential election, and police surveillance of journalists in Quebec, Thursday's Federal Court ruling on CSIS's Operational Data Analysis Centre (ODAC) likely heightened the uncertainty many Canadians feel over the actions of our national security services... Although the Macdonald Commission desired to create a civilian intelligence agency, the character of CSIS continues to reflect the organization from which it was born – the 1970s RCMP. While the focus in the Act is rightly on stopping the "bad guys," other intelligence functions of national security organizations, especially analysis, are secondary considerations. Indeed, other than noting in Section 12(1) that the Service "shall report to and advise the Government of Canada" on national security threats, the role of intelligence analysis is barely given any consideration. There is no guidance as to how this role should be done, how intelligence should support operations or in what way advice is to be given... But complicating matters is the largely haphazard structure of the Canadian intelligence community's (IC) analytical branches. There is considerable overlap between several, including the Privy Council Office's Intelligence Assessment Secretariat, the Integrated Terrorism Assessment Centre (ITAC), and CSIS's analytical branches... On Thursday, **Public Safety Minister Ralph Goodale** stated that he was taking seriously the concerns about CSIS's bulk data collection activities. He must also take the time to consider what CSIS's analytical role should be and ensure there is appropriate oversight and review of its activities. After all, there are many excellent analysts in the government. Review will ensure their work helps Canada to be a safer place." Globe and Mail

CSIS must come clean on its spying
An editorial states, "So Canada's spy agency has gobs of people's metadata in a secret database. Well, it's just numbers, isn't it? You know, telephone numbers and Internet IP addresses and so forth. Who cares? The justice system, to begin with. On Thursday, the Federal Court released a ruling saying that the Canadian Security Intelligence Service's retention and analysis of wide swaths of data, which had been going on for 10 years, was illegal. And CSIS hadn't bothered to inform the court of what it was doing. This duplicity is unacceptable; keeping data you're not entitled to is a scandal that concerns all Canadians. And it's happening as a related mess unfolds in Quebec, where police have been spying on journalists, collecting their metadata too... Let's say your information, being scooped up by spies, shows a telephone call from your boss. Next, you telephone your mother. Then, you phone a number associated with a suicide hotline. What could be happening? It doesn't take a highly trained intelligence analyst to figure it out... **Public Safety Minister Ralph Goodale was shifty** on Friday when asked if the Liberals' planned security oversight committee would have stopped this sort of spying; instead **he** repeated talking points. **He also refused** to say how many Canadians had their data captured. Reassuringly, though, the government won't appeal the court ruling. But here are some questions CSIS and **the minister** still must answer: – How many Canadians had their privacy violated in this way? – Will their data be destroyed? If not, why not?... It's a bad day for our intelligence services. Shame on our spies. And on our lackadaisical oversight system." Ottawa Citizen

After trust has eroded, CSIS might get left out in the cold by ministers
An opinion piece states, ""Trust, but verify." Academics Craig Forcese and Kent Roach argue that this should be the maxim in the security sector when dealing with powerful state agencies like the Canadian Security Intelligence Service and the RCMP. But trust in Canada's security services is thin on the ground, after the news Thursday that a CSIS unit illegally kept data deemed unrelated to national security threats. **Public Safety Minister Ralph Goodale said Friday** that a Federal Court decision by Justice Simon Noel, who found CSIS has ***"breached, again, the duty of candour it owes the court,"*** is timely because the Liberals are in the midst of reviewing Canada's national security laws. The latest hit to the spy agency's reputation is unlikely to endear it to this government, and makes it more likely the Liberals will roll back what Forcese and Roach call the "outer limits" of C-51, the anti-terror legislation introduced last year by the Conservatives... Given the fact that the country's foremost jurists on national security law have repeatedly censured the spy agency for deliberately misleading them, it seems a good bet that the government will decide to shorten CSIS's leash. **Yet Goodale did not** rule out a change to the law to allow CSIS to keep the information ruled offside by the court. ***"This is an issue that I think needs to be examined in the context of our national security review,"*** **he said.** ***"I want to hear the professional advice on both sides ... Our security agencies to be effective in keeping Canadians safe. At the same time, what the agencies do needs to be in accord with the law and with the Constitution."*** Phil Gurski, a former CSIS analyst, said the metadata was retained for a reason — namely to identify people involved with, or sympathetic to, terror groups. "It was a legal opinion that this was illegal because the service is only allowed to retain information that is strictly necessary. I'm saying that it is strictly necessary and the data would inform future investigations."... Now trust has broken down, both with the judges who issue the warrants CSIS needs and with **the minister** to whom it answers. When consultations with Canadians over national security end, and the government reports back, the spies could find themselves left out in the cold." National Post

Broadcast Media / Médias télédiffusés :

CBC News Network's Power & Politics held a panel discussion with Parliamentary Secretary to **Minister of Public Safety**, Michel Picard, Conservative MP Michael Cooper, and NDP MP Murray Rankin regarding the Federal Court's ruling on CSIS' retainment of metadata. **Public Safety Minister Ralph Goodale** was quoted during this segment. Rough Transcript

CTV News' Power Play interviewed director of investigations with the Security Intelligence Review Committee, Jacques Shore, regarding the Federal Court's ruling on CSIS' retainment of metadata. **Public Safety Minister Ralph Goodale** was quoted during this segment. Rough Transcript

TOP STORIES / MANCHETTES

Animal Rights Groups, the KKK, and ISIS—the RCMP's New Guide To Extremism
For the past few years, the Canadian government has faced accusations that it's been asleep at the switch when it comes to stopping youth from being programmed by violent extremist groups. The Royal Canadian Mounted Police are striking back at that notion with a 140-page guide to radicalization, extremist groups operating in Canada, and terrorist groups abroad. The agency's Terrorism and Violent Extremism Awareness Guide, which was officially unveiled in October, "is intended for first responders, parents, colleagues or friends of persons at risk alike and is meant to help the reader to better understand and recognize the growing phenomenon of radicalization to violence." A large chunk of the report is just compiling resources on radicalization, offering different models that try to explain how someone might come around to violence and extremism based on their social, religious, and political beliefs. But the report also sheds light on exactly which domestic groups the RCMP are keeping an eye on. The report's language borrows heavily from internal security and intelligence assessments prepared by groups like the Canadian Security Intelligence Service and the Integrated Terrorism Assessment Centre... The RCMP also warns about the Internationalist Resistance (IR), which it describes as an "extremist anti-capitalist group." The classification is interesting, because the RCMP has spent the better part of a decade investigating a small group of Quebec Communists, accusing them of making up the central cell of the IR,

and for carrying out three bombings throughout Quebec from 2004 to 2010. A VICE Canada investigation raised questions about that investigation and whether the RCMP really has the right culprits. The RCMP report also names Skinheads Against Racial Prejudice and Red and Anarchist Skinheads, both committed to anti-fascism and anti-racism, as being two radical groups. Vice News

Quebec Mounties seek to launch discrimination lawsuit against RCMP
The association that represents RCMP members in Quebec is seeking to certify a class action lawsuit against the force on behalf of members across the country, alleging systemic harassment and discrimination against members by superiors. "There's some cases that have been done privately but on behalf of all members, this has never been done," said Frederic Serre, media officer for the Quebec Mounted Police Members Association. "You're looking at power trips and unfortunately there's a lot of it within the force … That's what we're trying to point out with this action." Serre said that although it's an association representing Quebec Mounties that's seeking to launch the suit, the class action is meant to represent all RCMP members across Canada — not just those in Quebec or francophones. iPolitics; Global News

City of Richmond: Volunteer cops need gun training
The amount of time Richmond's volunteer RCMP auxiliary constables are on the beat has dropped by 70 per cent this year, over 2014, after Mounties were ordered to have direct armed supervision of the complementary force and end all ride-along duties. Now, Richmond city council wants Ottawa to reinstate unsupervised duties for the unarmed auxiliary force and allow for firearms familiarization training. "We would like to see the auxiliary force back to what they used to be. It's been a great resource to augment our police force," said Coun. Bill McNulty. The city is backing a proposal by the Union of B.C. Municipalities to introduce a three-tier training program that would allow auxiliary constables to increase the number of duties they perform — such as public ceremonies, bike patrols and traffic and crowd control — without supervision. Richmond News

Boyfriend of pregnant killer Kelly Ellard a suspect in a 2016 disappearance
The boyfriend of pregnant killer Kelly Ellard is a suspect in the May 2016 disappearance of a low-level drug dealer, according to just released Parole Board of Canada documents. Darwin Dorozan had his parole revoked after Correctional Services of Canada officials were made aware of the investigation into Dorozan, the documents say. "On the same date full parole was granted, police advised CSC that you were a person of interest in the suspicious disappearance of a low-level drug dealer in May 2016," the parole board said in its Oct. 27 ruling...Her lawyer Sarah Rauch told Postmedia that they had known each other for about five years and that CSC followed all the rules in allowing them to have conjugal visits..."Corrections, as they do with everyone, does a huge scrutiny for a number of months if not a number of years," Rauch said. "Corrections did everything they always do in order to scrutinize the private family visits before granting them."... Under the Correction's mother-child program, there are currently six babies across Canada being cared for by their mothers in federal jails. Postmedia Network (Vancouver Sun, National Post)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

VIDEO & STORY: Port contributes $52,500 to Ground Search and Rescue
The Ground Search and Rescue team has grown from three to 16 volunteers since 2013 and to aid their efforts the Port of Prince Rupert has contributed $52,500 for training and equipment. Prince Rupert Ground Search and Rescue (PRGSAR) manager Dallas Allison was among the three who first revived the team and they had to use their own equipment. "We were incapable of recruiting because we're asking somebody to buy $2,000 worth of gear in order to join our team and volunteer," he said. Northern View

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Animal Rights Groups, the KKK, and ISIS—the RCMP's New Guide To Extremism
For the past few years, the Canadian government has faced accusations that it's been asleep at the switch when it comes to stopping youth from being programmed by violent extremist groups. The Royal Canadian Mounted Police are striking back at that notion with a 140-page guide to radicalization, extremist groups operating in Canada, and terrorist groups abroad. The agency's Terrorism and Violent Extremism Awareness Guide, which was officially unveiled in October, "is intended for first responders, parents, colleagues or friends of persons at risk alike and is meant to help the reader to better understand and recognize the growing phenomenon of radicalization to violence." A large chunk of the report is just compiling resources on radicalization, offering different models that try to explain how someone might come around to violence and extremism based on their social, religious, and political beliefs. But the report also sheds light on exactly which domestic groups the RCMP are keeping an eye on. The report's language borrows heavily from internal security and intelligence assessments prepared by groups like the Canadian Security Intelligence Service and the Integrated Terrorism Assessment Centre... The RCMP also warns about the Internationalist Resistance (IR), which it describes as an "extremist anti-capitalist group." The classification is interesting, because the RCMP has spent the better part of a decade investigating a small group of Quebec Communists, accusing them of making up the central cell of the IR, and for carrying out three bombings throughout Quebec from 2004 to 2010. A VICE Canada investigation raised questions about that investigation and whether the RCMP really has the right culprits. The RCMP report also names Skinheads Against Racial Prejudice and Red and Anarchist Skinheads, both committed to anti-fascism and anti-racism, as being two radical groups. Vice News

Broadcast Media / Médias télédiffusés :

CTV News' Power Play interviewed former Ontario Privacy Commissioner Ann Cavoukian regarding the privacy implications of CSIS' retainment of metadata. Rough Transcript

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

UB, Brock partner on cross-border business workshops
UB and Brock University will kick off a series of Cross-Border Innovation and Prosperity Workshops next week to advance a collaborative infrastructure for economic innovation across the binational Buffalo Niagara region. UB Now;

But United Way drive is about $30,000 behind from last year's pace
The United Way of Sarnia-Lambton campaign has slowed from its earlier pace and now stands at $1,360,000, or 68 per cent of the $2-million goal. The local fundraising campaign has slipped about $30,000 behind last year's pace at this point in time. This is significant because this year's $2-million goal represents last year's final achievement... The Department of Fisheries and Oceans wrapped up their employee campaign on Friday and sailed past their 2016 campaign goal by some 20 per cent, and Transport Canada also had a very successful drive. Canada Border Services are off to a great start. The Observer

Budget Travel: Airlines offering bargains to Europe
During recent phone calls to financial analysts asking why the recent profits for trans-Atlantic flights were down by as much as 9 percent, an official of the mighty Delta Airlines listed all the reasons you'd normally cite: the current presidential election season (which traditionally reduces international travel), a slowdown

in the European economy, the fear felt by numerous Americans of terrorist attacks overseas and so on... Nevertheless, if you live near the U.S./Canadian border and can drive to Toronto, you often can find an unusually low price to London and other European gateways. News Chief

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

Quebec Mounties seek to launch discrimination lawsuit against RCMP
The association that represents RCMP members in Quebec is seeking to certify a class action lawsuit against the force on behalf of members across the country, alleging systemic harassment and discrimination against members by superiors. "There's some cases that have been done privately but on behalf of all members, this has never been done," said Frederic Serre, media officer for the Quebec Mounted Police Members Association. "You're looking at power trips and unfortunately there's a lot of it within the force ... That's what we're trying to point out with this action." Serre said that although it's an association representing Quebec Mounties that's seeking to launch the suit, the class action is meant to represent all RCMP members across Canada — not just those in Quebec or francophones. iPolitics; Global News

City of Richmond: Volunteer cops need gun training
The amount of time Richmond's volunteer RCMP auxiliary constables are on the beat has dropped by 70 per cent this year, over 2014, after Mounties were ordered to have direct armed supervision of the complementary force and end all ride-along duties. Now, Richmond city council wants Ottawa to reinstate unsupervised duties for the unarmed auxiliary force and allow for firearms familiarization training. "We would like to see the auxiliary force back to what they used to be. It's been a great resource to augment our police force," said Coun. Bill McNulty. The city is backing a proposal by the Union of B.C. Municipalities to introduce a three-tier training program that would allow auxiliary constables to increase the number of duties they perform — such as public ceremonies, bike patrols and traffic and crowd control — without supervision. Richmond News

Drugs, guns, cash found during traffic stop near Fort Qu'Appelle
A loaded handgun, shotgun, cocaine and cash were found inside a vehicle RCMP stopped outside Fort Qu'Appelle. RCMP pulled over a vehicle on Highway 10 before midnight on Oct. 28. 980 CJME

Conception Bay South man arrested after child-luring investigation
A Conception Bay South man is facing charges of child luring after a five-month investigation. The 28-year-old man was arrested Friday without incident as a result of the investigation by the Combined Forces Special Enforcement Unit, an investigative unit comprising members of both the RCMP and the Royal Newfoundland Constabulary. CBC News

Almost $60K worth of drugs seized by London police
London police seized almost $60,000 worth of drugs during a raid on Thursday. Police executed a search warrant at an Adelaide Street residence in regards to methamphetamine trafficking. Police seized the following items during the warrant. CTV News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Meet the 21 new Trudeau-appointed senators
Prime Minister Justin Trudeau has appointed 21 new independent senators, further bolstering the number of non-affiliated members in the upper chamber to 44... Marc Gold is a constitutional law expert who has

held major leadership roles in the Jewish community at the local, national and international levels, including being Chair of Jewish Federations of Canada... He currently serves as a part-time member of the Parole Board of Canada and is an adjunct professor of law at McGill University. CBC News

Boyfriend of pregnant killer Kelly Ellard a suspect in a 2016 disappearance
The boyfriend of pregnant killer Kelly Ellard is a suspect in the May 2016 disappearance of a low-level drug dealer, according to just released Parole Board of Canada documents. Darwin Dorozan had his parole revoked after Correctional Services of Canada officials were made aware of the investigation into Dorozan, the documents say. "On the same date full parole was granted, police advised CSC that you were a person of interest in the suspicious disappearance of a low-level drug dealer in May 2016," the parole board said in its Oct. 27 ruling...Her lawyer Sarah Rauch told Postmedia that they had known each other for about five years and that CSC followed all the rules in allowing them to have conjugal visits..."Corrections, as they do with everyone, does a huge scrutiny for a number of months if not a number of years," Rauch said. "Corrections did everything they always do in order to scrutinize the private family visits before granting them."... Under the Correction's mother-child program, there are currently six babies across Canada being cared for by their mothers in federal jails. Postmedia Network (Vancouver Sun, National Post)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

'I am sending you home': Judge shows compassion for Sask. woman after Gladue report
An Ontario judge has decided to give a Regina woman a second chance. More than five years ago, the 31-year-old woman, originally from the Muskowekwan First Nation, was given a three-year sentence for robbery, arson and assault. She was also given long-term offender supervision for seven years. CBC News

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Algoma Public Health takes another kick at cannabis
Almost two years since its widely denounced initial foray into the medical marijuana business, Algoma Public Health has re-entered the cannabis fray. This time, there's no private company involved, no plans to grow cannabis in the Sault and no secret arrangements with the city. Soo Today

Shutting down pot shops – about time
An editorial states, "After months of "monitoring" and "investigating," Ottawa police are finally moving to close some of the many illegal private marijuana dispensaries that have been operating with impunity in Ottawa. Ottawa Citizen journalist Jacquie Miller reported this morning that an arrest had been made at Wee Medical Dispensary Society on Rideau street just east of Nelson Street. Reports then began coming in about raids on as many as six pot shops elsewhere in the city..." Ottawa Citizen

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

NIL

INTERNATIONAL

NIL

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

TimesTranscript
Federal security review to examine CSIS powers in the digital age, Goodale says ow.ly/x3dG305Sfh7 @TJProvincial @DailyGleaner pic.twitter.com/i48PvgTvpe

MacleansMag
Public safety minister promises a review of national security and CSIS after it was rebuked over data collection: ow.ly/5fS9305Sb1C

chronicleherald
VIDEO: Federal security review to examine CSIS powers in the digital age: Goodale herald.ca/u3X pic.twitter.com/1srHT2gcUr

NATIONAL SECURITY / SÉCURITÉ NATIONALE

natnewswatch
Civilian watchdog defends CSIS and embattled director over 'metadata' on.thestar.com/2elcQiq via @TorontoStar

amandacconn
CSIS illegal data storage a "gross abuse of power:" NDP #C51 #C22 #natsec ipolitics.ca/2016/11/04/csi…

CTVNews
Former Ontario privacy commissioner wants CSIS metadata deleted ow.ly/wkiH305Sh1E pic.twitter.com/VdbUKhzUXF

ReutersUK
Canada's spy agency may be hobbled by ruling on data collection reut.rs/2ea4rlk pic.twitter.com/DMNiiRyARh

CBCTechSci
What you need to know about the CSIS metadata ruling ift.tt/2f9QKWl pic.twitter.com/7EbjBsS9Wu

JimBronskill
A timeline of events in the case of CSIS's illegal data analysis metronews.ca/news/canada/20… #cdnpoli #hw

cforcese
RT @JimBronskill: A timeline of events in the case of CSIS's illegal data analysis metronews.ca/news/canada/20… #cdnpoli #hw

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

kkirkup
Feds to appoint special adviser on border crossing challenges for First Nations via @Cdnpress http://www.brandonsun.com/ #cdnpoli

MetroNewsCanada
RT @metroottawa: Feds to appoint special adviser on border crossing challenges for #FirstNations travelers ow.ly/ku1I305RUjV #CDNpoli

nationalpost
Via @fullcomment: John Ivison: After trust has eroded, CSIS might get left out in the cold by ministers ow.ly/p8DK506asi2

vicecanada
Animal rights groups, the KKK, and ISIS—the RCMP's new guide to extremism: bit.ly/2fLZLci pic.twitter.com/2Ra2uaCjlY

LAW ENFORCEMENT / APPLICATION DE LA LOI

CBCSaskatoon
Policing concerns in rural Saskatchewan prompt meeting of ministers cbc.ca/1.3837029 #yxe #ypa #yqr #skpoli #policing #sask

ipoliticsca
Quebec Mounties seek to launch discrimination lawsuit against RCMP| iPolitics ipoli.ca/2f2nJie pic.twitter.com/TV4feR8YjG

CJMENews
Drugs, guns, cash found during traffic stop near Fort Qu'Appelle. ow.ly/z0j3305RHs5

TheDailyDigest
Conception Bay South man arrested after child-luring investigation newfoundland.dailydigest.us/2016/11/04/con...

CBCNL
NEW | Conception Bay South man arrested after child-luring investigation cbc.ca/1.3837103 pic.twitter.com/6qGT4jLDGd

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

Today's News / Actualités
November 4, 2016 / le 4 novembre 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Civilian watchdog defends CSIS and embattled director over 'metadata'
Michel Coulombe, Canada's top spy, is in deep trouble with the courts and his political boss, **Public Safety Minister Ralph Goodale**, over revelations CSIS kept a decade's worth of data on Canadians who are no threat to national security. But Pierre Blais, head of the civilian watchdog agency over CSIS, says Coulombe "acted in good faith" and should not lose his job over the affair. "He's doing a good job. And that's a difficult issue, that we have to act as big girls and big boys and we look at this and we should do the best for the future," said Pierre Blais, chair of the Security Intelligence Review Committee

(SIRC)... Still, the judge said CSIS breached its ***"duty of candour"*** when it failed to reveal what it was up to. **Goodale said** Friday he first learned of it was two weeks ago when an unredacted copy of the pending judgment reached his desk. Asked point blank if he still has confidence in Coulombe, **the Public Safety Minister** would say only that he has made his expectations to the director abundantly clear. ***"A serious error has been made. (Coulombe) maintains that in his view, and in the view of the advice he got from the Department of Justice over the course of the last number of years, that the course of conduct by CSIS was within the parameters of law,"*** **Goodale told** reporters. ***"The court has now said very clearly and unequivocally that it was not. This situation needs to be remedied. It has to be remedied quickly . . . CSIS must be forthcoming and candid with the court. That will happen."*** Blais says Coulombe, who rose through the ranks of CSIS to become its head, should not resign or be fired, and expressed total confidence that he "is a very efficient person and he will make the correction that has to be done for the future no question about that." Asked if he was concerned CSIS had lied by omission to the courts, Blais said "lying, it's a very strong word." "As far as I'm concerned — I cannot say that; they never lied to the judge. They maybe (didn't) put everything that should have been presented to the judge," but he repeated "I'm sure that everybody's acting in good faith." A former chief justice of the Federal Court of Appeal who heard national security cases before taking the top job at SIRC, Blais was also once a Progressive Conservative solicitor general and justice minister, and said: "It's not that black and white all the time, particularly in this area. . . . It's never black and white, it's always grey, and we try to make sure that we do the best job possible in respecting the law." University of Ottawa law professor Craig Forcese said the debate over the scope of CSIS powers to collect and retain metadata "is one of these technical lawyerly discussions" but the Federal Court's findings about the spy agency's failure to be open and transparent are "very concerning" if not "astonishing" given that SIRC had recommended it disclose its activities to the court... **Goodale** left open the possibility of changing CSIS's governing legislation to allow new types of investigative techniques, noting the ruling said the CSIS Act could benefit from an update... **But Goodale was adamant** Friday that innocent people should not have their information tracked and stored by Canada's spies. ***"That's a fundamental principle of Canadian privacy,"*** **Goodale said.** Toronto Star

CSIS illegal data storage 'gross abuse of power': NDP

Revelations that Canada's spy agency has been illegally storing data not directly related to threats against national security for at least a decade continued to reverberate on Parliament Hill Friday. NDP justice critic Randall Garrison and public safety critic Matthew Dubé held a morning press conference to condemn the government for not revealing the behaviour, and to stress the need for committee of parliamentarians empowered to get to the bottom of such practices. "I think it reveals a gross abuse of power by Canada's spy agency," said Garrison. "This case makes clear the need for strong oversight of Canada's security agencies ... The bill which is before Parliament, Bill C-22, just simply doesn't do the job."... ***"A strong and timely remedial plan is required to assure the Federal Court about the issue of candour,"*** **said Public Safety Minister Ralph Goodale** in a press conference Friday morning, **stressing** the case shows the Security Intelligence Review Committee did its job by flagging this issue and bringing it to the Federal Court's attention. ***"I will discuss with the executive management of the service how they plan to respond to this judgment in full consultation with the Department of Justice,"*** **Goodale said** when asked specifically whether anyone might be fired over the metadata program. iPolitics

Former Ontario privacy commissioner wants CSIS metadata deleted

Information illegally held by Canada's spy agency over the course of a decade should be deleted from CSIS servers, according to Ontario's former information and privacy commissioner. Ann Cavoukian said metadata – the information included in a communication, such as a telephone number or email address – never should have been gathered because it included details on Canadians who didn't pose a security threat. "The Act is now more than 35 years old," said Jacques Shore, former director of research and investigation for the Security Intelligence Review Committee (SIRC), who now works as partner with Gowling WLG. "Clearly with new technologies, we have to address it." **Public Safety Minister Ralph Goodale said Friday he** was taking the finding ***"very seriously"*** and following up with CSIS top brass. ***"(CSIS) has confirmed to me that it is taking immediate steps to address the court's decision,"*** **Goodale said.** ***"It has blocked all access to, and analysis of, any associated data while it considers its next steps to comply."*** CTV News

Canada's spy agency may be hobbled by ruling on data collection

Canada's spy agency will not be able conduct normal operations until it assesses the effects of a court ruling that curtailed its ability to gather data and could make it less useful to key allies, say sources and officials. A federal court judge on Thursday said the Canadian Security Intelligence Service (CSIS) had secretly operated a data analysis center for 10 years and illegally retained electronic information from people in Canada who were not linked to particular security threats... CSIS could now also have trouble working with its allies in the so-called Five Eyes intelligence-sharing network, which also includes Britain, the United States, Australia and New Zealand, said a leading security expert. "The implications are major because the new constraints are now part of every warrant going forward," Christian Leuprecht, politics professor at the Royal Military College of Canada... If CSIS finds its ability to act is crimped it could in theory turn to the Royal Canadian Mounted Police, which shares responsibility for national security. Two sources with knowledge of the matter say relations between the agencies have deteriorated. Counterintelligence was originally handled by the RCMP's security service, but this was disbanded after a scandal and folded into the new CSIS in 1984 along with a new generation of civilian employees, a move that generated friction... CSIS officials said they retained the data in question because of its value. **Public Safety Minister Ralph Goodale**, who publicly criticized CSIS on Friday, **said** all intelligence and security agencies had to follow the law. Both agencies ultimately report to **Goodale**, **who said** CSIS director Michel Coulombe understood the need for immediate action in the wake of the court ruling. ***"A serious error has been made ... this situation needs to be remedied, it has to be remedied quickly," Goodale told reporters***. **He declined** to answer directly when asked whether he still had confidence in Coulombe, who has been in his position since May 2013. Reuters

What you need to know about the CSIS metadata ruling

A Federal Court judge's ruling this week that CSIS has been illegally storing Canadians' communications data for more than a decade has shed new light on the agency's secretive data analysis program. In his redacted ruling, Justice Simon Noël found the domestic spy agency held on to what it calls "associated data," vast amounts of data about private electronic communications obtained under warrant, long after it had decided the information was not related to a security threat... This practice, Noël wrote, goes beyond CSIS's limited mandate, which restricts its activities to those that are "strictly necessary for the purpose of protecting the security of Canada."... "We've heard the court loud and clear," Robert Frater, chief general counsel for the Department of Justice, who attended the press conference with Coulombe, said. "We are taking steps to improve our practices and we will meet that standard." Who knew about this operation? CSIS told the court that it had informed Stockwell Day, who was serving minister of public safety, about the associated data collection program. But Day refuted that claim in an interview with CBC News Network's Power & Politics. "If he is suggesting, or anybody, that they thought they told me something inappropriate was going on, yeah, I would suggest they did not." The current **public safety minister, Ralph Goodale**, **said Friday** the Security Intelligence Review Committee (SIRC) initially flagged possible problems with the collection and storage of associated data in a report tabled earlier this year. **Goodale said he** only became aware of the full extent of the problem recently, when Noël filed a preliminary report ***"a couple of weeks ago." "I took the immediate step of informing SIRC of the issue and asking SIRC to intervene in the situation to supervise the management of the data and to make sure that there was full compliance with the federal court's judgment," Goodale told*** reporters. CSIS does not need a warrant to review Revenue Canada files... **Goodale said** the Federal Court ruling is ***"timely"*** as it comes in the midst of the government's public consultations over the future of national security. **He has** already promised to launch a parliamentary oversight committee of CSIS, a promise the Liberals made after it tacitly endorsed parts of the controversial Bill C-51... Daniel Therrien, the country's privacy commissioner, told CBC News Friday that CSIS has already reached out to his agency to propose next steps. "At this point I can tell you that we welcome discussions on changes to CSIS policies required by the judgement. We also welcome a proposal from CSIS to meet to discuss their Privacy Impact Assessment for the Operational Data Analysis Centre and how it should be updated following the Court's decision." CBC News

A timeline of events in the case of CSIS's illegal data analysis

A timeline of events in the case of the Canadian Security Intelligence Service's illegal data analysis: 2005: A CSIS task force recommends the spy service retain all data collected from investigations and warrants in order to exploit that information in ongoing and future investigations through a technological program.

April 2006: CSIS sets up the Operational Data Analysis Centre (ODAC), a powerful program that processes metadata — the data trails associated with calls and messages, but not the actual content — to glean otherwise unknowable insights... January 2016: **Public Safety Minister Ralph Goodale tables** the 2014-15 annual report of the Security Intelligence Review Committee, the watchdog over CSIS. In reading it, Federal Court Justice Simon Noel understands for the first time that the service is retaining information collected through judicial warrants about people who were not actual targets of investigations. Noel directs CSIS to provide information at coming hearings concerning CSIS retention and use of metadata gathered through warrants. October 2016: In his ruling, Noel says CSIS violated the law by keeping potentially revealing metadata about people who were not under investigation over a 10-year period. **Goodale** receives a preliminary copy of the highly critical ruling. **He** immediately asks the intelligence review committee to supervise management of the data and ensure full compliance with the judgment. November 2016: A redacted version of the ruling is made public. CSIS says it has halted all access to, and analysis of, the data in question while it thoroughly reviews the court decision. **Goodale says** he expects CSIS to follow the court ruling. Canadian Press (Winnipeg Free Press, Metro News)

Commission d'enquête: Legault veut un examen de tous les corps policiers
Le chef de la Coalition avenir Québec, François Legault, estime que «tous les corps policiers du Québec» doivent être soumis à l'examen de la commission d'enquête chargée de se pencher sur la surveillance de journalistes. De passage à Montréal, vendredi, le chef caquiste a également réclamé que cette commission scrute attentivement la question de la nomination des directeurs de services policiers et les relations entre policiers et dirigeants politiques. «C'est un drôle de hasard que les deux derniers premiers ministres - ou première ministre - du Québec, dès leur arrivée, aient changé le directeur général de la SQ», a-t-il fait valoir. «Que M. (Stéphane) Bergeron (ancien ministre de la Sécurité publique) sente qu'il a le droit d'appeler le DG de la SQ pour demander ce qui se passe avec son ami Michel Arsenault de la FTQ, écoutez, c'est troublant. (...) Il y a beaucoup trop de proximité entre les chefs de police et les dirigeants politiques», a-t-il ajouté... Vendredi, aux Communes, **le ministre fédéral de la Sécurité publique, Ralph Goodale**, a reconnu que les révélations de la semaine au Québec sont ***«très inquiétantes»***, mais interrogé sur les gestes passés de la GRC et du SCRS, **il a clairement indiqué qu'il** n'avait pas l'intention d'aller fouiller dans les placards de ses organisations de sécurité. ***«La question porte sur ce qui se passe maintenant et nous pouvons offrir l'assurance que ce genre d'activité n'a pas lieu. Je ne sais rien sur les événements qui se sont produits lorsque nous (le Parti libéral du Canada) ne formions pas le gouvernement»,*** **a-t-il dit.** Presse Canadienne (La Presse, L'Actualité, Journal Métro)

Federal security review to examine CSIS powers in the digital age: Goodale
A federal review of national security will consider whether Canada's spy service should be able to sift through the kind of personal data it kept illegally for years, says **Public Safety Minister Ralph Goodale. Goodale** said Friday the notion that the Canadian Security Intelligence Service should avoid stashing away information about innocent people is a ***"fundamental principle of Canadian privacy."*** But the minister appeared to leave the door open to one day giving CSIS the legal authority to keep and analyze electronic data about individuals who do not pose a security threat. ***"I want to hear the professional advice on both sides,"*** **Goodale told** a news conference in the foyer of the House of Commons. ***"I'm not pre-empting the consultation."*** A Federal Court judge says CSIS violated the law by keeping potentially revealing electronic data about people who were not targets of investigation over a 10-year period...**Goodale said he** became aware of the ***"full scope of the issue"*** when the court judgment was made available to him in preliminary form a couple of weeks ago. **He said he** took the immediate step of informing the Security Intelligence Review Committee, the watchdog over CSIS, and asked the review committee to supervise management of the data and ensure full compliance with the judgment. Coulombe ***"understands my expectations here,"*** **Goodale added.** ***"A serious error has been made. This situation needs to be remedied. It has to be remedied quickly."*** The NDP said Friday the revelations underscore the need for stronger parliamentary oversight... **Goodale flatly** rejected the criticism, **saying** the committee would have extraordinary authority to look at classified information. Canadian Press (Chronicle-Herald, Metro News, Mississauga.com, Prince George Citizen)

Feds to appoint border crossing adviser
The federal government is set to appoint a special ministerial representative to look at border crossing issues faced by First Nations. In a joint letter written in response to a Senate committee study, Indigenous Affairs Minister Carolyn Bennett, Immigration Minister John McCallum and **Public Safety Minister Ralph Goodale** say the adviser and First Nations will discuss significant and complex challenges. It also says the resolution of these issues will require a "horizontal approach" involving several departments and agencies. The ministers say the results of the engagement between the representative and First Nations will shape the work of an interdepartmental committee of senior officials. The Senate committee on aboriginal peoples outlined border crossing issues in its June report. The committee said some First Nations believe they should have the right to freely cross the Canada-U.S. border, based on the 1794 Jay Treaty between Britain and the U.S. Canadian Press (Inside Ottawa Valley, CBC News); Presse Canadienne (Journal Métro)

Policing concerns in rural Saskatchewan prompt meeting of ministers - 'Public safety continues to be our challenge,' says Minister of Justice Gord Wyant
Saskatchewan's minister of justice says he went to the federal minister responsible for the RCMP over rural policing concerns. Gord Wyant said he and **Minister of Public Safety Ralph Goodale** agreed to have further meetings to discuss adequate RCMP deployment and resources allocated to this matter. "Public safety continues to be our challenge," said Wyant, adding that comments and concerns from the public prompted the meeting with the Saskatchewan MP. "We need to make sure that not only is the proper protection there, but people feel they are being protected," said Wyant. He said **Goodale is doing a review of vacancy management**. "I think that was a big concern that was expressed in rural Saskatchewan," said Wyant. **CBC has reached out to Goodale for comment.** CBC News; Radio-Canada

5 things to know about the CSIS metadata ruling
In a scathing ruling released Thursday, a Federal Court judge said the Canadian Security Intelligence Service illegally held on to potentially revealing electronic data about people over a 10-year timeframe. We break down the ramifications of the major decision and what it means for the future of Canada's spy agency: What do we know? Justice Simon Noel said CSIS held on to metadata that was not directly linked to threats to Canadian security... How has the government reacted? **Public Safety Minister Ralph Goodale said** the government won't appeal the decision and said he will follow up with CSIS top brass about the ruling. **He** added that ***"Canadians need to have confidence"*** about all federal departments and agencies. CTV News

MISE À JOUR : Canada - le renseignement rappelé à l'ordre pour abus de collecte de données
Le gouvernement canadien a rappelé à l'ordre vendredi le Service canadien du renseignement de sécurité (SCRS) reconnu coupable par un tribunal d'avoir mené une collecte "excessive" de données des citoyens, sans lien avec une menace précise à la sécurité nationale. ***"Le SCRS et toutes les agences de renseignement et de sécurité du gouvernement du Canada doivent respecter la loi"***, a **tonné le ministre de la Sécurité publique, Ralph Goodale**, après un jugement dévastateur rendu public jeudi par un tribunal fédéral***. "Le respect de la vie privée est très clairement une valeur canadienne fondamentale. Le respect de nos droits et libertés et de la justice est absolument fondamental"***, **a-t-il déclaré** lors d'une conférence de presse. La Cour fédérale a conclu que le SCRS avait violé son devoir d'être "franc" à son égard pour ne pas lui avoir dévoilé l'existence d'un programme qui, de 2006 à 2015, a permis de collecter et de conserver des métadonnées de tierces personnes, telles des numéros de téléphones et des adresses de courriel, sans que les personnes en question ne posent une quelconque menace à la sécurité nationale. ***"Le juge a conclu que la quantité d'informations collectées était excessive et injustifiée"***, **a rappelé M. Goodale** en réitérant que le gouvernement ne comptait pas faire appel de la décision. Michel Coulombe, directeur du SCRS, a indiqué jeudi que son organisme avait "déjà pris des mesures immédiates" comme la suspension de "tout accès aux données" obtenues en dehors des mandats ainsi que leur analyse... En vertu d'un projet de loi à l'examen au Parlement, ***"un nouveau comité parlementaire aura toute l'autorité pour examiner le travail de toutes nos agences de renseignement et de sécurité, non seulement du SCRS mais de toutes les autres aussi"***, **a dit M. Goodale.** Ce comité aura aussi le pouvoir d'examiner "les opérations en cours" de ces agences, a-t-il promis. Agence France-Presse (L'Orient le Jour)

UPDATE: Canadian Court Rules Spy Agency Illegally Kept Data Unrelated to Threats
A Canadian court issued a strong rebuke to the country's intelligence agency in a ruling released Thursday, saying the Canadian Security Intelligence Service broke the law by holding on to data that wasn't directly related to security threats... The issue of data collection has come under greater scrutiny since former U.S. National Security Agency contractor Edward Snowden revealed that agency was conducting surveillance of U.S. citizens... **Canada Public Safety Minister Ralph Goodale said** in a statement that the government doesn't intend to appeal the court's decision. **Speaking in Ottawa** early Friday, **Mr. Goodale said he** would follow up with the agency's executive management on its failure to inform the court of its actions. ***"CSIS must be forthcoming and candid with the court,"* he said. *"That will happen."* Mr. Goodale said** a government-mandated watchdog, known as the Security Intelligence Review Committee, has also been tasked with supervising CSIS to ensure the data flagged by the court is dealt with properly. **The minister said he** first became aware of the issue through a report by the watchdog that was made public in January, but only learned the full scope of the CSIS program from the court's judgment. Wall Street Journal

Where is the review of intelligence analysis in CSIS?
An opinion piece by Stephanie Carvin, assistant professor of international relations at the Norman Paterson School of International Affairs at Carleton University and a former national security analyst with the federal government, states, "In a week dominated by headlines alleging the FBI meddling in the U.S. presidential election, and police surveillance of journalists in Quebec, Thursday's Federal Court ruling on CSIS's Operational Data Analysis Centre (ODAC) likely heightened the uncertainty many Canadians feel over the actions of our national security services... Although the Macdonald Commission desired to create a civilian intelligence agency, the character of CSIS continues to reflect the organization from which it was born – the 1970s RCMP. While the focus in the Act is rightly on stopping the "bad guys," other intelligence functions of national security organizations, especially analysis, are secondary considerations. Indeed, other than noting in Section 12(1) that the Service "shall report to and advise the Government of Canada" on national security threats, the role of intelligence analysis is barely given any consideration. There is no guidance as to how this role should be done, how intelligence should support operations or in what way advice is to be given... But complicating matters is the largely haphazard structure of the Canadian intelligence community's (IC) analytical branches. There is considerable overlap between several, including the Privy Council Office's Intelligence Assessment Secretariat, the Integrated Terrorism Assessment Centre (ITAC), and CSIS's analytical branches... On Thursday, **Public Safety Minister Ralph Goodale** stated that he was taking seriously the concerns about CSIS's bulk data collection activities. He must also take the time to consider what CSIS's analytical role should be and ensure there is appropriate oversight and review of its activities. After all, there are many excellent analysts in the government. Review will ensure their work helps Canada to be a safer place." Globe and Mail

CSIS must come clean on its spying
An editorial states, "So Canada's spy agency has gobs of people's metadata in a secret database. Well, it's just numbers, isn't it? You know, telephone numbers and Internet IP addresses and so forth. Who cares? The justice system, to begin with. On Thursday, the Federal Court released a ruling saying that the Canadian Security Intelligence Service's retention and analysis of wide swaths of data, which had been going on for 10 years, was illegal. And CSIS hadn't bothered to inform the court of what it was doing. This duplicity is unacceptable; keeping data you're not entitled to is a scandal that concerns all Canadians. And it's happening as a related mess unfolds in Quebec, where police have been spying on journalists, collecting their metadata too... Let's say your information, being scooped up by spies, shows a telephone call from your boss. Next, you telephone your mother. Then, you phone a number associated with a suicide hotline. What could be happening? It doesn't take a highly trained intelligence analyst to figure it out... **Public Safety Minister Ralph Goodale was shifty** on Friday when asked if the Liberals' planned security oversight committee would have stopped this sort of spying; instead **he** repeated talking points. **He also refused** to say how many Canadians had their data captured. Reassuringly, though, the government won't appeal the court ruling. But here are some questions CSIS and **the minister** still must answer: – How many Canadians had their privacy violated in this way? – Will their data be destroyed? If not, why not?... It's a bad day for our intelligence services. Shame on our spies. And on our lackadaisical oversight system." Ottawa Citizen

After trust has eroded, CSIS might get left out in the cold by ministers
An opinion piece states, ""Trust, but verify." Academics Craig Forcese and Kent Roach argue that this should be the maxim in the security sector when dealing with powerful state agencies like the Canadian Security Intelligence Service and the RCMP. But trust in Canada's security services is thin on the ground, after the news Thursday that a CSIS unit illegally kept data deemed unrelated to national security threats. **Public Safety Minister Ralph Goodale said Friday** that a Federal Court decision by Justice Simon Noel, who found CSIS has ***"breached, again, the duty of candour it owes the court,"*** is timely because the Liberals are in the midst of reviewing Canada's national security laws. The latest hit to the spy agency's reputation is unlikely to endear it to this government, and makes it more likely the Liberals will roll back what Forcese and Roach call the "outer limits" of C-51, the anti-terror legislation introduced last year by the Conservatives... Given the fact that the country's foremost jurists on national security law have repeatedly censured the spy agency for deliberately misleading them, it seems a good bet that the government will decide to shorten CSIS's leash. **Yet Goodale did not** rule out a change to the law to allow CSIS to keep the information ruled offside by the court. ***"This is an issue that I think needs to be examined in the context of our national security review,"*** **he said.** ***"I want to hear the professional advice on both sides ... Our security agencies to be effective in keeping Canadians safe. At the same time, what the agencies do needs to be in accord with the law and with the Constitution."*** Phil Gurski, a former CSIS analyst, said the metadata was retained for a reason — namely to identify people involved with, or sympathetic to, terror groups. "It was a legal opinion that this was illegal because the service is only allowed to retain information that is strictly necessary. I'm saying that it is strictly necessary and the data would inform future investigations."... Now trust has broken down, both with the judges who issue the warrants CSIS needs and with **the minister** to whom it answers. When consultations with Canadians over national security end, and the government reports back, the spies could find themselves left out in the cold." National Post

Broadcast Media / Médias télédiffusés :

CBC News Network's Power & Politics held a panel discussion with Parliamentary Secretary to **Minister of Public Safety**, Michel Picard, Conservative MP Michael Cooper, and NDP MP Murray Rankin regarding the Federal Court's ruling on CSIS' retainment of metadata. **Public Safety Minister Ralph Goodale** was quoted during this segment. Rough Transcript

CTV News' Power Play interviewed director of investigations with the Security Intelligence Review Committee, Jacques Shore, regarding the Federal Court's ruling on CSIS' retainment of metadata. **Public Safety Minister Ralph Goodale** was quoted during this segment. Rough Transcript

TOP STORIES / MANCHETTES

Animal Rights Groups, the KKK, and ISIS—the RCMP's New Guide To Extremism
For the past few years, the Canadian government has faced accusations that it's been asleep at the switch when it comes to stopping youth from being programmed by violent extremist groups. The Royal Canadian Mounted Police are striking back at that notion with a 140-page guide to radicalization, extremist groups operating in Canada, and terrorist groups abroad. The agency's Terrorism and Violent Extremism Awareness Guide, which was officially unveiled in October, "is intended for first responders, parents, colleagues or friends of persons at risk alike and is meant to help the reader to better understand and recognize the growing phenomenon of radicalization to violence." A large chunk of the report is just compiling resources on radicalization, offering different models that try to explain how someone might come around to violence and extremism based on their social, religious, and political beliefs. But the report also sheds light on exactly which domestic groups the RCMP are keeping an eye on. The report's language borrows heavily from internal security and intelligence assessments prepared by groups like the Canadian Security Intelligence Service and the Integrated Terrorism Assessment Centre... The RCMP also warns about the Internationalist Resistance (IR), which it describes as an "extremist anti-capitalist group." The classification is interesting, because the RCMP has spent the better part of a decade investigating a small group of Quebec Communists, accusing them of making up the central cell of the IR,

and for carrying out three bombings throughout Quebec from 2004 to 2010. A VICE Canada investigation raised questions about that investigation and whether the RCMP really has the right culprits. The RCMP report also names Skinheads Against Racial Prejudice and Red and Anarchist Skinheads, both committed to anti-fascism and anti-racism, as being two radical groups. Vice News

Quebec Mounties seek to launch discrimination lawsuit against RCMP
The association that represents RCMP members in Quebec is seeking to certify a class action lawsuit against the force on behalf of members across the country, alleging systemic harassment and discrimination against members by superiors. "There's some cases that have been done privately but on behalf of all members, this has never been done," said Frederic Serre, media officer for the Quebec Mounted Police Members Association. "You're looking at power trips and unfortunately there's a lot of it within the force … That's what we're trying to point out with this action." Serre said that although it's an association representing Quebec Mounties that's seeking to launch the suit, the class action is meant to represent all RCMP members across Canada — not just those in Quebec or francophones. iPolitics; Global News

City of Richmond: Volunteer cops need gun training
The amount of time Richmond's volunteer RCMP auxiliary constables are on the beat has dropped by 70 per cent this year, over 2014, after Mounties were ordered to have direct armed supervision of the complementary force and end all ride-along duties. Now, Richmond city council wants Ottawa to reinstate unsupervised duties for the unarmed auxiliary force and allow for firearms familiarization training. "We would like to see the auxiliary force back to what they used to be. It's been a great resource to augment our police force," said Coun. Bill McNulty. The city is backing a proposal by the Union of B.C. Municipalities to introduce a three-tier training program that would allow auxiliary constables to increase the number of duties they perform — such as public ceremonies, bike patrols and traffic and crowd control — without supervision. Richmond News

Boyfriend of pregnant killer Kelly Ellard a suspect in a 2016 disappearance
The boyfriend of pregnant killer Kelly Ellard is a suspect in the May 2016 disappearance of a low-level drug dealer, according to just released Parole Board of Canada documents. Darwin Dorozan had his parole revoked after Correctional Services of Canada officials were made aware of the investigation into Dorozan, the documents say. "On the same date full parole was granted, police advised CSC that you were a person of interest in the suspicious disappearance of a low-level drug dealer in May 2016," the parole board said in its Oct. 27 ruling...Her lawyer Sarah Rauch told Postmedia that they had known each other for about five years and that CSC followed all the rules in allowing them to have conjugal visits..."Corrections, as they do with everyone, does a huge scrutiny for a number of months if not a number of years," Rauch said. "Corrections did everything they always do in order to scrutinize the private family visits before granting them."... Under the Correction's mother-child program, there are currently six babies across Canada being cared for by their mothers in federal jails. Postmedia Network (Vancouver Sun, National Post)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

VIDEO & STORY: Port contributes $52,500 to Ground Search and Rescue
The Ground Search and Rescue team has grown from three to 16 volunteers since 2013 and to aid their efforts the Port of Prince Rupert has contributed $52,500 for training and equipment. Prince Rupert Ground Search and Rescue (PRGSAR) manager Dallas Allison was among the three who first revived the team and they had to use their own equipment. "We were incapable of recruiting because we're asking somebody to buy $2,000 worth of gear in order to join our team and volunteer," he said. Northern View

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Animal Rights Groups, the KKK, and ISIS—the RCMP's New Guide To Extremism
For the past few years, the Canadian government has faced accusations that it's been asleep at the switch when it comes to stopping youth from being programmed by violent extremist groups. The Royal Canadian Mounted Police are striking back at that notion with a 140-page guide to radicalization, extremist groups operating in Canada, and terrorist groups abroad. The agency's Terrorism and Violent Extremism Awareness Guide, which was officially unveiled in October, "is intended for first responders, parents, colleagues or friends of persons at risk alike and is meant to help the reader to better understand and recognize the growing phenomenon of radicalization to violence." A large chunk of the report is just compiling resources on radicalization, offering different models that try to explain how someone might come around to violence and extremism based on their social, religious, and political beliefs. But the report also sheds light on exactly which domestic groups the RCMP are keeping an eye on. The report's language borrows heavily from internal security and intelligence assessments prepared by groups like the Canadian Security Intelligence Service and the Integrated Terrorism Assessment Centre... The RCMP also warns about the Internationalist Resistance (IR), which it describes as an "extremist anti-capitalist group." The classification is interesting, because the RCMP has spent the better part of a decade investigating a small group of Quebec Communists, accusing them of making up the central cell of the IR, and for carrying out three bombings throughout Quebec from 2004 to 2010. A VICE Canada investigation raised questions about that investigation and whether the RCMP really has the right culprits. The RCMP report also names Skinheads Against Racial Prejudice and Red and Anarchist Skinheads, both committed to anti-fascism and anti-racism, as being two radical groups. Vice News

Broadcast Media / Médias télédiffusés :

CTV News' Power Play interviewed former Ontario Privacy Commissioner Ann Cavoukian regarding the privacy implications of CSIS' retainment of metadata. Rough Transcript

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

UB, Brock partner on cross-border business workshops
UB and Brock University will kick off a series of Cross-Border Innovation and Prosperity Workshops next week to advance a collaborative infrastructure for economic innovation across the binational Buffalo Niagara region. UB Now;

But United Way drive is about $30,000 behind from last year's pace
The United Way of Sarnia-Lambton campaign has slowed from its earlier pace and now stands at $1,360,000, or 68 per cent of the $2-million goal. The local fundraising campaign has slipped about $30,000 behind last year's pace at this point in time. This is significant because this year's $2-million goal represents last year's final achievement... The Department of Fisheries and Oceans wrapped up their employee campaign on Friday and sailed past their 2016 campaign goal by some 20 per cent, and Transport Canada also had a very successful drive. Canada Border Services are off to a great start. The Observer

Budget Travel: Airlines offering bargains to Europe
During recent phone calls to financial analysts asking why the recent profits for trans-Atlantic flights were down by as much as 9 percent, an official of the mighty Delta Airlines listed all the reasons you'd normally cite: the current presidential election season (which traditionally reduces international travel), a slowdown

in the European economy, the fear felt by numerous Americans of terrorist attacks overseas and so on... Nevertheless, if you live near the U.S./Canadian border and can drive to Toronto, you often can find an unusually low price to London and other European gateways. News Chief

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

Quebec Mounties seek to launch discrimination lawsuit against RCMP
The association that represents RCMP members in Quebec is seeking to certify a class action lawsuit against the force on behalf of members across the country, alleging systemic harassment and discrimination against members by superiors. "There's some cases that have been done privately but on behalf of all members, this has never been done," said Frederic Serre, media officer for the Quebec Mounted Police Members Association. "You're looking at power trips and unfortunately there's a lot of it within the force ... That's what we're trying to point out with this action." Serre said that although it's an association representing Quebec Mounties that's seeking to launch the suit, the class action is meant to represent all RCMP members across Canada — not just those in Quebec or francophones. iPolitics; Global News

City of Richmond: Volunteer cops need gun training
The amount of time Richmond's volunteer RCMP auxiliary constables are on the beat has dropped by 70 per cent this year, over 2014, after Mounties were ordered to have direct armed supervision of the complementary force and end all ride-along duties. Now, Richmond city council wants Ottawa to reinstate unsupervised duties for the unarmed auxiliary force and allow for firearms familiarization training. "We would like to see the auxiliary force back to what they used to be. It's been a great resource to augment our police force," said Coun. Bill McNulty. The city is backing a proposal by the Union of B.C. Municipalities to introduce a three-tier training program that would allow auxiliary constables to increase the number of duties they perform — such as public ceremonies, bike patrols and traffic and crowd control — without supervision. Richmond News

Drugs, guns, cash found during traffic stop near Fort Qu'Appelle
A loaded handgun, shotgun, cocaine and cash were found inside a vehicle RCMP stopped outside Fort Qu'Appelle. RCMP pulled over a vehicle on Highway 10 before midnight on Oct. 28. 980 CJME

Conception Bay South man arrested after child-luring investigation
A Conception Bay South man is facing charges of child luring after a five-month investigation. The 28-year-old man was arrested Friday without incident as a result of the investigation by the Combined Forces Special Enforcement Unit, an investigative unit comprising members of both the RCMP and the Royal Newfoundland Constabulary. CBC News

Almost $60K worth of drugs seized by London police
London police seized almost $60,000 worth of drugs during a raid on Thursday. Police executed a search warrant at an Adelaide Street residence in regards to methamphetamine trafficking. Police seized the following items during the warrant. CTV News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Meet the 21 new Trudeau-appointed senators
Prime Minister Justin Trudeau has appointed 21 new independent senators, further bolstering the number of non-affiliated members in the upper chamber to 44... Marc Gold is a constitutional law expert who has

held major leadership roles in the Jewish community at the local, national and international levels, including being Chair of Jewish Federations of Canada... He currently serves as a part-time member of the Parole Board of Canada and is an adjunct professor of law at McGill University. CBC News

Boyfriend of pregnant killer Kelly Ellard a suspect in a 2016 disappearance
The boyfriend of pregnant killer Kelly Ellard is a suspect in the May 2016 disappearance of a low-level drug dealer, according to just released Parole Board of Canada documents. Darwin Dorozan had his parole revoked after Correctional Services of Canada officials were made aware of the investigation into Dorozan, the documents say. "On the same date full parole was granted, police advised CSC that you were a person of interest in the suspicious disappearance of a low-level drug dealer in May 2016," the parole board said in its Oct. 27 ruling...Her lawyer Sarah Rauch told Postmedia that they had known each other for about five years and that CSC followed all the rules in allowing them to have conjugal visits..."Corrections, as they do with everyone, does a huge scrutiny for a number of months if not a number of years," Rauch said. "Corrections did everything they always do in order to scrutinize the private family visits before granting them."... Under the Correction's mother-child program, there are currently six babies across Canada being cared for by their mothers in federal jails. Postmedia Network (Vancouver Sun, National Post)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

'I am sending you home': Judge shows compassion for Sask. woman after Gladue report
An Ontario judge has decided to give a Regina woman a second chance. More than five years ago, the 31-year-old woman, originally from the Muskowekwan First Nation, was given a three-year sentence for robbery, arson and assault. She was also given long-term offender supervision for seven years. CBC News

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Algoma Public Health takes another kick at cannabis
Almost two years since its widely denounced initial foray into the medical marijuana business, Algoma Public Health has re-entered the cannabis fray. This time, there's no private company involved, no plans to grow cannabis in the Sault and no secret arrangements with the city. Soo Today

Shutting down pot shops – about time
An editorial states, "After months of "monitoring" and "investigating," Ottawa police are finally moving to close some of the many illegal private marijuana dispensaries that have been operating with impunity in Ottawa. Ottawa Citizen journalist Jacquie Miller reported this morning that an arrest had been made at Wee Medical Dispensary Society on Rideau street just east of Nelson Street. Reports then began coming in about raids on as many as six pot shops elsewhere in the city..." Ottawa Citizen

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

NIL

INTERNATIONAL

NIL

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

TimesTranscript
Federal security review to examine CSIS powers in the digital age, Goodale says ow.ly/x3dG305Sfh7 @TJProvincial @DailyGleaner pic.twitter.com/i48PvgTvpe

MacleansMag
Public safety minister promises a review of national security and CSIS after it was rebuked over data collection: ow.ly/5fS9305Sb1C

chronicleherald
VIDEO: Federal security review to examine CSIS powers in the digital age: Goodale herald.ca/u3X pic.twitter.com/1srHT2gcUr

NATIONAL SECURITY / SÉCURITÉ NATIONALE

natnewswatch
Civilian watchdog defends CSIS and embattled director over 'metadata' on.thestar.com/2elcQiq via @TorontoStar

amandacconn
CSIS illegal data storage a "gross abuse of power:" NDP #C51 #C22 #natsec ipolitics.ca/2016/11/04/csi…

CTVNews
Former Ontario privacy commissioner wants CSIS metadata deleted ow.ly/wkiH305Sh1E pic.twitter.com/VdbUKhzUXF

ReutersUK
Canada's spy agency may be hobbled by ruling on data collection reut.rs/2ea4rlk pic.twitter.com/DMNiiRyARh

CBCTechSci
What you need to know about the CSIS metadata ruling ift.tt/2f9QKWl pic.twitter.com/7EbjBsS9Wu

JimBronskill
A timeline of events in the case of CSIS's illegal data analysis metronews.ca/news/canada/20… #cdnpoli #hw

cforcese
RT @JimBronskill: A timeline of events in the case of CSIS's illegal data analysis metronews.ca/news/canada/20… #cdnpoli #hw

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

kkirkup
Feds to appoint special adviser on border crossing challenges for First Nations via @Cdnpress http://www.brandonsun.com/ #cdnpoli

MetroNewsCanada
RT @metroottawa: Feds to appoint special adviser on border crossing challenges for #FirstNations travelers ow.ly/ku1l305RUjV #CDNpoli

nationalpost
Via @fullcomment: John Ivison: After trust has eroded, CSIS might get left out in the cold by ministers ow.ly/p8DK506asi2

vicecanada
Animal rights groups, the KKK, and ISIS—the RCMP's new guide to extremism: bit.ly/2fLZLci pic.twitter.com/2Ra2uaCjlY

LAW ENFORCEMENT / APPLICATION DE LA LOI

CBCSaskatoon
Policing concerns in rural Saskatchewan prompt meeting of ministers cbc.ca/1.3837029 #yxe #ypa #yqr #skpoli #policing #sask

ipoliticsca
Quebec Mounties seek to launch discrimination lawsuit against RCMP| iPolitics ipoli.ca/2f2nJie pic.twitter.com/TV4feR8YjG

CJMENews
Drugs, guns, cash found during traffic stop near Fort Qu'Appelle. ow.ly/z0j3305RHs5

TheDailyDigest
Conception Bay South man arrested after child-luring investigation newfoundland.dailydigest.us/2016/11/04/con...

CBCNL
NEW | Conception Bay South man arrested after child-luring investigation cbc.ca/1.3837103 pic.twitter.com/6qGT4jLDGd

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

Today's News / Actualités
November 7, 2016 / le 7 novembre 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

La GRC et la surveillance des journalistes: rien de rassurant
Une article d'opinion mentionne, « Depuis les révélations sur la surveillance des journalistes par la police de Montréal et la Sûreté du Québec, la réaction du gouvernement Trudeau a de quoi rendre perplexe. Et inquiet. Même si le premier ministre et ses ministres répètent que la liberté de la presse est un pilier «essentiel pour une démocratie qui fonctionne bien et une société libre», et qu'ils suivent cette situation de près, ils se comportent davantage comme un gouvernement qui souhaite que la controverse ne franchisse pas la rivière des Outaouais. Le **ministre de la Sécurité publique, Ralph Goodale**, qualifie la

surveillance des journalistes au Québec de «très inquiétante», mais il ne cherche pas à faire toute la lumière sur les agissements passés de la GRC et du SCRS... La semaine dernière, le commissaire de la GRC, Bob Paulson, a dit «ne pas être au courant» s'il y a eu des enquêtes ou de la surveillance à l'égard des journalistes, avant de préciser qu'il n'y en a pas «actuellement». Même réponse du premier ministre Justin Trudeau, qui a voulu se faire rassurant après avoir parlé à la GRC et au Service canadien de renseignement de sécurité (SCRS), affirmant qu'il n'y a «aucune activité de ce type au niveau fédéral actuellement». Mais jamais de réponse sur les activités passées, même récentes... **Le ministre Goodale** y est allé d'une belle contradiction. D'abord, il a affirmé aux journalistes à Ottawa que leurs questions sur les activités et les enquêtes de la GRC et du SCRS étaient dangereuses pour la séparation des pouvoirs entre le gouvernement et la police. ***«Vous allez sur une pente très dangereuse quand vous invitez les politiciens à aller dans ce domaine»***, a-t-il dit. Et dans le même point de presse, il a ajouté: ***«Je n'ai pas connaissance de choses qui se sont produites quand nous ne formions pas le gouvernement du Canada.»*** Faut-il en déduire que **M. Goodale** est au courant de ce qui se passe dans les opérations de la GRC et du SCRS lorsque son parti forme le gouvernement? Si oui, où est la séparation des pouvoirs à propos de laquelle le ministre sermonne les journalistes qui veulent en savoir plus? Et si un pilier de la démocratie est atteint au point d'inquiéter le ministre de la Sécurité publique, comme il l'affirme, pourquoi ce manque de curiosité sur les agissements récents de ses forces de l'ordre? Il ne s'agit pas d'intervenir dans des enquêtes en cours, mais de savoir si une telle surveillance a eu lieu de la part de la GRC et du SCRS dans le passé, et si oui, quand, pourquoi et à combien de reprise? **Le ministr**e ne veut-il pas savoir?... » L'actualité

Security forces must be held accountable
A letter states "Re: CSIS kept metadata illegally, court rules, Nov. 4 - Given the director of CSIS's recent display of contempt for Canada's Parliament, if not for our constitution, **Public Safety Minister Ralph Goodale** has no other option than to demand Michel Coulombe's resignation. It will send a strong message to all of our security forces from CSIS, CSEC, the RCMP and the Quebec police, on both the municipal and provincial levels, to respect our laws. The 1982 McDonald Commission found the RCMP Security Service, PROFUNC, had a history of bending and breaking the law, violating rights, and essentially waging clandestine wars against its self-labelled "enemies." In fact, it was the McDonald Commission which recommended the foundation of our civilian intelligence service. It was called CSIS. To continue to give Coulombe unsupervised and non-accountable power is an incredible risk to our democracy. I mean no disrespect to Coulombe for this comparison, but Canada does not need its own J. Edgar Hoover, the disgraced former director of the FBI, who was infamous for spying on citizens like Dr. Martin Luther King and later using this information as psychological warfare and blackmail." Vancouver Sun

TOP STORIES / MANCHETTES

Man accused in Tina Fontaine's killing claims police entrapped him
The woman who raised Tina Fontaine says she is confused and upset that the man charged with killing the teen is alleging that police entrapped him in an undercover operation and fabricated evidence to build their case... Raymond Cormier, who is facing a charge of second-degree murder in Tina's 2014 death in Winnipeg, told CBC News that he was "sucked into a 'Mr. Big' operation" – a controversial technique in which undercover officers create a fake underworld organization headed by a Mr. Big, who asks an individual for a confession to a crime, ostensibly so that the person can prove their criminal bona fides. Manitoba's Law Enforcement Review Agency, a non-police body that investigates public complaints of police misconduct, confirmed that Mr. Cormier filed a complaint about the investigation in July. Commissioner Max Churley said in an e-mail that he advised Mr. Cormier that the complaint is "outside the scope" of the province's Law Enforcement Review Act. Mr. Cormier launched an appeal, to be heard by a provincial court judge. The next hearing is slated for Nov. 23. Tina's death captured the country's attention and reignited calls for an independent inquiry into Canada's more than 1,181 missing and murdered indigenous women and girls. The two-year, $54-million national inquiry was launched in September. Globe and Mail

CBSA seizes over 100 kg of cocaine at border
The Canada Border Services Agency announced that its officers had seized a major seizure of cocaine from a commercial vehicle last month. A trucker was arrested after agents found 107.5 kilograms of cocaine hidden in a shipment of rice inside a vehicle at the Pacific Highway Commercial port of entry on Oct. 21. CBSA said in a news release that the cocaine and the man were turned over to the RCMP. The suspect's name was not released. The driver was headed north bound through the border when his truck was sent for a secondary inspection. Vancouver Sun; The Now; Cloverdale Reporter

Trudeau announces $1.5 billion national coastal strategy at Vancouver stop
Prime Minister Justin Trudeau announced Monday a five-year, $1.5 billion national Oceans Protection Plan to ensure "environmental sustainability" and "responsible commercial use"... The program "will make Canada a world leader in marine safety and takes a powerful step toward co-management of our coasts with Indigenous and coastal communities, together making sure they remain healthy, clean, and safe for generations to come," he said at a subsequent news conference at the Royal Canadian Navy's HMCS Discovery shore-based facility at Stanley Park... Trudeau's announcement today didn't include many of the specific requests that Victoria has put forward, including three new salvage rescue tugs costing up to $50 million apiece, a new $6 million CCG station in Prince Rupert, and funding for a maritime training centre at the B.C. Institute of Technology. The announcement also doesn't include any reference to Trudeau's promise to bring in a crude oil tanker ban for B.C.'s north coast. However, the government has insisted that campaign vow will be kept. Vancouver Sun; CBC News; Canadian Press (City News)

Police say alleged ISIL supporter broke off electronic ankle bracelet that let authorities track him
An Ottawa man the RCMP says it fears may engage in terrorism allegedly broke off his electronic ankle bracelet over the weekend, prompting police to take him into custody for the second time in two weeks. Tevis Gonyou-McLean, a 24-year-old alleged ISIL supporter, was arrested on Saturday. He has been charged with three counts of breaching his release conditions, uttering threats and mischief under $5,000. The Ottawa Police Service said Monday the mischief charge was for removing the GPS monitoring system Gonyou-McLean was required to wear following his arrest on a terrorism peace bond three months ago. National Post

Denis Coderre admits he spoke to ex-police chief about Patrick Lagacé
Montreal Mayor Denis Coderre has admitted he telephoned then-police chief Marc Parent in 2014 to talk about journalist Patrick Lagacé, just before police obtained search warrants to look at Lagacé's cell phone logs. But Coderre insists he did not ask Parent to investigate the La Presse columnist, who has been at the centre of the unfolding police surveillance scandal. "I never mix police and politics, no matter what people try to interpret," Coderre told reporters on Monday. Montreal police have confirmed investigators spied on Lagacé a second time, in 2014, during an investigation completely unrelated to the one revealed last week. CBC News; Canadian Press (Global News); Vice News; Globe and Mail

Independent police investigation called for after fatal accident in NW Saskatchewan
The RCMP are reporting a death after a short police pursuit Sunday night, which was called off just before the driver lost control. Around 9 o'clock, RCMP officers were conducting a check-stop in the Onion Lake area. A stopped vehicle sped off and a pursuit ensued, but was called off for public safety. Police say the lone male in the vehicle was pronounced dead at the scene. As a result, the Saskatchewan RCMP has requested an independent, external investigation around the circumstances, which will be conducted by the Regina Police Service. The RCMP has also requested the Ministry of Justice appoint an independent observer. CKRM; StarPhoenix; Global News

Edmonton Institution inmates launch lawsuit over solitary confinement
Three federal inmates at the Edmonton Institution are suing the Attorney General of Canada for more than $5.5-million over their solitary confinement that only ended when a judge stepped in. The inmates are each claiming their charter rights were violated after they were placed in segregation this summer for 43 days, 13 days more than is permitted under the Corrections and Conditional Release Act. In a statement of claim filed last month in Edmonton Court of Queen's Bench, the men claim several breaches of their charter rights, including that the segregation amounted to "cruel and unusual punishment" and

that their punishment was "grossly disproportionate" and failed to comply with principles of fundamental justice. CBC News

Why Canada's Prisons Abuse Solitary Confinement
An opinion piece states, "... Solitary confinement is only supposed to be used when other less restrictive alternatives have been exhausted or are rendered ineffective. So why has it seemingly become a standard practice? Long-term stays are linked to an ambiguous category in corrections—administrative segregation. While rules and regulations around segregation can differ between federal and provincial corrections, some experts say that administrative segregation is being deliberately overused and has actually become the go-to choice because it's easier to get away with. "Sometimes you see prison administrations themselves get very creative with how they justify keeping people in segregation," Correctional Investigator of Canada Howard Sapers told VICE... These practices target Indigenous inmates at a higher rate because they are more likely to be classified as maximum security and spend more time in segregation, according to the latest Correctional Investigator of Canada report released on Oct. 31. Specifically, Indigenous women are significantly over-represented in maximum security and make up 50 percent of the segregation placements in women's prisons, although they make up only about four percent of the Canadian population... While the number of inmates heading into solitary confinement federally has decreased over the past two years, it certainly hasn't disappeared. The Globe and Mail reported that "of all inmates released from segregation in the 2015-16 fiscal year" 246 had spent more than 120 days in isolation, although that's a drop from 498 the year before. It's not time to pop the cork on the congratulatory champagne just yet when, according to United Nations, segregation placements longer than 15 days can be considered "torture or other cruel, inhuman or degrading treatment or punishment." There's another problem. That only shows the numbers of inmates in for the long-haul of segregation in federal institutions. Once provincial numbers come in it's a much larger problem..." Vice News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Heavy rain, swelling rivers threaten Vancouver Island First Nation
A First Nation near Port Alberni, B.C., expects to evacuate some homes as heavy rains cause rivers to flood. Tseshaht Nation emergency preparedness co-ordinator Hugh Braker said the community has been sand bagging riverside properties and roads, but with up to 120 millimetres of rain expected by Wednesday, the risk for flooding remains high. Out buildings including garages and carports were damaged by flooding on the weekend, but no homes have been affected yet, Braker said. Six families who were forced to leave their homes on the weekend as a precaution were able to return, but a new round of evacuations is anticipated to begin Monday evening. Braker said the reserve's major thoroughfare, Highway 4, is also expected to be washed out by rising water levels, posing challenges for emergency crews as they try to reach people. Canadian Press (CTV News); Alberni Valley News

St. John's search and rescue centre to reopen by 2018
The St. John's Maritime Rescue Sub-Centre will reopen within 18 months. Fisheries Minister Dominc LeBlanc said Monday night that the federal government would restore the closed centre by 2018. The Coast Guard will also construct two new lifeboat stations in the province, and two new radars in Atlantic Canada... Before it was closed, the centre responded to about 500 incidents in an average year. CBC News; Canadian Press (Metro News)

Trudeau announces $1.5 billion national coastal strategy at Vancouver stop
Prime Minister Justin Trudeau announced Monday a five-year, $1.5 billion national Oceans Protection Plan to ensure "environmental sustainability" and "responsible commercial use"... The program "will make Canada a world leader in marine safety and takes a powerful step toward co-management of our coasts with Indigenous and coastal communities, together making sure they remain healthy, clean, and safe for generations to come," he said at a subsequent news conference at the Royal Canadian Navy's HMCS Discovery shore-based facility at Stanley Park... Trudeau's announcement today didn't include many of the specific requests that Victoria has put forward, including three new salvage rescue tugs costing up to $50 million apiece, a new $6 million CCG station in Prince Rupert, and funding for a maritime training

centre at the B.C. Institute of Technology. The announcement also doesn't include any reference to Trudeau's promise to bring in a crude oil tanker ban for B.C.'s north coast. However, the government has insisted that campaign vow will be kept. Vancouver Sun; CBC News; Canadian Press (City News)

B.C. premier says federal spill plan allays her concerns
Prime Minister Justin Trudeau has announced a $1.5-billion plan to protect Canada's oceans, which received immediate approval from B.C.'s premier, who has made "world-leading marine spill response" a condition for new heavy-oil pipelines. The premier's quick endorsement appears to remove a major barrier for major resource projects in B.C. such as Kinder Morgan's proposed Trans Mountain pipeline expansion, which the province has opposed in large part over concerns about oil spill cleanup. Mr. Trudeau said Monday that the federal Oceans Protection Plan will strengthen the Coast Guard, improve information sharing with an eye to prevent spills from happening, and strengthen laws to ensure owners of problem vessels are held responsible. Globe and Mail

Alberta to update immunization records to better respond to outbreaks
Alberta is moving to bring in new rules to get a handle on which children are immunized so that the province can better respond to outbreaks. The government introduced a bill Monday that would allow health officials to cross-match immunization records with school enrolment lists to see who is being overlooked. Canadian Press (Metro News)

Group says outdoor enthusiasts are not getting the message
Two searches in one week, on opposite sides of the island — one for a berry picker, the other a hunting guide — has the group responsible for searching for lost people reminding outdoor enthusiasts to 'be prepared' because it could happen to you. Bill Snelgrove, 82, spent a cold wet night in the woods in Conception Bay South, while, on the island's southwest coast, hunting guide Randy Hilliard spent three nights in a remote area of the Long Range Mountains. Both men lived to tell the tale. "They think they're prepared but they're really not," says Harry Blackmore, president of the Newfoundland and Labrador Search and Rescue Association. CBC News

UPDATED: Search continues for overdue boater on Slocan Lake
RCMP Sergeant Monty Taylor said in a media release Monday the search continues for a man last seen on Slocan Lake Wednesday (November 2). "The search for David Taylor continues," the RCMP Sergeant said in the release. "Since being reported missing the search has consisted over land, air and water utilizing ground searchers, boats, helicopter, RCMP float plane and Underwater Recovery Team, SONAR and underwater camera." RCMP was notified late Wednesday evening after Taylor had not returned from a 15-minute trip in a 14-foot aluminum boat on Slocan Lake at 7:30 p.m. Castlegar Source; Nelson Star

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Police say alleged ISIL supporter broke off electronic ankle bracelet that let authorities track him
An Ottawa man the RCMP says it fears may engage in terrorism allegedly broke off his electronic ankle bracelet over the weekend, prompting police to take him into custody for the second time in two weeks. Tevis Gonyou-McLean, a 24-year-old alleged ISIL supporter, was arrested on Saturday. He has been charged with three counts of breaching his release conditions, uttering threats and mischief under $5,000. The Ottawa Police Service said Monday the mischief charge was for removing the GPS monitoring system Gonyou-McLean was required to wear following his arrest on a terrorism peace bond three months ago. National Post

Are you ready for the new anti-money laundering rules?
The clock is ticking for financial institutions to comply with new regulations on how they verify the identities of their clients. Financial institutions have until June 17, 2017 to ensure they're following the new rules introduced under the Proceeds of Crime (Money Laundering) Anti-Terrorist Financing Act (PCMLTFA). "It's a short time to put a solution in place," Julia Szadowski, senior legal counsel with Equifax Canada, told participants in an ITWC webinar on the regulatory changes. "It's a challenge the whole industry is facing and the best way to face it is to be as vigilant and agile as possible"... Financial institutions need to be prepared because there are serious consequences for non-compliance with the rules, said Jim Love, ITWC CIO and host of the webinar. They include monetary penalties, criminal sanctions, and more importantly, reputational risk. FINTRAC has imposed fines totaling more than $3.5 million under the Act since December 30, 2008. IT World Canada

Denis Coderre admits he spoke to ex-police chief about Patrick Lagacé
Montreal Mayor Denis Coderre has admitted he telephoned then-police chief Marc Parent in 2014 to talk about journalist Patrick Lagacé, just before police obtained search warrants to look at Lagacé's cell phone logs. But Coderre insists he did not ask Parent to investigate the La Presse columnist, who has been at the centre of the unfolding police surveillance scandal. "I never mix police and politics, no matter what people try to interpret," Coderre told reporters on Monday. Montreal police have confirmed investigators spied on Lagacé a second time, in 2014, during an investigation completely unrelated to the one revealed last week. CBC News; Canadian Press (Global News); Vice News; Globe and Mail

CSIS and the Metadata Muddle Pt 1: What is this case really about?
An opinion piece by Craig Forcese states, "I have prepared a series of blog entries on Noël J's recent Federal Court judgment on CSIS's retention of metadata from its warranted threat investigations. In this first entry, I try to articulate what this case is about. It may be useful to start with an analogy (however imperfect): this case is about CSIS fishing in the sea for sharks. When it uses certain sorts of intrusive nets to sweep up sharks, that net use must be authorized by the court. But technology being what it is, the nets also sweep up other fish – a by-catch. The court accepted that by-catch can happen, but did not actually know what CSIS was doing with the by-catch. In fact, CSIS was keeping a fin from each fish caught in the by-catch. The court learned about this after 10 years of CSIS fin-collection. And then when it learned about it, the court concludes that the law governing CSIS obliged "catch-and-release": the by-catch fish should have been released unmolested once identified as by-catch and not sharks. Because CSIS did not do this, it acted unlawfully. Plus in failing to tell the court, it violated very strong duties that it do so. I will deal with the by-catch issue in this blog entry, and the duty of candour in a subsequent entry..." National Security Law

CSIS and the Metadata Muddle Pt 2: On Secret Law, Courts and the Rule of Law
An opinion piece by Craig Forcese states, "This is the second of a series of blog entries on Noël J's recent Federal Court judgment on CSIS's retention of metadata from its warranted threat investigations. In my first entry, I tried to explain what this case is about. In this blog entry, I begin to explore its implications, as I see them. First up: what a tangled web our legal system has weaved..." National Security Law

Dissecting CSIS' Statement Concerning Indefinite Metadata Retention
An opinion piece states, "In this brief post I debunk the language used by CSIS Director Michel Coulombe in his justification of CSIS's indefinite data retention program. That program involved CSIS obtaining warrants to collect communications and then, unlawfully, retaining the metadata of non-targeted persons indefinitely. This program was operated out of the Operational Data Analysis Centre (ODAC). A Federal Court judge found that CSIS' and the Department of Justice's theories for why the program was legal were incorrect: CSIS had been retaining the metadata, unlawfully, since the program's inception in 2006. More generally, the judge found that CSIS had failed to meet its duty of candour to the court by failing to explain the program, and detail its existence, to the Court. The public reactions to the Federal Court's decision has been powerful, with the **Minister of Public Safety** being challenged on CSIS's activities and numerous mainstream newspapers publishing stories that criticize CSIS' activities. CSIS issued a public statement from its Director on the weekend following the Court's decision, which is available at CSIS' website. The Federal Court's decision concerning this program is being hosted on this website, and is

also available from the Federal Court's website. In what follows I comprehensively quote from the Director's statement and then provide context that, in many cases, reveals the extent to which the Director's statement is designed to mislead the public…" Christopher Parsons

Orwell, quand la fiction devient la réalité
Une pièce d'opinion dit « Il y a de ces moments, dans la vie, où l'on se dit que le timing est irréprochable, et que des événements se produisant en rapide succession sont forcément liés par le destin, plutôt que de n'être que des coïncidences. La sortie d'Orwell, un jeu de gestion développé par la boîte allemande Osmotic Studios, est l'un de ces événements. Comment ne pas estimer, en effet, que l'arrivée de ce jeu de surveillance policière et d'espionnage étatique sur la plateforme Steam, le 27 octobre, ne tombe pas exactement au bon moment? Au Québec, mais aussi dans l'ensemble du pays, des affaires d'espionnage de journalistes et de simples citoyens font trembler les piliers de la démocratie, et remettent en question les fondements de la notion de vie privée. À l'échelon fédéral, le Service canadien de renseignement de sécurité (SCRS), a conservé pendant 10 ans une gigantesque banque de métadonnées sur la population, allant à l'encontre du principe de protection des informations personnelles. Tandis que chez nous, la Sûreté du Québec et la police de Montréal ont procédé au filtrage des registres d'appel et des métadonnées liées aux conversations téléphoniques d'une dizaine de policiers. Pire encore, on apprenait lundi matin que le maire de Montréal, Denis Coderre, aurait directement demandé au chef de la police de la métropole de s'intéresser à une affaire de contravention supposément impayée rapportée par Patrick Lagacé, un chroniqueur influent du journal La Presse. » Pieuvre.ca

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CBSA seizes over 100 kg of cocaine at border
The Canada Border Services Agency announced that its officers had seized a major seizure of cocaine from a commercial vehicle last month. A trucker was arrested after agents found 107.5 kilograms of cocaine hidden in a shipment of rice inside a vehicle at the Pacific Highway Commercial port of entry on Oct. 21. CBSA said in a news release that the cocaine and the man were turned over to the RCMP. The suspect's name was not released. The driver was headed north bound through the border when his truck was sent for a secondary inspection. Vancouver Sun; The Now; Cloverdale Reporter

Canada introducing gender-neutral option on visitor border document
Some foreign visitors to Canada will be allowed to identify themselves as male, female or other in a border document being introduced this week, officials said on Monday, as Canada joins a handful of nations offering gender neutral options. The new Electronic Travel Authorizations (eTAs) with three gender options will be introduced on Thursday for travelers flying into or through Canada, officials said. Canada also has taken steps toward allowing people who have changed genders to switch the designation on passports and other documents, said a spokeswoman for the Immigration, Refugees and Citizenship Canada (IRCC), the federal agency that issues travel documents. Reuters (Globe and Mail)

Federal Court dismisses bid to stop feds revoking citizenship without a hearing
A bid to stop the federal government from revoking Canadians' citizenship without a hearing has failed. Federal Court Justice Russell Zinn has dismissed a case brought by the Canadian Association of Refugee Lawyers and the British Columbia Civil Liberties Association. The two advocacy groups had sought a stay of a section of the Citizenship Act which allows the government to revoke the citizenship of anyone deemed to have misrepresented themselves — a provision which they argued could potentially ensnare Democratic Institutions Minister Maryam Monsef… The law is being challenged as unconstitutional but until that case is settled, the Federal Court has since January been systematically granting stays to individuals who apply for them… But Zinn ruled Monday that a blanket stay can only be ordered if the harm caused by the law is unavoidable. In this case, he said it is avoidable because any individual can apply to the court for a stay… The Liberals had denounced the law when they were in opposition and, since forming government, have promised to change it to provide for a proper hearing and appeal process for those believed to have misrepresented themselves to gain citizenship. However,

the government has so far refused to stop enforcing the law in the meantime. Canadian Press (Winnipeg Free Press)

Bill Lee wants to dissolve U.S.-Canadian border
Former Montreal Expos pitcher Bill "Spaceman" Lee says he'll work to dissolve the borders between Vermont, Quebec and the Maritime provinces if he is elected governor of the northeastern state Tuesday. Erasing the borders would allow Vermont to get its energy from the "biggest tides in the world" off the Atlantic Ocean, Lee says, describing his main election platform issue during an interview with The Canadian Press. The state will choose its governor the same day as the United States elects its president, and the former Major League Baseball pitcher is running with the Liberty Union Party, which describes itself as "non-violent" and "socialist." "We should form an alliance with the Maritime provinces," Lee, 69, said Monday. "That's an energy issue. We'll get all our energy from Canada." In an interview in which his remarks were difficult to distinguish between lighthearted banter and serious opinion, Lee said Canadians should have no problem incorporating Vermont because "we're just like you." Canadian Press (Guelph Mercury Tribune)

More Americans set their career sights north of the border
A growing number of Americans are setting their career sights north of the border, according to government and other data, and experts believe that is partly due to the spectre of a Donald Trump presidency. Data from Immigration, Refugees and Citizenship Canada (IRCC) shows a significant spike in the number of work permits being granted to American residents. The number of people receiving Canadian work permits in the first eight months of the year soared 54 per cent over the same period in 2015. Both the government and immigration lawyers say there have not been any policies to account for the increase. Canadian Press (City News; Times Colonist; Business News World)

Sorry Americans, you're just not our type
An opinion piece states, "… But for those of you thinking of moving to Canada as your Plan B, we're sorry. We really like newcomers, generally speaking. Canada takes in 250,000 annually, and this year has welcomed Syrian refugees by the planeload (or, as your Republican nominee says, by the Trojan horse load). But we can be a picky lot, and most of you need not apply. The median American adult is about in his or her mid-40s, and has not completed a college degree. Based on the criteria to enter the country as an economic immigrant—that is, not as a refugee or a Canadian's relative—those are two strikes against you. If you are not applying to migrate with a Canadian job already lined up in a field where there's a domestic skills shortage, that's more or less strike three…" Maclean's

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Meeting murderer Dale Ogden on Plenty of Fish highlights perils of online dating
Millions of people sign up for online dating websites in hopes of finding love, and it's not unusual to meet someone who isn't exactly the person they've made themselves out to be online. But the story of a British Columbia woman who learned the man she met online and dated for several weeks was a convicted killer is serving as a cautionary tale. CBC News

Unsealed Court Docs Show FBI Used Malware Like 'A Grenade'
In 2013, the FBI received permission to hack over 300 specific users of dark web email service TorMail. But now, after the warrants and their applications have finally been unsealed, experts say the agency illegally went further, and hacked perfectly legitimate users of the privacy-focused service. "That is, while the warrant authorized hacking with a scalpel, the FBI delivered their malware to TorMail users with a grenade," Christopher Soghoian, principal technologist at the American Civil Liberties Union (ACLU), told Motherboard in an email. Motherboard

Turks Are Flocking to Tor After Government Orders Block of Anti-Censorship Tools
Turkish internet users are flocking to Tor, the anonymizing and censorship-circumvention tool, after Turkey's government blocked Twitter, Facebook, and YouTube. Usage of Tor inside of Turkey went up

from around 18,000 users to 25,000 users on Friday, when the government started blocking the popular social media networks, according to Tor's official metrics. To prevent Turks from doing exactly that and connecting to the blocked sites through censorship-circumvention tools such as Tor and Virtual Private Networks (VPNs), the government took a step further and ordered internet providers to block those too. Motherboard

Raid on 20,000 Tesco Bank accounts fuels cybercrime fears
Tesco Bank, owned by Britain's biggest retailer Tesco, halted online transactions from all current accounts on Monday after money was stolen from 20,000 of them in the country's first such cyber heist. The bank, which manages 136,000 current accounts, said it would repay people who had lost money in the attack, which targeted 40,000 accounts in all and fuelled fears about the British financial sector's vulnerability. Tesco Bank's Chief Executive Benny Higgins told the BBC he thought "relatively small amounts" had been stolen, but the bank declined to give details of how much money in total had been taken or if it knew how the thefts had transpired. Other British banks have been targeted by hackers in recent years, but the Financial Conduct Authority (FCA) regulator said it was not aware of any previous incident in which customers had had money stolen. Reuters

UK privacy watchdog says Facebook agrees to suspend using WhatsApp users' data
Britain's privacy watchdog said on Monday that Facebook FB.O has agreed to suspend using data from UK users of its WhatsApp messaging app for advertisements or product-improvement purposes after the watchdog said consumers weren't properly protected. The watchdog said the social media giant faces action if it uses such data without valid consent. The Information Commissioner's Office (ICO) had said in August that it would monitor WhatsApp's new privacy policy, after WhatsApp, acquired by Facebook in 2014, said it would share user data with its parent company to better fight spam and improve users' experiences of both services. The two companies have also come under scrutiny from the European Union's 28 data protection authorities, who last month requested that WhatsApp pause sharing users' data with its parent company until the appropriate legal protections could be assured. Reuters

LAW ENFORCEMENT / APPLICATION DE LA LOI

Independent police investigation called for after fatal accident in NW Saskatchewan
The RCMP are reporting a death after a short police pursuit Sunday night, which was called off just before the driver lost control. Around 9 o'clock, RCMP officers were conducting a check-stop in the Onion Lake area. A stopped vehicle sped off and a pursuit ensued, but was called off for public safety. Police say the lone male in the vehicle was pronounced dead at the scene. As a result, the Saskatchewan RCMP has requested an independent, external investigation around the circumstances, which will be conducted by the Regina Police Service. The RCMP has also requested the Ministry of Justice appoint an independent observer. CKRM; StarPhoenix; Global News

Canada-wide warrants issued for violent offenders believed heading to Alberta
Prince George RCMP is asking the public to be on the lookout for two violent offenders believed to be heading to Alberta. Canada-wide warrants have been issued for 25-year-old Aaron Dueanne Conners and 29-year-old Blake Allan Morand after they failed to show up at their designated residence Sunday night. 660 News; Prince George Citizen

RCMP investigate suspicious death in Pelly Crossing
The Yukon RCMP's major crime unit is investigating after an 18-year old man died in Pelly Crossing Friday. Neither the man's name, nor circumstances surrounding his death have been released. Police say they're treating the death as suspicious. Yukon News

Man charged with indecent acts in Sherwood Park
A 21-year-old is facing charges after a man exposed himself to two people in Sherwood Park on Friday, say Mounties. Police said one person reported seeing a man expose himself and masturbate on the northwest side of Broadmoor Lake Park around 8:40 a.m. Shortly after, a second person flagged down a

police patrol and reported seeing a man walking and holding his genitals in his hand. A man was then arrested near Beauvista Drive, said Strathcona County RCMP. Edmonton Sun; Global News

How should police be policed? Oversight hearing in Hamilton Tuesday
Justice Michael Tulloch will be in Hamilton on Tuesday looking for public input on how police in Ontario should be policed. All three agencies that oversee policing in the province are facing questions about how well they serve the public interest and about their transparency and accountability. CBC News

RCMP reminds the public to beware of counterfeit money
There was a report about two occasions when two different banks in Drayton Valley received counterfeit US dollar bills. RCMP advises the public to beware of counterfeit money. According to Sgt. Erin Matthews, the counterfeit US dollar bills received by local banks have serial numbers stamped in red, but real US dollar bills do not have serial numbers stamped in red. Drayton Valley Western Review

Kamloops Mounties identify suspect in fatal hit and run
Police have identified a suspect in Friday's hit-and-run crash that left a Kamloops teenager dead on a residential street in Aberdeen, KTW has learned. The suspect did not turn himself in to police. Kamloops This Week

Ottawa police table draft 2017 budget with $8.9 million increase
Ottawa police tabled their draft budget for 2017 just hours after the force laid yet another a murder charge in a year that has seen a record number of shootings and homicides across the city. The police service proposed a budget that would increase by $8.9 million over next year, adding $11 to the average homeowner's tax bill. Ottawa Citizen; CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Edmonton Institution inmates launch lawsuit over solitary confinement
Three federal inmates at the Edmonton Institution are suing the Attorney General of Canada for more than $5.5-million over their solitary confinement that only ended when a judge stepped in. The inmates are each claiming their charter rights were violated after they were placed in segregation this summer for 43 days, 13 days more than is permitted under the Corrections and Conditional Release Act. In a statement of claim filed last month in Edmonton Court of Queen's Bench, the men claim several breaches of their charter rights, including that the segregation amounted to "cruel and unusual punishment" and that their punishment was "grossly disproportionate" and failed to comply with principles of fundamental justice. CBC News

Why Canada's Prisons Abuse Solitary Confinement
An opinion piece states, "... Solitary confinement is only supposed to be used when other less restrictive alternatives have been exhausted or are rendered ineffective. So why has it seemingly become a standard practice? Long-term stays are linked to an ambiguous category in corrections—administrative segregation. While rules and regulations around segregation can differ between federal and provincial corrections, some experts say that administrative segregation is being deliberately overused and has actually become the go-to choice because it's easier to get away with. "Sometimes you see prison administrations themselves get very creative with how they justify keeping people in segregation," Correctional Investigator of Canada Howard Sapers told VICE... These practices target Indigenous inmates at a higher rate because they are more likely to be classified as maximum security and spend more time in segregation, according to the latest Correctional Investigator of Canada report released on Oct. 31. Specifically, Indigenous women are significantly over-represented in maximum security and make up 50 percent of the segregation placements in women's prisons, although they make up only about four percent of the Canadian population... While the number of inmates heading into solitary confinement federally has decreased over the past two years, it certainly hasn't disappeared. The Globe and Mail reported that "of all inmates released from segregation in the 2015-16 fiscal year" 246 had spent more than 120 days in isolation, although that's a drop from 498 the year before. It's not time to pop the cork on the congratulatory champagne just yet when, according to United Nations, segregation

placements longer than 15 days can be considered "torture or other cruel, inhuman or degrading treatment or punishment." There's another problem. That only shows the numbers of inmates in for the long-haul of segregation in federal institutions. Once provincial numbers come in it's a much larger problem..." Vice News

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Confront scourge of sexual abuse, stand up for children, Inuit leaders demand
Prominent Inuit politicians are urging Canada's leaders — indigenous and otherwise — to protect children from the scourge of sexual abuse and suicide running through indigenous communities, saying no child deserves to have their innocence stolen. The head of Canada's national Inuit organization says it is incumbent upon all leaders to proclaim that abuse in indigenous communities is unacceptable. Canadian Press (Brandon Sun)

FSIN Chief Bobby Cameron stands by banishment of drug dealers on First Nations
The chief of Saskatchewan's Federation of Sovereign Indigenous Nations says he supports First Nations that exile criminals. Bobby Cameron, who represents 74 of the province's First Nations, says he backs banishment if it means getting rid of drug dealers or protecting young people from drugs and alcohol. An outraged Cameron says drug dealers in some communities are selling to 10-year-old kids and something has to be done to stop it. The chief says he supports a recent move by the Makwa Sahgaiehcan First Nation to banish six non-band members and give warnings to more than a dozen band members because of a crystal meth problem. Cameron says the RCMP has a big role to play too, helping band councils identify and stop drug dealers. Muskoday First Nation, Mistawasis First Nation and the Lac La Ronge Indian Band have also banished people to help control crime. Canadian Press (CKRM); Leader Post; CBC News

Liquid fentanyl seizure in Hamilton not the 1st in Canada
Health Canada says that the seizure of liquid fentanyl found in Hamilton that was announced last week is not the first in Canada, despite what Hamilton police investigators say. The national health agency also says Hamilton police knew the drug they had found was fentanyl in the summer, yet they did not release that information to the public until last week... "Health Canada's Drug Analysis Service (DAS) has received liquid samples for testing that have been found to contain fentanyl in the past," spokesperson Renelle Briand said in an email. CBC News

Drop-in centre for sex workers wins community safety award
Early every Friday morning between 5 a.m. and 8 a.m., sex workers drift into Daisy's Drop-In as their nighttime working day winds up. The drop-in is held in a west-end community centre, where child-sized chairs are stacked against one wall awaiting daytime programs. As dawn breaks, the women pick up clean needles, crack pipes and condoms. Nurses are available to offer testing for sexually transmitted infections, HIV, Hepatitis C and pregnancy. The sex workers warn each other about violent johns. Nikki Jalbert, the drop-in's counsellor, cooks up hot breakfasts in the kitchen. Some women grab naps, the only rest they will get all week in a warm place that is not a stairwell or a doorway... On Monday, Daisy's Drop-In won one of seven community safety awards from Crime Prevention Ottawa for its harm reduction approach that improves the lives of its clients and reduces harm to the community. Ottawa Citizen

B.C. mom jailed for making child porn using her own kids
A 37-year-old Fort St. James woman was sentenced Monday to 2 1/2 years in prison for making pornography involving her son and daughter and then sending the images and videos to a man she met through an Internet dating site. In issuing her decision, B.C. Supreme Court Justice Marguerite Church agreed entirely with Crown prosecution's decision on sentencing, noting it was actually at the low end of the range for the offences in question. Prince George Citizen

Stop sexual abuse on reserves: Editorial
An opinion piece states, "Women are taking the first step to stopping rampant sexual violence on First Nations reserves by coming forward to talk about it. Native and non-native leaders must provide victim support services and stop the cycle of violence..." Toronto Star

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Man accused in Tina Fontaine's killing claims police entrapped him
The woman who raised Tina Fontaine says she is confused and upset that the man charged with killing the teen is alleging that police entrapped him in an undercover operation and fabricated evidence to build their case... Raymond Cormier, who is facing a charge of second-degree murder in Tina's 2014 death in Winnipeg, told CBC News that he was "sucked into a 'Mr. Big' operation" – a controversial technique in which undercover officers create a fake underworld organization headed by a Mr. Big, who asks an individual for a confession to a crime, ostensibly so that the person can prove their criminal bona fides. Manitoba's Law Enforcement Review Agency, a non-police body that investigates public complaints of police misconduct, confirmed that Mr. Cormier filed a complaint about the investigation in July. Commissioner Max Churley said in an e-mail that he advised Mr. Cormier that the complaint is "outside the scope" of the province's Law Enforcement Review Act. Mr. Cormier launched an appeal, to be heard by a provincial court judge. The next hearing is slated for Nov. 23. Tina's death captured the country's attention and reignited calls for an independent inquiry into Canada's more than 1,181 missing and murdered indigenous women and girls. The two-year, $54-million national inquiry was launched in September. Globe and Mail

Messages supporting residential school survivors make up 'Healing Forest'
Handmade hearts containing messages of hope and love transformed a popular river valley trail into the city's first "Healing Forest." More than 1,000 hearts line the trail in honour of those affected by the legacy of residential schools in Alberta and across the country... While initially made to acknowledge residential school survivors, the idea is for the Healing Forest to be a place of reflection for missing and murdered Indigenous women as well as for children taken from their homes by the child welfare system. CBC News

Calgary police end search for Indigenous woman's body parts
The search for an Indigenous woman's remains at a Calgary landfill is over and that's news to her family. They say the Calgary Police Service hasn't kept them in the loop about the case of Joey English, 25. English's partial remains were found in the early morning on June 11, 2016, in a lightly forested area in the Crescent Heights neighbourhood. Calgary police told CBC the case is not being considered a homicide, but the family did not know that detail... The Calgary Police did not alert the family that they have ended their search. According to the family, police have not provided regular updates about the case. CBC News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Alberta researches legal weed market in Colorado
In an effort to prepare for Canada's coming legal recreational marijuana market, an Alberta government official visited Colorado recently to find out how that state's experiment with legal weed has worked out. Kathleen Ganley, provincial minister of justice, traveled to Colorado on Oct. 18 for a three-day trip to learn about the complex issues around legalization. She said she learned legalization will be a lot more involved than she expected. "We learned just how complex regulation around marijuana is going to be," Ganley said. Ganley said one lesson she learned in Colorado is the value of early action: It's important to have strict regulations in place before the first legal sale is made, because it's much harder to impose strict laws after the fact. Canadian Press (iPolitics)

Handful of marijuana dispensaries back in business, days after police raids
A stream of new customers dropped into the Weeds Glass & Gifts store on Bank Street Monday to purchase dried weed, cannabis cookies, brownies and oils. They flashed membership cards from the seven Ottawa marijuana dispensaries closed in police raids last week, said Weeds manager Kristina Simpson. The customers were politely turned away unless they could prove they need marijuana for medical reasons, said Simpson. Police investigators found the seven raided shops did not restrict their sales to medical patients, said Ottawa police Chief Charles Bordeleau. He said he hopes the raids send a warning to all dispensaries. That message had not prompted any changes by Monday morning, when a handful of the city's remaining pot shops were open for business, including Magna Terra on Carling Avenue, the Ottawa Medical Dispensary on Antares Drive, Sylk Medy on Gladstone Avenue and the Bank Street Weeds shop. (Three of the city's dispensaries are temporarily closed for other reasons — two were robbed at gunpoint and a third was hamstrung after its marijuana shipments from B.C. were seized by Canada Post.) Ottawa Citizen

Ottawa medical marijuana dispensary plans to stay open despite raids
An owner of one of the Ottawa medical marijuana dispensaries not targeted in a police operation last week is vowing to stay open, even if he has to take legal action to make that happen. Don Briere, owner of Weeds Glass and Gifts in Ottawa, as well as multiple similar stores in British Columbia, said he is not planning to close after Ottawa police raided other marijuana dispensaries last Friday. Metro News

Kettleman's Bagels contemplating a marijuana bagel
Could you one day be adding a half dozen bud bagels and some "herb" cream cheese to your Kettleman's order? "We are interested in your thoughts on this for bagels," reads a post added to the local business's Facebook page on Friday, linking to an article about cannabis being declared kosher. "Please let us know if you'd buy bagels if this became legal." Metro News

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Woman thrown from carriage after horse spooked by pipeline protest
A woman riding a horse-drawn carriage in Stanley Park was thrown off after the animal was apparently spooked by a protest nearby. The accident comes ahead of a planned announcement by Prime Minister Justin Trudeau as to how the federal government will handle spills off of B.C.'s coast. The prime minister is slated to make an announcement in Stanley Park alongside Transport Minister Marc Garneau. CTV News

INTERNATIONAL

FBI director under attack from own agents, Congress for handling of Hillary Clinton email inquiry
FBI Director James Comey was under attack from some of his own agents and members of Congress on Monday over his handling of an inquiry into Hillary Clinton's emails, but the White House was remaining supportive, for now. In stunning fashion, Comey has injected the Federal Bureau of Investigation, meant to be politically neutral, into the thick of the 2016 U.S. presidential race, making a series of announcements on the inquiry. Reuters (Global News)

US official: Security controls 'working' despite NSA theft
The top U.S. counterintelligence official says secret government data is vulnerable to thieves, such as the National Security Agency insider accused of working undetected for 20 years to steal a large trove of classified material, even as he defends the security controls put in place after the Edward Snowden theft.

"I believe the reforms are working very well. I think we've done an amazing job in the intelligence community and across the government in executing our reforms," said Bill Evanina, the chief counterintelligence and security adviser to the national intelligence director. "However, I will say that if someone wakes up tomorrow and they make a decision that they're going to steal data from the government, they will be successful at it." Evanina told The Associated Press in a recent interview that no matter how good security controls are, they will never catch every insider or hacker -- and they must be continually improved because of technological advances. His remarks were the most extensive comments he's made since former NSA contractor Harold Thomas Martin III, 51, of Glen Burnie, Maryland, was arrested by the FBI in August. Associated Press (CTV News)

Official: 40 to 50 buildings damaged in Oklahoma quake
Dozens of buildings sustained "substantial damage" after a 5.0 magnitude earthquake struck an Oklahoma town that's home to one of the world's key oil hubs, but officials said Monday that no damage has been reported at the oil terminal. Cushing City Manager Steve Spears said 40 to 50 buildings were damaged in Sunday's earthquake, which was the third in Oklahoma this year with a magnitude of 5.0 or greater. No major injuries have been reported, and Spears said the damage included cracks to buildings and fallen bricks and facades. Oklahoma has had thousands of earthquakes in recent years, with nearly all traced to the underground injection of wastewater left over from oil and gas production. Sunday's quake was centered 1 mile west of Cushing and about 25 miles south of where a magnitude 4.3 quake forced a shutdown of several wells last week. Associated Press (Yahoo! News)

20 Islamists Found Infiltrating German Army
At least 20 Islamists successfully infiltrated the German army and more may yet be uncovered, according to an investigation by Germany's military counter-espionage service (MAD). The news was reported on November 5 by Funke Mediengruppe, according to Deutsche Welle. A spokesperson for MAD said 60 additional individuals in the Bundeswehr were under investigation for suspected Islamist links. He said the army was contacted by a suspicious number of individuals seeking to join the army for a few months just to receive weapons training. Clarion Project

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

JustinTrudeau
Nous annonçons ajd notre Plan de protection des océans pour que nos côtes soient protégées, sûres et durables : http://pm.gc.ca/fra/nouvelles/

CTV_PowerPlay
On addressing tankers in distress, @MarcGarneau says the plan is to be able to handle all sizes of vessels on all of our coasts. #cdnpoli

cathmckenna
Notre Plan de Protection des Océans protégera les communautés du Canada Atlantique par de nouvelles mesures pr répondre aux incidents en mer

cathmckenna
So proud to be able to tell Atlantic Canadians about their Oceans Protection Plan: will improve spill response ½

cathmckenna
2/2 And it will strengthen our action in dealing with derelict & abandoned vessels off our beautiful coasts.

EmilyLazatin980
.@christyclarkbc says B.C. Will benefit from today's marine response anncmt but still waiting on details, says there is more work to do.

CTVNewsVI
Heavy rain, swelling rivers threaten Vancouver Island First Nation https://t.co/pmUYqfbWMr

Laura Kane
PM @JustinTrudeau about to tour this icebreaker in Vancouver's harbour ahead of an expected announcement on spill response. #cdnpoli #bcpoli

CBCChrisBrown
Asked about northern tanker ban, Trudeau basically answers "stay tuned"

CBCChrisBrown
Few specifics in #trudeaus measures today - FN can be rapid responders but no word on where new bases would go; nor where new tugs would go

CBCChrisBrown
Trudeau re Kinder Morgan: says today's measures are overdue. (Asked if this satisfies BCs "world class" spill requirements

CBCChrisBrown
Trudeau: re world class, now as good as Alaska, Norway. Says measures will increase tow capacities.

CBCChrisBrown
Trudeau: we invite indigenous communities to partner with us to protect our coastlines. #cdnpoli

CBCChrisBrown
First Nations are always the first responders: Trudeau

CBCNL
UPDATED: St. John's search and rescue centre to reopen by 2018 http://cbc.ca/1.3840548 #cbcnl #nlpoli

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Colinfreeze
The Greatest Hits of Secret Canadian Laws for Spy Agencies !! Brought to you by @JusticeCA !! via @cforcese http://craigforcese.squarespace.com/national-security-law-blog

Colinfreeze
Wherein @cforcese expresses understandable frustration with those who'd write their own rulebook & then lock it away http://craigforcese.squarespace.com/national-security-law-blog

Colinfreeze
Where @cforcese says the downstream effect of @csiscanada ruling is judges will no longer trust. They will verify. http://craigforcese.squarespace.com/national-security-law-blog

caparsons
CSIS And The Metadata Muddle Pt 1: What Is This Case Really About?
http://craigforcese.squarespace.com/national-security-law-blog

cforcese
CSIS & the Metadata Muddle, Pt 2: On Secret Law, Courts & the Rule of Law,
http://craigforcese.squarespace.com/national-security-law-blog #natsec #cdnpoli

StewartBellNP
Ottawa ISIL supporter broke off electronic ankle bracelet, police say. http://natpo.st/2fUlWfj @nationalpost

BC Civil Liberties
Spy watchdog that triggered scathing rebuke of illegal #CSIS activities facing job cuts
http://bit.ly/2fy5E8G @theprovince #c51 #cdnpoli

OpenMediaOrg

Any remaining trace of trust in Canadian #surveillance agencies has been irreversibly lost. @mgeist explains why: http://ow.ly/iXlP305Wqc2

CBC News
CSIS chief argues data was collected legally, but accepts court ruling http://www.cbc.ca/1.3838968

poirieryvesTVA
Le syndicat des policiers réplique au maire Coderre. "Les relations de travail ne sont pas responsables de l'espionnage de journalistes."

vicecanada
Montreal mayor asked cops to check into a journalist, says he's the real victim: http://bit.ly/2ePoSqi

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Sheila_Scott
#CokeBust: CBSA says 107.5 KG of cocaine hidden w/ rice in a commercial vehicle was seized from the Pac Highway Truck crossing last month

Sheila_Scott
That's about 236 pounds of suspected cocaine. RCMP investigating

MacleansMag
Want to move to Canada in the event of a President Trump? We may not want you: https://t.co/4QGdd2QaDz

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

motherboard
Unsealed court documents show FBI used malware "like a grenade" http://bit.ly/2fyxEZI

motherboard
Turks are flocking to Tor after government blocks popular sites like Facebook and YouTube http://bit.ly/2eGnVTB

LAW ENFORCEMENT / APPLICATION DE LA LOI

620ckrm
Independent police investigation called for after fatal accident in NW Saskatchewan. More at http://bit.ly/2eGQmkF

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

John Howard Society
#MentalIllness #addiction & broken system turned Jamie's perfect life into a perfect nightmare http://www.lfpress.com/2016/10/09/indiscernible-mental-illness-addiction-and-a-broken-system-turned-jamie-highs-perfect-life-into-the-perfect-nightmare … via @randyratLFPress

John Howard Society
Lessons Learned From 1,500 Days in Isolation - https://www.hrw.org/news/2016/11/01/lessons-learned-1500-days-isolation … #AdamCapay #solitaryconfinement #segregation

StewartBellNP
Government announces online public consultations on what to have for dinner. #FakeHeadlinesThatCouldBeReal

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

620ckrm
FSIN Chief Bobby Cameron stands by banishment of drug dealers on First Nations. http://bit.ly/2exA8gl

BC Civil Liberties
Government to reduce #mandatoryminimum sentences http://bit.ly/2eFW7il via @RCInet #cdnpoli

OttawaCitizen
Drop-in centre for sex workers wins community safety award http://ow.ly/j4DA305WU0t

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

OpenCanada
We're headed to the #COPAwards tonight! ICYMI - @AngelaSterritt's A Movement Rises is up for best feature! https://t.co/T2fuKBJN8l

AngelaSterritt
Content Warning(CW): Journalist learns about end of a search for Indigenous woman's body parts before family. http://www.cbc.ca/1.3839918

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

OttawaCitizen
Handful of marijuana dispensaries back in business, days after police raids http://ow.ly/qNuJ305WYkj

OTHER / AUTRES

darcynews
Reports of several people injured after horses spooked by Kinder Morgan pipeline protest bolt onto Stanley Park seawall.

CTVNewsBen
Kinder Morgan protestors chanting as Prime Minister Justin Trudeau leaves announcement about oil spill response. @CTVVancouver #cdnpoli

INTERNATIONAL

StewartBellNP
Ohio man arrested at airport was on his way to Libya to join ISIL, FBI says.

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

Today's News / Actualités
November 11, 2016 / le 11 novembre 2016
09:00 - 18:00 ET

This collection contains news items that appeared online between 9:00 a.m. and 6:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 09h00 et 18h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Canopy Growth Corp becomes Canada's first billion dollar marijuana stock
When it comes to Canada's sizzling medical marijuana sector, a million dollars just isn't cool anymore. Well, at least not for Canopy Growth Corp (TSX:CGC)... Medical marijuana stock began to gain serious attention from market watchers a few months into this year, when comments from **Canada's Minister of Public Safety Ralph Goodale** were interpreted as a sign that marijuana legalization was closer to becoming a reality than previously thought, a development that is generally regarded as good news for Licensed Producers. ***"The preset regime with respect to marijuana has obviously failed and failed***

miserably because Canadian teenagers are among the heaviest users of marijuana in the Western Word, yet there has been no timeline set by the federal government," **Goodale told** CBC's "On The Coast" host Stephen Quinn. Cantech Letter

New Regina lab will use data to predict potential critical events
A new data-crunching centre in Regina is hoping to predict when potential critical events may happen. A centre of excellence for data analytics opened its doors Thursday on the University of Regina campus. The lab is a partnership between Information Services Management (ISM Canada) and the province of Saskatchewan. ISM Canada CEO Mark MacLeod said the lab offers an opportunity to provide better insight into the information and data collected through all levels of government and social organizations... **Federal minister of public safety and emergency preparedness Ralph Goodale said** the new lab will make the delivery of federal programs much easier. ***"This will make decision-making fact-based — based on research, based on hard evidence — and that is a major improvement for public policy,"*** **he said. He hopes** it leads to ***"precision policy-making"*** that can improve public safety. **Goodale also said he hopes** the centre will build partnerships with Indigenous communities — something MacLeod said the centre would "love" to do. CBC News

TOP STORIES / MANCHETTES

High waves challenge for crews lifting sunken tugboat off B.C. coast
A rough sea is preventing crews from inflating air bags to lift the bow of a submerged tugboat that sank off British Columbia's central coast last month, spilling more than 100,000 litres of diesel fuel. Other pollutants also spilled into the water when the Nathan E. Stewart ran aground on Oct. 13, about 28 kilometres from Bella Bella. Despite the challenges facing crews, an incident report released Thursday says a cradle that will lift the tug is in position. As well, a receiving barge the boat will be placed on has been moved closer to the site. A boom that will contain any additional pollutants has been set up around the receiving barge. Heiltsuk Nation spokeswoman Jess Housty posted on Twitter Friday morning that all boats monitoring the site are operational, and efforts to move the vessel off the rocks into deeper water for removal are continuing. Canadian Press (Vancouver Sun)

Les municipalités rurales veulent plus d'efforts pour combattre le crime
L'association des municipalités rurales de la Saskatchewan affirme que plus d'efforts doivent être faits afin de lutter contre le crime en milieu rural... Plusieurs fermiers frustrés par ce qu'ils considèrent comme un manque d'action de la part de la Gendarmerie royale du Canada (GRC) ont d'ailleurs créé un groupe Facebook afin de surveiller eux-mêmes toute activité suspecte en région rurale... Cette semaine, le nouveau commandant de la GRC en Saskatchewan, Curtis Zablocki, s'est adressé au groupe lors de son congrès annuel. Il a dit que la meilleure façon de réduire la criminalité était de mettre l'accent sur l'engagement communautaire. Radio-Canada

Lutte contre les crimes contre la propriété: les efforts de la GRC Codiac rapportent
Un peu plus de 77% de la population du Grand Moncton se sent en sécurité. Cette mesure est le résultat d'un premier sondage réalisé par des étudiants du Collège communautaire en collaboration avec le service Codiac de la GRC. Le surintendant Paul Beauchesne, le grand patron de la GRC dans le Grand Moncton, a fait rapport au conseil de l'Autorité policière régionale de Codiac sur la performance de son service de police pour l'année en cours. Acadie Nouvelle

Jury makes 28 recommendations in Lena Anderson inquest
The inquest into the death of a Kasabonika Lake First Nation woman while in police custody has come to a close, with the jury making 28 recommendations around police funding and community grief counseling and suicide prevention. Lena Anderson hung herself in February 2013, using a draw string she removed from her pants while being held in the back of a Nishnawbe Aski Police Service (NAPS) vehicle. She had been left in the back of the vehicle as Kasabonika Lake didn't have any holding cells... The jury's 28 recommendations included: That police services in indigenous communities use the Police Services Act (PSA) as their governing legislation; That Canada, Ontario and Indigenous communities work together to ensure policing standards and service levels in Indigenous communities are equivalent to those in non-

Indigenous communities; That Indigenous police services are provided with enough funding to ensure an adequate complement of backup officers, and that they have access to a central communications and dispatch centre that meets PSA requirements; That Indigenous police services have adequate detachment buildings, proper training, and that officers review policies on prisoner care and identification of individuals at risk of self-harm. CBC News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

High waves challenge for crews lifting sunken tugboat off B.C. coast
A rough sea is preventing crews from inflating air bags to lift the bow of a submerged tugboat that sank off British Columbia's central coast last month, spilling more than 100,000 litres of diesel fuel. Other pollutants also spilled into the water when the Nathan E. Stewart ran aground on Oct. 13, about 28 kilometres from Bella Bella. Despite the challenges facing crews, an incident report released Thursday says a cradle that will lift the tug is in position. As well, a receiving barge the boat will be placed on has been moved closer to the site. A boom that will contain any additional pollutants has been set up around the receiving barge. Heiltsuk Nation spokeswoman Jess Housty posted on Twitter Friday morning that all boats monitoring the site are operational, and efforts to move the vessel off the rocks into deeper water for removal are continuing. Canadian Press (Vancouver Sun)

Pemberton residents clean up after rain, snowmelt causes heavy flooding
Emma Sturdy will never forget the wave of water that suddenly gushed into her family's Pemberton vegetable and fruit farm early Wednesday, flooding not only her and her sister's bedrooms, but almost the entire 21 hectares of their property. The flooding left them no choice but to place all of North Arm Farm's animals — pigs, sheep, turkeys and chickens — into the same pen, which made them none too happy, she noted... An evacuation alert for residents was issued for several areas around Pemberton on Wednesday, with about 20 residents forced to leave their homes. The alert was rescinded Thursday after the flood alert was downgraded to a high streamflow advisory due to decreasing river flows. Both the Village of Pemberton and the Squamish-Lillooet Regional District issued bulletins Thursday saying that dry conditions had resulted in decreasing flows in the Howe Sound region and that flows were expected to continue to drop through the day as dry conditions persisted until late Thursday. Vancouver Sun

«Je n'aurais jamais pensé que c'était de cette ampleur», dit le propriétaire
L'important glissement de terrain qui s'est produit à Saint-Luc-de-Vincennes a laissé un trou béant d'environ 152 mètres de large sur une terre agricole. Luc Normandin s'estime chanceux d'être ici pour nous parler. Mercredi soir, un cratère de la grandeur d'un terrain de baseball s'est formé dans sa cour arrière. Il s'en est fallu de peu pour que sa maison soit elle aussi emportée... Les ingénieurs de la sécurité civile sont toujours sur place. On ignore s'il pourra un jour réintégrer sa maison. En fin d'avant midi, le député fédéral Francois-Philippe Champagne est venu rencontrer les sinistrés afin d'évaluer concrètement de quelle façon l'État peut leur venir en aide. TVA Nouvelles

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

L'indépendance policière n'est pas un absolu
Un article d'opinion déclare, « À la suite des saisissantes révélations concernant la surveillance technologique de journalistes d'enquête par la Sûreté du Québec, le premier ministre Couillard a manifesté une colère froide. Résultat : une commission d'enquête publique (quasi judiciaire) aura comme vocation de colliger tous les faits pertinents, pour ensuite recommander au gouvernement les mesures

appropriées susceptibles d'être prises... Commentant les forfaitures de la police fédérale canadienne (GRC) pendant la crise d'Octobre en 1970, le premier ministre canadien Pierre Elliott Trudeau déclara en point de presse : en matière criminelle, ce n'est pas le gouvernement qui assure la protection des citoyens contre les abus policiers, ce sont les tribunaux. La police enquête sur des crimes sans l'autorisation du ministre responsable, et même à son insu, avait-il précisé. Il nuança son propos en matière de sécurité publique : la police doit agir dans le cadre d'orientations et de directives générales énoncées par le gouvernement du jour. Récemment, le Service canadien du renseignement de sécurité (SCRS) fut sévèrement blâmé par la Cour fédérale pour avoir manqué de transparence envers le tribunal à propos de son programme de collecte de données exécuté en vertu d'ordonnances judiciaires. En conférence de presse, penaud, le directeur du SCRS Michel Coulombe a dit regretter que la cour « s'inquiète en ce qui a trait au respect de l'obligation de franchise » du SCRS. Ce chef espion n'a rien compris : l'efficacité du contrôle judiciaire n'a de sens que si les agents de l'État jouent franc-jeu... » La Presse

Man charged in explosives-related incident at Montreal airport says he was set up
A Montreal man on trial for trying to board an airplane with explosives-related materials in his suitcase says he was set up. Antony Piazza, an Iranian-Canadian, is facing four charges stemming from the Montreal airport bomb scare on Oct. 27, 2013. Piazza, 74, told the court today he suspects an acquaintance in Spain with whom he had a falling-out likely inserted illegal materials into the handles of his carry-on luggage. Testifying in his own defence, Piazza says he was shocked when security screeners turned up the materials while X-raying his luggage. Canadian Press (CityNews, CTV News)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Lanes will be reduced from three to two on Peace Bridge beginning Tuesday
Expect to encounter fewer and narrower lanes going across the Peace Bridge beginning Tuesday. The number of lanes will be reduced from three to two as work starts on a $100 million project to replace the bridge's deck. The two lanes will each be narrowed from 12 feet to 11 feet, to accommodate 24-inch Jersey barriers that will straddle both lanes... Delays aren't expected because of the construction, but could occur if inspection booths going into Canada continue to be poorly manned, said Ron Rienas, president and executive director of the Peace Bridge Authority... "U.S. Customs and Border Protection have committed to staff and resource primary inspection booths to ensure the bridge functions with no congestion, at least entering the U.S.," Rienas said. "We have not had a similar commitment from Canadian customs." The Canadian Border Services Agency has repeatedly claimed union rules regarding overtime make it difficult to ensure enough agents to staff the booths. Buffalo News

Canada: The Looming Uncertainty Of Softwood Lumber
The 8,891 km boundary between Canada and the United States is often referred to as "the world's longest undefended border," but that's only in a military sense. Despite free trade agreements, disputes over softwood lumber have been ongoing since 1982, stemming, largely, from US sentiment that the Canadian softwood lumber industry is unfairly subsidized. Mondaq

United Way looking for final $520,000 to meet $2M target
The United Way of Sarnia-Lambton reached 74 per cent of its $2-million fundraising goal this week. "We are definitely in the final stretch of the campaign now," said Richard Kelch, "but we are in need of finding the final $520,000."... Almost all industrial campaigns continue to raise money and many are still a long way from wrapping up, as are many of the small industry, and government offices. Canada Border Services are off to a good start. The Observer

Guy Caron, inquiet des enjeux régionaux en suspens
Le député fédéral de Rimouski-Neigette—Témiscouata—Les Basques, Guy Caron, estime que la première année du gouvernement Trudeau a été loin d'être un succès pour la région et se dit inquiet des développements observés sur des enjeux d'importance, tels que l'agriculture, le bois d'œuvre et les infrastructures... Il y a ensuite la question du lait diafiltré qui traîne toujours en longueur. L'Agence des services frontaliers du Canada considère ce lait transformé comme une «protéine», lui permettant de

contourner les quotas de la gestion de l'offre. L'Agence canadienne d'inspection des aliments considère quant à elle qu'il s'agit toujours de «lait» et qu'il peut donc être utilisé dans la production de fromage et de yogourt. Infodimanche.com

Wanted California woman awaits extradition in Pembina County
A woman wanted in California for parental kidnapping is awaiting extradition in Pembina County after being arrested trying to cross the Canadian border with her two children. Rene Snider, 36, currently is being held in the Pembina County Jail in Cavalier. She had an extradition hearing Nov. 7 to send her back to Merced, Ca., where she is wanted on felony parental kidnapping charges. Grand Forks Herald

Toronto man arrested in connection with high-end auto theft ring
Toronto police have made another arrest in connection with a massive investigation into high-end GTA vehicles stolen and shipped overseas. Wael Hussein, a 27-year-old Toronto man, was arrested on Wednesday, Nov. 9 and is facing 111 charges. He was slated to appear in court at 2201 Finch Ave. W. on Wednesday, Nov. 9... Assisting Toronto police were police services in York, Peel, Halton and Regina, Royal Canadian Mounted Police, Canadian Nation Police Service, Canada Border Service Agency, Insurance Bureau of Canada, and the Department of Homeland Security. Inside Toronto (2016-11-10)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

After High Profile Busts, Dozens of Dark Web Child Porn Sites Remain
The FBI and other law enforcement have a daunting task when it comes to the problem of dark web child pornography. Despite recent successes at shutting sites down, just under 30 related Tor hidden services remain up and running, according to a researcher who focuses on the dark web. That figure reveals something of a constant whack-a-mole game for law enforcement: that even when one or several sites are shut down and many of their operators and users arrested, other sites spring up in their place. Motherboard

LAW ENFORCEMENT / APPLICATION DE LA LOI

Les municipalités rurales veulent plus d'efforts pour combattre le crime
L'association des municipalités rurales de la Saskatchewan affirme que plus d'efforts doivent être faits afin de lutter contre le crime en milieu rural... Plusieurs fermiers frustrés par ce qu'ils considèrent comme un manque d'action de la part de la Gendarmerie royale du Canada (GRC) ont d'ailleurs créé un groupe Facebook afin de surveiller eux-mêmes toute activité suspecte en région rurale... Cette semaine, le nouveau commandant de la GRC en Saskatchewan, Curtis Zablocki, s'est adressé au groupe lors de son congrès annuel. Il a dit que la meilleure façon de réduire la criminalité était de mettre l'accent sur l'engagement communautaire. Radio-Canada

Lutte contre les crimes contre la propriété: les efforts de la GRC Codiac rapportent
Un peu plus de 77% de la population du Grand Moncton se sent en sécurité. Cette mesure est le résultat d'un premier sondage réalisé par des étudiants du Collège communautaire en collaboration avec le service Codiac de la GRC. Le surintendant Paul Beauchesne, le grand patron de la GRC dans le Grand Moncton, a fait rapport au conseil de l'Autorité policière régionale de Codiac sur la performance de son service de police pour l'année en cours. Acadie Nouvelle

Jury makes 28 recommendations in Lena Anderson inquest
The inquest into the death of a Kasabonika Lake First Nation woman while in police custody has come to a close, with the jury making 28 recommendations around police funding and community grief counseling and suicide prevention. Lena Anderson hung herself in February 2013, using a draw string she removed from her pants while being held in the back of a Nishnawbe Aski Police Service (NAPS) vehicle. She had been left in the back of the vehicle as Kasabonika Lake didn't have any holding cells... The jury's 28 recommendations included: That police services in indigenous communities use the Police Services Act (PSA) as their governing legislation; That Canada, Ontario and Indigenous communities work together to

ensure policing standards and service levels in Indigenous communities are equivalent to those in non-Indigenous communities; That Indigenous police services are provided with enough funding to ensure an adequate complement of backup officers, and that they have access to a central communications and dispatch centre that meets PSA requirements; That Indigenous police services have adequate detachment buildings, proper training, and that officers review policies on prisoner care and identification of individuals at risk of self-harm. CBC News

Gunshot incident in NB
An RCMP investigation is under way after a man was wounded by a single gunshot on 14th Avenue in North Battleford on Thursday night. According to Battlefords RCMP the incident took place just after 7 p.m. that evening. The victim was found located in an alley between 106th and 107th St. north of 14th Ave. News Optimist

'Sweet, talented, beautiful': Crowdfunding page set up for mom of dead girl
A crowdfunding page has been set up to support the mother of a seven-year-old girl who was found dead in a northeastern Saskatchewan home. Police had issued an Amber Alert for Nia Eastman on Thursday after she was not returned to her mother the night before. Nia's father, Adam Jay Eastman, was found dead in a rural area from self-inflicted injuries, and hours later Nia's body was discovered in a house in the small community of Choiceland. Canadian Press (Chronicle Herald)

Police Are Best Substitute Teachers Ever, When Daycare Provider is Hospitalized
Three Canadian police officers aren't just good at protecting and serving – they're pretty good at babysitting too. When a daycare provider in Langford was taken to a nearby hospital as a precaution, these West Shore RCMP officers stepped up to look after the four kids awaiting their parents. Good News Network

U.S. cops can arrest Canadians in Canada, with restrictions -- can Trudeau stop Trump if he wants more power?
Back when Stephen Harper was Prime Minister, he signed a pact with President Obama that made many Canadians uneasy. The Integrated Cross Border Law Enforcement Operations Act was part of the 2012 omnibus budget package. It allows for American law enforcement agents to cross into Canada and gives, "Every designated officer has the same power to enforce an Act of Parliament as a member of the Royal Canadian Mounted Police." The program, called Shiprider, is limited to waterways between Canada and the United States. Law enforcement isn't supposed to be able to use these powers on land. But there were plans to expand Shiprider. Access to these powers on land was supposed come through another program. The plan would extend Canadian law enforcement powers to American officers, included creating new integrated units, focused on areas like crime and intelligence. Rabble

Key witnesses in probe of Indigenous man's 2015 death not interviewed by police, fifth estate finds
Police in Thunder Bay, Ont., never bothered to find and interview two key witnesses who were with an Indigenous man the night before he was found dead last year, the fifth estate has found. The body of Stacy DeBungee, 41, was discovered in the McIntyre River on the morning of Oct. 19, 2015. His death is one of several deaths of Indigenous people in Thunder Bay's waterways that were quickly deemed not suspicious with little apparent investigation by the city's police service. CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Prisoners Keep Dying in Winnipeg's Jails
The death penalty is illegal in Canada. But that doesn't mean prisoners aren't dying in Manitoba. Since March, five people have died in custody at the Winnipeg Remand Centre, including two in October. Four of the five were Indigenous men. That includes Errol Greene, a 26-year-old man who was killed on May 1 after being denied epilepsy medication, and handcuffed and shackled on his stomach after the first of two successive seizures. Most were in remand for breaching court orders while awaiting trial, including drinking alcohol while on probation. Vice News

Good Behaviour Earns Cofell Additional Parole
A convicted killer from Chatham who murdered three people 25 years ago will continue to be monitored for at least six more months while he's out of prison on parole. The Parole Board of Canada released a decision on November 3, 2016 saying 43-year-old Jason Cofell, who killed Jasen Pangburn and Virginia and Alfred Critchley in 1991, will be able to continue his day parole for another six months. Blackburnnews.com

After shooting, Prison Pump is back as founder instructs from afar
In a gym on Barton Ave., a fitness group cools down under the direction of their instructor who isn't actually there. Alejandro Jose Vivar can't be. For his own safety, he leads the stretches via cellphone from an undisclosed location. The former federal inmate and founder of Prison Pump - a "penitentiary-style" workout he created on the inside - is laying low three months after someone pumped five bullets into him during a morning workout class held across the street in Christie Pits Park on July 30. The shooter is still wanted by police... Vivar went to jail a gang leader but came out a certified fitness instructor with a mission to be a community ambassador for good health. Postmedia Network (Toronto Star)

Man surrenders after being threatened with stun gun
The old adage of not bringing a knife to a gunfight sort of applied to a short standoff in St. John's early Friday. Fleeing on foot from police at 12:30 a.m., a 25-year-old St. John's man stopped and confronted his pursuers, wielding what RNC officers thought was a hypodermic needle. A police officer, in turn, pointed a "conducted energy device" at the suspect and told him to surrender or be zapped, the RNC stated in a news release. The man gave up, and his weapon was determined to be an epinephrine auto-injector, police said. The man -- who was being sought because of a parole warrant issued by Correctional Services Canada -- was arrested and charged with resisting arrest, assault with a weapon and assaulting a police officer. He was held in custody and was to appear in court later Friday. Telegram

Canada-wide warrant issued for sex offender Darren Wheatley who broke curfew third time
Vancouver police issued a Canada-wide search warrant for a high-risk sex offender who did not return to his Vancouver halfway house on November 9... He is a two-time federal offender serving a 10-year sentence for two counts of sexual assault, sexual assault causing bodily harm, and two counts of overcoming resistance by choking. He was involved in three separate attacks on women in Ontario. The Straight (2016-11-10)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

SARM members want more action on rural crime
After a tense summer that saw farmers arming themselves during harvest, the Saskatchewan Association of Rural Municipalities (SARM) says more work needs to be done to battle rural crime. After becoming frustrated with what they saw as a lack of response from RCMP, farmers created a Facebook group this summer to track suspicious activity in rural areas. At one point, a farm worker said he was held up by three armed men with handguns during harvest. This week, Saskatchewan RCMP's new commanding officer, Curtis Zablocki, addressed the group at its annual convention. He said the best way to reduce crime was to focus on community engagement. While SARM president Ray Orb said he would still like to see more RCMP patrolling rural areas, he agreed that mobilizing farmers was a good idea. CBC News

Somali-Canadian officer a first for Edmonton Police Service
The first Somali-Canadian recruit to graduate from the Edmonton Police Service academy officially joined the ranks Thursday. Const. Amal Abdi, 28, was among 30 new officers celebrated during a ceremony at city hall. "We've been saying that we want to see representatives of our community be part of the Edmonton police," said advocate Ahmed Abdulkadi, with the Ogaden Somali Community of Alberta. "This is one step forward and this will heal a lot of wounds." Abdi shied away from attention herself, but friend Radwan Mohamed said, like the rest of her classmates, Abdi has worked hard to get to this point. "The diversity of experience that she brings will automatically make a difference," Mohamed said. CBC News

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Instagram project chronicles search for missing and murdered Indigenous women
There's another story to the tragic saga of missing and murdered Indigenous women (MMIW) and it's coming to light through an Instagram project created by the National Film Board (NFB). What Brings Us Here -- a project by writer and filmmaker Katherena Vermette and producer Alicia Smith -- profiles volunteers of the Drag the Red and Bear Clan Patrol of Winnipeg. These grassroots movements patrol neighbourhoods and search the banks and waterways of the Red River in response to the many missing in their communities. Rabble

'It could have been me'
An accountant, a chief, a nurse, a student, a counsellor—each of them came close to being on Canada's list of missing and murdered Indigenous women. Thirteen remarkable women tell their extraordinary stories of terrible violence and formidable resilience—stories that, as one survivor hopes, will serve as 'a pay-it-forward of women sharing their pain and triumph.' Maclean's

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Canopy Growth is Canada's first 'cannabis unicorn' with $1 billion valuation
Canopy Growth Corp. is Canada's first marijuana "unicorn" after reaching a billion-dollar valuation Friday as part of an industry-wide rally buoyed by this week's legalization push in eight U.S. states... The federal Task Force on Marijuana Legalization and Regulation is expected to release recommendations later this month on how to implement a market that has been estimated to be worth between $5 billion and $10 billion. National Post

Weedmaps: New app provides medical marijuana dispensary information
Medical marijuana users in Halifax can now check pricing, strain availability and even watch tutorials on cooking edibles through the new application, Weedmaps. Introduced through an office in Waterloo a year ago, Weedmaps can pinpoint the addresses of dispensaries, what they sell, and also direct people to delivery services and doctors likely to provide medical prescriptions. Chronicle Herald

Cops put the brakes on marijuana vending cart
A budding business plan for a marijuana vending cart went up in smoke thanks to some eagle-eyed cops. Victoria Police busted a man for dealing weed from a well-marked marijuana vending cart last week. It didn't take much for officers on a late-night patrol to smoke out the alleged drug dealer - he was bluntly advertising it. The run-of-the-mill bicycle food cart clearly read "420 Delivery" along with the caveat "no minors." "The officers spoke with the man and quickly determined that he was selling marijuana," police said in a press release Thursday. More than 150 grams of marijuana was seized, police said. Cops seemed baffled by the brazenness of the bud business. Postmedia Network (Ottawa Sun)

Centretown medical marijuana dispensary robbed
A medical marijuana dispensary in Centretown was robbed Friday morning. No one was injured, said the police officers responding to a call from the Sylk Medy dispensary, on Gladstone Avenue near Bay Street... Sylk Medy opened this fall in the downstairs room of a converted house. It's locally owned and operated. At the time, the owner said the shop decided not to sell dried weed in order to discourage customers looking for recreational pot... Like all the dispensaries, Sylk Medy operates illegally. This is the fifth robbery at a marijuana dispensary this fall. Six dispensaries closed last week after police drug raids. All of the raided dispensaries were operated by a B.C.-based chain that, according to police, had expanded sales beyond just medical marijuana patients. Police say they continue to investigate the remaining dispensaries and respond to public complaints. Ottawa Citizen

PUBLIC SERVICE / FONCTION PUBLIQUE

Built to crash: The ugly, sputtering beginning of Shared Services, and how politics conspired against it

Liseanne Forand really didn't know what to expect. On Aug. 4, 2011 she was making her way on foot to Phase III of the Gatineau office complex known as Place du Portage. A career bureaucrat, Forand had, the day before, been appointed president of Shared Services Canada — a new federal department that would manage the government's email, data centres and telecommunications. Her mandate — representing about one-third of the federal government's $5-billion-a-year technology services budget — was breathtaking in its scope and complexity. She was to simultaneously streamline and modernize the government's electronic backbone, and keep the old gear running. Sixty-three email systems would be collapsed into one. More than 500 data centres were to be decommissioned, to be replaced by a mere handful. Fifty telecommunications networks connecting 3,500 federal buildings were to be upgraded. Forand was to do this with staff cobbled together from 43 different departments. But on this day, she had no office, and the paperwork had been approved for just 1,200 of an eventual 6,000 employees. Ottawa Citizen

OTHER / AUTRES

Trump Protest Makes Its Way Through Downtown Vancouver

Hundreds of protesters snaked their way through downtown Vancouver on Thursday, pumping their fists in the air and chanting "Love trumps hate," as they rallied against the outcome of the United States presidential election. Dozens of placards bobbed above the crowd with various slogans disparaging president-elect Donald Trump, ranging from "Build kindness, not walls" and "Proud supporter of love," to "Make America safe again," and "Prejudice kills."... The protest was staged in front of Trump Tower, which attracted criticism and played host to another demonstration earlier this year thanks to its controversial namesake. The oversized letters spelling out the Trump name immediately above the building's front doors had been covered in blue sheets and a fence surrounded the entrance. Canadian Press (Huffington Post)

Public advocacy, private diplomacy secured Hoodfar's release: Cotler

A former MP and international human rights lawyer said he suspects a Concordia University professor was released after being detained by Iranian authorities only because of "the combination of effective public advocacy and effective private diplomacy." Irwin Cotler, former minister of Justice and Attorney General of Canada, added he believes timing was also a factor in the release of Homa Hoodfar, who became very ill during her detention in Tehran's notorious Evin prison. Iran became worried they might have "another Kazemi case on their hands," Cotler said, referring to Zahra Kazemi, an Iranian-Canadian freelance photographer who was arrested in Iran in 2003 and killed by officials. Fear about Hoodfar's declining health, pressure from the public and the Canadian government's behind-the-scenes work all convinced Iran that continuing to detain Hoodfar was no longer in their self-interest, Cotler said. iPolitics

INTERNATIONAL

Taliban attack on German consulate kills 4

A Taliban suicide bomber rammed a truck packed with explosives into a wall around the German consulate in the northern Afghan city of Mazar-i-Sharif, killing at least four civilians and wounding scores, officials said. The attack highlighted the security problems spreading across Afghanistan in recent months, underlining one of the most intractable foreign policy challenges that will face U.S. president-elect Donald Trump when he takes office next year. Reuters (CBC News)

Dozens of pipeline protesters arrested in latest skirmish

Law officers arrested about three dozen Dakota Access oil pipeline protesters in a confrontation that also shut down a state highway. The midday Friday incident began after about 100 protesters confronted crews doing work along the pipeline route where pipe had already been laid. Morton County sheriff's

spokeswoman Donnell Hushka says workers were safely evacuated. It happened about 20 miles away from a protest camp where hundreds of pipeline opponents have gathered for months. More than 470 people have been arrested since August. Associated Press (Star Tribune)

Trump protests surge across America
Another night of nationwide protests against Donald Trump's election came to a head in Portland, where thousands marched and some smashed store windows, lit firecrackers and sparked a dumpster blaze. Police termed the protest a riot and used "less lethal munitions" to help clear the streets. Some 4,000 protesters surged into the downtown area late Thursday night with chants like "we reject the president-elect!" Officers began physically pushing back against the crowd that at times threw objects at them as midnight approached, arresting several people and using flash-bang devices and types of smoke or tear gas to force people to disperse. After several orders to leave, police said officers used "less lethal munitions," such as pepper spray and rubber projectiles. Live video footage showed officers firing what appeared to be the non-lethal items. It wasn't immediately clear if anyone was hit. Associated Press (iPolitics)

Trump Homeland Security candidates include GOP lawmakers and, less likely, a sheriff
President-elect Donald Trump is considering two Republican members of Congress fo rDepartment of Homeland Security secretary, a critical post whose occupant would oversee his proposed crackdown on illegal immigration, people familiar with the deliberations said. The incoming chief executive is looking at Rep. Michael McCaul (R-Texas), chairman of the House Homeland Security Committee, and Sen. Jeff Sessions (R-Ala.), the people said. Sessions, who helped shape Trump's hardline views on immigration, is also under consideration for other top administration jobs such as defense secretary. Other names being floated for the Homeland Security post include former New York City mayor Rudy Giuliani and New Jersey Gov. Chris Christie, who leads Trump's transition team. But both are former U.S. attorneys also reportedly interested in being attorney general, so they could view DHS as a consolation prize. Washington Post

Daech à l'agonie
En un an, le nombre de photos et de vidéos diffusées par le groupe armé État islamique (EI) est passé d'un pic de 761 en août 2015 à 194 en août 2016, note le Combating Terrorism Center, de l'Académie militaire de West Point, aux États-Unis. Ce déclin serait d'abord attribuable à la mort de membres de l'équipe chargée des contenus visuels — dont celle du chef de la propagande, Wa'il Adil Hasan Salman al-Fayad — et à la destruction d'infrastructures de production de l'EI. Le ton des vidéos publiées a lui aussi changé. Le groupe ne vante plus les mérites du « califat », comme il le faisait en 2014, en diffusant des images de commerces florissants et de vie civile prospère. Les vidéos présentent désormais à 70 % des nouvelles de nature militaire, selon les chercheurs de West Point. Ce recul de la propagande de Daech est un coup dur pour un groupe qui a toujours cherché à attirer des combattants étrangers. Selon le Pentagone, le nombre d'étrangers rejoignant chaque mois les rangs du « califat » est passé d'environ 2 000 à à peine 200. L'actualité

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

AndrewMitrovica
ICYMI and b/c #CSIS and @RalphGoodale want you to, I'm re-posting my latest: ricochet.media/en/1530/no-law… #C51 #cdnpoli #Snowden

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

VancouverSun
High waves challenge for crews lifting sunken tugboat off B.C. coast https://t.co/VQL4W8zqNY

VancouverSun
Pemberton residents clean up after rain, snowmelt causes heavy flooding https://t.co/MlXlEFbOrE

tvanouvelles
À VOIR | Glissement de terrain à Saint-Luc-de-Vincennes: «Je n'aurais jamais pensé que c'était de cette ampleur» http://bit.ly/2frxzll

NATIONAL SECURITY / SÉCURITÉ NATIONALE

CityNews
Man charged in explosives-related incident at Montreal airport says he was set up http://ow.ly/sBjC3065tf1

Colinfreeze
What happens legally when cops find the needle onky after spies have been collecting all the haystacks first ?

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

NewsroomGC
HMCS Brandon intercepts estimated 700 kg of cocaine http://ow.ly/pMMA100oDUp

BBishopAirport
Meet Ian and Jagger. This duo can often be seen at @BBishopAirport as members of @CanBorder's Detector Dog Services team #ItsMyAirport

INFC_eng
Min Sohi and MI Gov Snyder celebrate impt milestone twds #GordieHoweBridge http://infc.gc.ca/86e2_ #cdnpoli #Windsor #Detroit @WDBAbridge

CTVNews
ICYMI: Some Canadians with dual citizenship to face passport restrictions http://ow.ly/vqlt3065tig

vicecanada
We go to the border to see if Trump's victory is driving Americans into Canada: http://bit.ly/1TdtUiO

CYBER SECURITY / CYBERSÉCURITÉ

globalnews
Casino Rama targeted in cyberattack, customer information stolen https://t.co/sD7bzOd9TU

motherboard
Russian hackers launch targeted cyberattacks hours after Trump's win http://bit.ly/2fhmkEw

motherboard
After high-profile busts, dozens of dark web child porn sites still remain http://bit.ly/2fr3XLb

LAW ENFORCEMENT / APPLICATION DE LA LOI

icisaskatchewan
Les municipalités rurales veulent plus d'efforts pour combattre le crime rc.ca/Mf2fXb

CBCNews
Key witnesses in Indigenous man's 2015 death not interviewed by police http://www.cbc.ca/1.3843241

CBCKatie
There are heavily armed police officers here today as part of the security detail.

620ckrm
RCMP investigate after man was found in alley with gunshot wound #SK #Sask - http://bit.ly/2fDHz1A

rabbleca
U.S. cops can arrest Canadians in Canada, with restrictions — can Trudeau stop Trump if he wants more power? @NoLore http://buff.ly/2el99Zk

vicecanada
The RCMP used police databases and social media to track Aboriginal protestors: http://bit.ly/2eWHCnW

RidgeRCMP
Good turnout at @YourMapleRidge service #LestWeForget

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

OttawaCitizen
NEW: Documents show Ottawa inmates told the government they were stripped naked and put into solitary confinement http://ow.ly/3cx33063ro1

vicecanada
Prisoners keep dying in Winnipeg's jails: http://bit.ly/2fl0GtW

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

ShelbyThom980
. @janephilpott says all levels of government must work together to tackle overdose crisis #bcpoli #cdnpoli

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

rabbleca
"What Brings Us Here" is an unfolding online project about the emotional reality of #MMIW for communities http://buff.ly/2fhDLVq @June_Chua

LivelyLexie
'It could have been me': 13 remarkable Indigenous women tell their stories of survival: http://ow.ly/NVV87 via @MacleansMag

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

nationalpost
Canopy Growth becomes Canada's first 'cannabis unicorn' as market cap tops $1 billion natpo.st/2flKR2i #business pic.twitter.com/fi2ylZpVJN

ottawasuncom
Cops put the brakes on marijuana vending cart http://ow.ly/eQPA306583k

JacquieAMiller
Ottawa police are at the Sylk Medy marijuana dispensary on Gladstone Avenue.

JacquieAMiller
Sylk Medy did not sell dried weed, partly to discourage customers interested in recreational marijuana. Only cannabis oil, creams, capsules.

OttawaCitizen
A Centretown marijuana dispensary was robbed Friday morning. It's at least the fifth dispensary robbery this fall. http://ow.ly/jvMZ3065zy6

PUBLIC SERVICE / FONCTION PUBLIQUE

DLeungOtt
Who's winning at Shared Services: Top five suppliers http://bit.ly/2f06lrw #ottnews #newsgraphics #ottawa @ottawacitizen

OttawaCitizen
Built to crash: The ugly, sputtering beginning of Shared Services, and how politics conspired against it http://ow.ly/L90b3065AZZ

OTHER / AUTRE

CBCPolitics
Soldiers honoured in Remembrance Day services in Ottawa, across Canada http://ift.tt/2eZfh0i #hw #cdnpoli

perrybellegarde
Today, we stand on the shoulders of 10,000 First Nations warriors who've served since 1812. #RemembranceDay

davidakin
More info on the GG and the wearing of military uniforms. (Includes pic of Sharon J in her navy uniform) http://bit.ly/2g2HJ5D

HannahThibedeau
Pm @PmoTrudeau arrives at #remembrance service #cdnpoli #hw

HuffPostCanada
Hundreds protest U.S. president-elect Donald Trump in Vancouver http://huff.to/2fqMfYc

INTERNATIONAL

politico
With chants like "We reject the president-elect," protests surge across America http://politi.co/2g2Ml6c | Getty

nationalpost
Ku Klux Klan plans 'victory' parade to celebrate election of Donald Trump, who 'united my people' http://natpo.st/2g2LnMP

Lactualite
Le déclin serait d'abord attribuable à la mort de membres de l'équipe chargée des contenus visuels http://www.lactualite.com/ #EI #Daech #Syrie

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

Today's News / Actualités
November 13, 2016 / le 13 novembre 2016
9:00 - 18:00 ET

This collection contains news items that appeared online between 09:00 a.m. and 6:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 09h00 et 18h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

RCMP tracked 89 indigenous activists considered 'threats' for participating in protests
The Trudeau government says Canada's national police force respects the right to peaceful demonstrations by indigenous activists, after it was revealed the RCMP compiled a list and distributed profiles of indigenous protesters it deemed "threats" who it determined were potentially willing and capable of criminal activities. Dubbed Project SITKA, the RCMP began soliciting information on indigenous activists who could be perceived "to have committed or commit" crimes from all of its divisions

and local police departments across the country in March 2014. Using the information it received and data collected from social media, the Mounties identified 313 activists — attendees of protests on issues ranging from natural resource development to missing and murdered indigenous women — who potentially posed a "criminal threat to Aboriginal public order events." The RCMP then narrowed that list to 89 individuals it said met "the criteria for criminality" and created unique profiles for each one. These profiles were then made available to front-line officers, analysts and other law enforcement agencies through two police databases, the RCMP's Automated Intelligence Information System and the Police Reporting and Occurrence System... A spokesperson for **Public Safety Minister Ralph Goodale** said Project SITKA was focused on identifying potential threats to public safety at indigenous events and protests. ***"This focus was in keeping with recommendations stemming from the 2007 Ipperwash Inquiry report, which highlighted the need to examine aboriginal protests as a separate and distinctive form of protest requiring dedicated and unique police resources, strategies and responses,"* said Scott Bardsley.** Bardsley added that the report on Project SITKA concluded there were no direct threats to critical infrastructure and no connection to organized crime associated with Indigenous protests. Postmedia News (Edmonton Journal; National Post; Montreal Gazette)

TOP STORIES / MANCHETTES

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Red Cross funds study into how Fort McMurray wildfire affected indigenous people
Melanie Dene still remembers the harrowing ordeal of driving through fiery hell during the evacuation of Fort McMurray six months ago with her two young daughters... She and others are now the subject of a research study into how the wildfire affected First Nation and Metis communities in and around the Fort McMurray region. The Canadian Red Cross is funding research, which involves talking to people whose homes were destroyed in the city, who faced food shortages in outlying communities and those who can no longer hunt, trap or pick berries because of the charred terrain. The study involves five First Nations that make up the Athabasca Tribal Council along with the Wood Buffalo, Willow Lake and Chard Metis communities and other organizations. Canadian Press (Yahoo News)

Tug recovery near Bella Bella delayed again by poor weather - Crews hope to resume salvage operation Monday if conditions improve
Attempts to salvage a tugboat that sank off B.C.'s Central Coast nearly a month ago spilling more than 100,000 litres of pollutants have been delayed again by bad weather. The salvage crew working to raise the tugboat had hoped to lift the vessel Saturday, but Environment Canada issued a storm warning for the region calling for high winds. It's hoped the salvage operation can resume Monday, said Jessie Housty, an elected tribal councilor for the nearby Heiltsuk First Nation. Crews need a 36-hour window of clear weather in order to lift the sunken vessel from the water, Housty said. A large crane from Seattle was brought in to hoist the tug onto a barge. Last week, crews dragged the tug about 30 metres into deeper waters of Seaforth Channel, positioning it so that it could be lifted onto that barge. CBC News

Military conducting SAR exercises in metro region
The public can expect increased military activity in and around St. John's this week as search and rescue training exercises take place. The Royal Canadian Air Force says in a news release that 103 Search and Rescue Squadron from 9 Wing Gander will be in the area for training exercises between Nov. 13-18. "Due to the high tempo of this training, the general public are advised that there will be extensive Cormorant helicopter flights and higher than normal military activity in these areas during this period," the news release states. Telegram

Northern Alberta hunter found safe after spending evening in woods
A 43-year-old hunter is safe after being lost in the woods south of Boyle Saturday, the RCMP say. The man became disoriented around 1 p.m. while hunting in dense brush near Long Lake Provincial Park, 130

kilometres northeast of Edmonton. He called for help using a cell phone, but reception was soon lost. The temperature was around o C with light rain. Boyle Fire and Rescue started a ground search with help from the Edmonton RCMP helicopter, which found the man around 11:45 p.m. He was in good health. Edmonton Journal

Cessna en difficulté: quatre personnes secourues par des chasseurs
Quatre personnes qui voyageaient à bord d'un Cessna ont été secourues par des chasseurs, dimanche matin, près du lac Cahill, à mi-chemin entre Gatineau et Maniwaki, en Outaouais. Vers 10 h 30, un témoin a contacté les secours par Skype après avoir vu un aéronef en difficulté dans ce secteur reculé, mais, vers midi, la Sûreté du Québec ne savait toujours pas si l'avion s'est écrasé ou si ses occupants se sont retrouvés en difficulté pour une autre raison. Toutefois, la SQ a pu confirmer que les quatre personnes étaient saines et sauves au moment où elles ont été secourues. Une équipe de sauvetage des Forces armées canadiennes a été envoyée de la base de Trenton, en Ontario, sur les lieux de l'événement. La Sûreté du Québec devait aussi dépêcher une équipe pour aller vérifier la situation. Agence QMI (TVA Nouvelles)

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Canada's energy industry ponders how to face activist 'threats'
Canadian security experts are increasing their vigilance against activists' threats to the country's energy infrastructure, as civil-liberties advocates worry about the use of improper surveillance on peaceful opponents to major projects. In what is billed as a training workshop, Carleton University's Infrastructure Resilience Research Group is playing host to a closed-door conference on Monday and Tuesday for lawyers, police, regulators and industry representatives on "the challenges of dealing with natural resource development projects and activism." One of the organizers, professor emeritus Martin Rudner, said there are significant threats from "domestic extremists" to Canada's energy infrastructure, including pipelines, generating stations and transmission lines… In an interview, he pointed to incidents such as the confrontation three years ago between First Nations demonstrators and RCMP in New Brunswick over proposed shale-gas drilling, and to the emergence of more militant elements in the indigenous and environmental communities… But critics argue police and intelligence agencies are armed with overly broad definitions of national security and critical infrastructure, which include projects that are in the planning and construction phase, in addition to assets that are operational and delivering energy across the country. "A lot of these concerns are overblown," Ottawa lawyer Paul Champ said. He is a board member of the British Columbia Civil Liberties Association that has alleged RCMP and the Canadian Security Intelligence Service (CSIS) engaged in illegal surveillance of Canadians protesting against Enbridge Inc.'s proposed Northern Gateway pipeline. Mr. Champ said the RCMP and CSIS became more active in natural-resources development under the former Conservative government, which defined national-security threats to include actions that could affect the economic stability of the country, and then defined resource development as essential to the health of the Canadian economy. Globe and Mail

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

NIL

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Signal Downloads Spiked After Election Results
If you use the popular encrypted messaging app Signal, you may have noticed an influx of friends downloading the app following the conclusion of the 2016 US presidential election. Signal received some significant buzz on November 9th, as the world awoke to find out Donald Trump was president-elect. In the 48 hours after the final results were announced, my phone had buzzed with no less than two dozen notifications informing me that friends and acquaintances—many of whom I'd long lost contact with—had finally installed the end-to-end encryption app, which has been praised by security experts and famously endorsed by NSA whistleblower Edward Snowden. "Signal's growth has really accelerated over the past week, and it isn't showing any sign of slowing down," Moxie Marlinspike, the pseudonymous creator of Signal's encryption protocol, told Motherboard in an encrypted chat. Motherboard

LAW ENFORCEMENT / APPLICATION DE LA LOI

RCMP looking to increase number of women on the force
The RCMP is looking for more women to join the force. Just over 21 per cent of officers across the country are women. The force would like to see that number increase to 30 per cent. Erika McGrattan, a proactive recruiter for the force, told Global News they want to make sure their officers reflect Canada's population. "We want more women in the police force so we can go to calls and make women more comfortable when we attend calls, when we show up so they're not intimidated to speak to us, and to let us help them better." To apply you need to have completed high school. Applications will be screened by the force and successful applicants will then go through six months of training in Regina. "We want that person that wanted to become a police officer because they want to help people," McGrattan said. "They want to go out, they want to make a difference. We want to find that person who is honest, who does genuinely care." One in 10 women who apply to the force will be accepted. 630 CHED

Cinq personnes arrêtées - Un mort dans une fusillade à Halifax
La police régionale d'Halifax a confirmé dimanche matin le décès d'un jeune homme de 21 ans survenu samedi vers 17 h, à Halifax, sur la rue Washmill Lake. À l'arrivée des policiers, la victime était déjà décédée sur la scène du crime. Un périmètre de sécurité a été érigé près du 600 Washmill Lake. La police a précisé que les tirs ont eu lieu à l'intérieur. Une escouade de la Gendarmerie royale du Canada et des policiers d'Halifax ont été dépêchés sur les lieux. Cinq personnes, tous des hommes, ont été arrêtés et conduits au quartier général de la police. Dimanche matin, quatre suspects étaient toujours détenus. L'unité des crimes majeurs et des enquêtes criminelles poursuivent leur enquête sur cet homicide. TVA Nouvelles

Lloydminster RCMP say missing man found dead
A 48-year-old Lloydminster man who had been missing since Nov. 3, was found dead Saturday. RCMP released the man's description last week and asked the public for assistance in locating him. No foul play is suspected. Police thanked the public for their assistance during the search. The RCMP said no further details will be provided out of respect for his family. Global News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

A touch of déjà vu: Harold Backer case rekindles Ian Thow scandal
The disappearance of mutual fund dealer Harold Backer, who former clients believe defrauded them of millions of dollars, has dredged up memories of another Victoria investment adviser who cost his clients millions. Calling it a touch of déjà vu, some of Ian Thow's former clients say they see strong parallels in the two cases. "Definitely," said Ron Black, a former Thow client who was bilked of $700,000. "It never does go out of your mind, it's there all the time and I'm reminded every time I see something like that. Yeah, I think about it." Thow took money from clients for schemes that included a Jamaican bank and short-term loans for developers. He never made those investments. The RCMP Integrated Market Enforcement Team led a five-year investigation into Thow, a former Berkshire Investment Group vice-president, based on allegations he cheated clients and friends out of more than $32 million. Thow was jailed in 2010 for defrauding 20 clients of $8 million, the total that the Crown felt it was able to prove...

Thow is on full parole and living in the Fraser Valley, where at last report he was working for a landscaping firm and paying $100 a month for restitution to his former clients. A court order requires him to pay back $3.8 million. Thow's warrant expiry date — the end of his sentence — is March 3, 2017. After that, he will no longer be under the jurisdiction of the Correctional Service of Canada or the Parole Board of Canada. Backer, meanwhile, is still considered a missing person by Victoria police. Times Colonist

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Isolation a barrier to exposing sexual abuse, incest on reserve: Bellegarde
At night, he would arrive in Corey's room by crawling through the window next to the bunk bed where she slept. She knew from the smell when he was there. By day, she endured different hands, sometimes under the most mundane circumstances — once, she recalls, while in the kitchen eating lunch. He pulled down her underwear and started fondling her. He left money on the table. They were family members, these two predators — their unwanted touch impossible to escape for a young girl living on a remote First Nation in British Columbia. That isolation, a fact of life for many Aboriginal Peoples, is a pernicious barrier to the essential goal of exposing the scourge of indigenous sexual abuse and incest, says Perry Bellegarde, the national chief of the Assembly of First Nations. Bellegarde is pleading with chiefs to confront the problem head-on. But he also acknowledges a difficult truth: many First Nations people who live in remote areas are reluctant to come forward with their allegations for fear of reprisals in their small, tightly knit communities. Canadian Press (Yahoo News)

People, projects winners of mayor's safety awards
Two individuals and three community projects have been recognized in the sixth annual Mayor's Community Safety Awards. "I wish to offer my sincerest congratulations and thanks to each of this year's recipients," said Mayor Keith Hobbs in a ceremony at city hall. "This year's recipients are setting an example through their outstanding efforts to make our community safer and more welcoming for everyone. I hope we can all look at these recipients as inspirations as we work together to make our own changes to better our community." Chronicle-Journal

Les agressions sexuelles, un fléau chez les autochtones
Enfant, elle sentait sa présence dès qu'il arrivait, la nuit, dans sa chambre en entrant par la fenêtre qui donnait sur son lit superposé. Corey, qui a aujourd'hui 55 ans, est l'une des nombreuses femmes autochtones du Canada qui ont été victimes d'agressions sexuelles par des proches ou des membres de leur famille au cours de leur enfance. Corey (nom fictif) a enduré plusieurs fois de faire l'objet d'attouchements, parfois dans des circonstances des plus banales, en plein jour. Elle se souvient entre autres de la fois où, alors qu'elle mangeait à la cuisine, l'un de ses deux proches agresseurs a retiré sa petite culotte et s'est mis à la caresser. Après avoir mis fin à ces attouchements, l'homme a laissé de l'argent sur la table. L'isolement de nombreuses communautés autochtones est un des éléments qui freine les victimes d'abus sexuel ou d'inceste à dénoncer de tels actes, estime le chef de l'Assemblée des Premières Nations, Perry Bellegarde. Ce dernier souhaite que des actions soient entreprises pour faire face à ce problème, un appel qui est appuyé par d'autres chefs autochtones. Il note cependant que de nombreuses victimes ont peur de parler puisqu'elles craignent des représailles. Presse canadienne (La Presse)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Légalisation du cannabis : les intervenants jeunesse aux aguets
La légalisation de la marijuana promise par le gouvernement fédéral pourrait modifier le quotidien des intervenants jeunesse. Des formations sont déjà offertes pour mieux outiller les professionnels, dont certains craignent l'arrivée de la nouvelle loi. Des dizaines de professionnels de la santé, en majorité des intervenants jeunesse, seront formés au cours des prochains mois par le Groupe de recherche et d'intervention psychosociale (GRIP), un organisme qui se spécialise dans la prévention des toxicomanies. L'initiative, lancée par l'organisation située à Montréal, vise avant tout à rassurer les craintes de nombreux intervenants. « Les gens [à qui on a donné la formation] sont soulagés. Beaucoup avaient peur que la légalisation amène plus de consommation alors qu'en général, dans les pays où il y a eu la décriminalisation, c'est plutôt l'inverse : on voit moins de consommation. Ça a soulagé beaucoup d'intervenants », souligne Jessica Turmel, formatrice du GRIP. Radio-Canada

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Canadian troops watching for human rights abuses as battle for Mosul rages
Canadian special forces troops have been told to keep an eye out for possible human rights abuses and sectarian score-settling as the battle to liberate Iraq's second largest city continues to unfold. The bloody fight to evict the Islamic State in Syria and Iraq (ISIS) from Mosul — which has been going on for almost a month — is being waged by uneasy allies who could quickly turn into enemies. Already Kurdish troops have been accused of destroying large numbers of Arab homes, and leaving Kurdish-owned homes untouched in areas cleared of ISIS control, according to a report released Sunday from Human Rights Watch. CBC News

INTERNATIONAL

A year after Paris attacks, Europe's extremism problem shows no signs of going away
In a series of attacks on "precisely chosen targets," nine Islamic State militants wrought devastation in Paris on Nov. 13, 2015, killing at least 130 people. A year later, the world is still grappling with violence exported from Iraq and Syria and carried out by those influenced by the missive to build an Islamic caliphate, even as the group's footprint shrinks. How did Europe get to this point? And why is it so hard for authorities to stop it? This is a look back at The Post's reporting on a year of attacks, and an attempt to explain how we got there. Washington Post

Islamic State group flourishes and recruits in Pakistan
The Islamic State group is increasing its presence in Pakistan, recruiting Uzbek militants, attracting disgruntled Taliban fighters and partnering with one of Pakistan's most violent sectarian groups, according to police officers, Taliban officials and analysts. Its latest atrocity was an attack Saturday on a Sufi shrine in southwestern Pakistan that killed at least 50 people and wounded 100 others. The group said in a statement that a suicide bomber attacked the shrine with the intent of killing Shiite Muslims and issued a picture of the attacker. Associated Press (Yahoo News)

Colombia signs peace deal with FARC
Colombia's government and the FARC rebel group signed a revised peace accord Saturday after years of negotiations and a half a century of conflict. Colombian President Juan Manuel Santos announced the new deal in a TV address Saturday evening, saying it will build a "broader, deeper peace." A peace deal negotiated earlier this year with FARC rebels was unexpectedly defeated by Colombian voters in October. Many were angered by what they saw as insufficient punishment for those who perpetrated a litany of crimes against their people. Negotiations for a peace deal continued after the defeat with rebels

and those opposed to the original agreement. Among the new stipulations are reparations for victims which will come from FARC's assets and money, Santos said. FARC can still form a political party under the agreement and members with minor offenses can apply to get their records cleared. CNN

2 dead after powerful earthquake, tsunami hit near Christchurch, New Zealand
New Zealand Prime Minister John Key says at least 2 people were killed in powerful earthquake. The earthquake hit New Zealand's South Island early Monday, shaking residents awake, causing damage to buildings and prompting emergency services to warn people along the coast to move to higher ground to avoid tsunami waves. The magnitude-7.8 earthquake struck just after midnight in a mostly rural area close to the city of Christchurch, but appeared to be more strongly felt in Wellington, the capital, more than 200 kilometres (120 miles) to the north. The quake was followed by a number of strong aftershocks. The quake temporarily knocked out New Zealand's emergency call number, 111, police reported. Associated Press (Global News)

Large 6.2 Magnitude Earthquake Hits Northeastern Argentina
A large earthquake with a magnitude of 6.2 has struck northeastern Argentina, but there are no immediate reports of damage or injuries. The earthquake struck just after 8 a.m. local time (14:00 GMT) and was centered about 16 miles (26 kilometers) north of the community of Chilecito in La Rioja province, near the border with Chile. It had a depth of around 62 miles (100 kilometers). Associated Press (ABC News)

Around 80,000 rally in Barcelona for Catalan independence
Around 80,000 people rallied in Barcelona on Sunday in a show of support for Catalan leaders locked in a tug-of-war with Madrid over independence for their region, police said.The demonstration aimed in particular at supporting Catalonia's former president, Artur Mas, and the head of its parliament, Carme Forcadell. Agence France-Presse

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

GgNewsCA
Red Cross funds study into how Fort McMurray wildfire affected indigenous people https://t.co/T7o5DpW2LS

metromontreal
Une étude sur les effets de l'incendie de Fort McMurray sur les membres des Premières Nations http://bit.ly/2fKhnlZ

CBCCanada
Tug recovery near Bella Bella delayed again by poor weather http://ift.tt/2eT9ITt

LAW ENFORCEMENT / APPLICATION DE LA LOI

nationalpost
RCMP tracked 89 indigenous activists considered 'threats' for participating in protests http://natpo.st/2q86VYv

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

LP_LaPresse
Les agressions sexuelles, un fléau dans les communautés autochtones https://t.co/IUFNNrxaNb

OTHER / AUTRE

CBCNunavut
Delta Airlines flight 37 enroute from London Heathrow to Seattle diverted to Iqaluit for a medical emergency this afternoon.

CBCPolitics
Canadian troops watching for human rights abuses as battle for Mosul rages http://ift.tt/2g7RyiL #hw #cdnpoli

INTERNATIONAL

natnewswatch
At least 2 dead after 7.8 magnitude earthquake shakes New Zealand https://t.co/pQy9iRTQL8

nationalpost
Two dead after earthquake rocks New Zealand as evacuation orders stand even as tsunami threat recedes http://natpo.st/2fNEsms

CKNW
No #tsunami threat for #BC after #NewZealand quake generates #tsunami

CBCNews
7.8 magnitude earthquake strikes New Zealand http://www.cbc.ca/news/world/new-zealand-quake-1.3848896?cmp=rss ...

HumanityRoad
#nz Great tips from @Caz_Milligan on what to do when an earthquake hits #hmrd

TheEconomist
Colombia and the FARC strike a new peace agreement https://t.co/fNv2p3JrMr

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

Today's News / Actualités
November 15, 2016 / le 15 novembre 2016
08:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 08h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Liberals to revamp 'discriminatory' age law for anal intercourse

The Liberal government is repealing what it calls a "discriminatory" law that makes it illegal to have anal sex under the age of 18, unless it is between a husband and wife. Right now, the age of consent for sexual activity is 16 but the Criminal Code prohibits anal intercourse for people under the age 18 unless they are husband and wife, a discrepancy many have denounced as unconstitutional. Justice Minister Jody Wilson-Raybould announced the change today, saying the "outdated" law violates equality rights. Wilson-Raybould said the change is substantive and not just symbolic. In 2014 and 2015, there were 69

charges laid under the law, though none led to convictions. The minister said appellate courts across the country have deemed the law unconstitutional. The bill, C-32, is retroactive to 1983, but Wilson-Raybould said the law does not mean automatic pardons. That falls under the jurisdiction of **Public Safety Minister Ralph Goodale**, who is studying the issue, she said. Jake Wright, press secretary to interim Conservative Leader Rona Ambrose, said she backs the change. CBC News

Police investigating death of seven-year-old Nia Eastman in Choiceland
An Amber Alert issued on Thursday had a tragic result with the discovery of the body of seven-year-old Nia Eastman, just hours after the body of her father, Adam Jay Eastman, was found near Snowden. Nia's body was found in a home in Choiceland shortly after noon on November 10, just a block from WM Mason School where she attended Grade One. Nia was reported missing after her father failed to return her home to her mother on November 9. He had picked her up after school and was to have returned her by 7 pm. Eastman's body was found on a quarter-section of land along Highway 55 near Snowden, dead of self-inflicted injuries. **Federal Minister of Public Safety Ralph Goodale** issued a statement on Nia's death on Thursday afternoon. "***It was with great sadness that I learned that Nia Eastman was found deceased by the RCMP today following an Amber Alert***," **said Goodale** in the statement. "***It is heartbreaking to lose a child, and nothing can ever make that right. I wish to extend my heartfelt condolences to Nia's mother and family, her community and all those who have been touched by this tragedy. We are all grieving together this most terrible loss***." Melfort Journal

TOP STORIES / MANCHETTES

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Saskatchewan emergency smartphone app doesn't issue Amber Alerts
The Saskatchewan government's emergency notification app for smartphones does not notify the public when an Amber Alert is initiated. The SaskAlert app notifies the public for emergency situations such as boil water advisories, tornado warnings and freezing rain. But a government spokesperson tells CTV Regina that although the app is capable of issuing missing person information, the administration of the Amber Alert program falls under the RCMP's jurisdiction. CBC News

'A lot of learning to do': Wawanesa Insurance on Fort McMurray wildfire response
Alberta's second-largest insurer admits it could have done things better in its response to the Fort McMurray wildfire. Wawanesa Insurance will review how the company performed in the aftermath of the wildfire, the company said in an interview with CBC News. It will survey all of its customers once claims are completed. "I think there's a lot of learning to do on this. It's tough," said Graham Haigh, Wawanesa's vice-president, business development. "It really does kill both us and our staff when we are not producing service at a level that we would want to for our families." The Insurance Bureau of Canada said the Fort McMurray wildfire is the country's costliest disaster. It estimates payouts will hit $3.58 billion. Wawanesa said it has settled 74 per cent of the 4,094 claims it has received to date. It has closed 71 per cent of 2,997 homeowner claims. CBC News

Before practice, the real thing for Arrowsmith Search and Rescue
Last week, area search and rescue teams were looking forward to some training at Little Qualicum Falls on Sunday. Little did they know they would be needed for a real-life rescue on Saturday in the hills above Nanoose Bay. A Victoria man was tired, cold but not seriously hurt after being rescued at Bonnell Falls. Arrowsmith Search and Rescue's Ken Neden told The NEWS the man was hiking with a friend on a trail near the falls and proceeded down a muddy slippery section with the aid of a rope that was in place... Neden said the man's friend called the RCMP for help who then called Arrowsmith Search and Rescue to assist at 3 p.m. Saturday. Parksville Qualicum Beach News

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

NIL

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Peace Bridge lane restrictions begin
Crossing the Peace Bridge may be more difficult for the next six months, as traffic will be down to one lane in each direction from November 15 through May 15, 2017 for construction related to the ongoing $100 million Peace Bridge rehabilitation. “So long as Customs appropriately staffs and keeps inspection lanes open this winter, then we anticipate little to no traffic disruption,” remarked PBA Board Chair Sam Hoyt. “But that commitment really needs to be made and maintained and that is why the Authority is calling on all levels of government from both sides of the border to get involved and speak up about the importance of these traffic flow and staffing issues at the Peace Bridge. We’ve gotten strong indications from U.S. Customs and Border Protection that they can meet the staffing demand and we need Canada Border Services Agency to follow suit.”” (…) A series of traffic management improvements have been completed, including the recently completed widening of the Peace Bridge’s U.S. approach allows an increased number of trucks to be queued off the bridge. An eighth commercial inspection booth is also slated for installation by December to increase throughout capacity for trucks within the U.S. plaza. On the Canadian side, a partial fourth lane has been added to provide Canada-bound trucks and NEXUS users easier access off of the bridge. WBFO; WKBW

Thicker Canada-US border unlikely, Ridge says
The Canada-U.S. border is unlikely to see any thickening under president-elect Donald Trump despite the Republican's protectionist campaign rhetoric, former American security czar Tom Ridge said Tuesday. While Trump's views on Mexican migrants and Syrian refugees appeared to be sharply at odds with Canada's approach, Ridge said Canada needs to take a deep breath and wait to see what actually emerges from a Trump administration. Ridge, appointed as first Homeland Security secretary in the aftermath of the 9-11 attacks on the United States, was fiercely critical of the campaigning Trump, denouncing his "bumper-sticker approach" to policy and a bombastic tone that "reflects the traits of a bully." Now that the campaign is over, Ridge said he hoped Trump would "substantially alter his approach" to borders. "There's always a difference between the political rhetoric and actually the governing posture that he takes," Ridge told The Canadian Press in an interview. (…) Any thickening of the northern border in particular would be a "huge mistake" given the critical relationship Canada and the United States have, he said. "If you want to look at a relationship that has proven to be very sensitive to the needs of both countries, and the culture of both countries, take a look at the Canada-U.S. border." Canadian Press (Mississauga News, Times Colonist, Toronto Sun, iPolitics, CTV News)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

From WhatsApp to Hawala, How the Taliban Moves Money Around
The Taliban has been trying to fundraise on the internet longer than Afghanistan’s current government has existed. In recent years, however, the insurgents have turned to internet messaging platforms secured by end-to-end encryption, such as Telegram, Viber, and WhatsApp, to solicit donations. On September 9, the Taliban posted a statement to its English Telegram channel in anticipation of an annual Islamic holiday. “As you know, Islamic Emirate of Afghanistan is the guardian of thousands of widows and orphans and provide them sacrifice of Eid-ul-Azha,” read the post, written in broken English. It implored

"every fortune and sympathizer Muslim" to contact the Taliban's treasury through its Gmail account or a phone number linked to Telegram, Viber, and WhatsApp. The statement failed to mention how potential donors could send money to the Islamic Emirate of Afghanistan, the Islamic state that the Taliban ruled from 1996 to 2001 and the name by which it still refers to itself. Taliban officials declined to comment for this article for "security reasons," referring to whatever money transmitter the insurgents might use as "a secret of the Emirate." Motherboard

Signal Protocol's crypto core has no major flaws, researchers find
A group of computer science and cryptography professors and doctoral students has effected a security analysis of the secure messaging Signal Protocol – specifically, of its Key Agreement and Double Ratchet multi-stage key exchange protocol (the effective cryptographic core). The results of the analysis are encouraging. "We have found no major flaws in the design, and hope that our presentation and results can serve as a starting point for other analyses of this widely adopted protocol," they noted in the paper detailing their research. The Signal cryptographic protocol is used by a variety of popular messaging apps, including Facebook Messenger, WhatsApp, Google Allo, Signal (the app developed by Open Whisper Systems, the company that also developed the secure protocol in question), as well as Silent Circle, CryptoCat (v2), and others. In short, billions of users depend on it for end-to-end encrypted, secure communication. Help Net Security

Spies Use Tinder, and It's as Creepy as You'd Think
On September 4, a group of young activists planned to attend a demonstration against Interim President Michel Temer in the city center of São Paulo. They never made it. Their group had been infiltrated by an Army Captain Willian Pina Botelho—via Tinder. Surveillance and infiltration are not new tactics, but the ACLU revelation last month that Twitter, Instagram, and Facebook had been sharing data with surveillance service Geofeedia reminds us that the internet is bringing it to whole new levels. The story of the "Tinder infiltrator" serves as a reminder for a generation of young activists who are organizing online: don't stop organizing, but be vigilant. Motherboard

Hacker shows how easy it is to take over a city's public Wi-Fi network
In a perfect example of how public wireless networks can be dangerous for privacy and security, an Israeli hacker showed that he could have taken over the free Wi-Fi network of an entire city. CSO

Cozy Bear campaign 'PowerDuke' rides post-election wave
Russian advanced persistent threat (APT) group Cozy Bear has reportedly been targeting U.S. think tanks and non-governmental organisations (NGOs) in the immediate aftermath of the U.S. presidential race, devising malware campaigns that capitalise on post-election controversies. Cozy Bear, aka APT29, is already known for previously hacking the Democratic National Committee (DNC) and targeting Russia-focused think tanks in Washington D.C. According to a report from incident response and suppression service Volexity, the APT is now focusing its efforts on organisations specialising in national security, defence, international affairs, public policy and European and Asian studies. While these organisations and their members operate outside of the government, "A lot of times these people have close ties with political [groups]," noted Steven Adair, founder and CEO of Volexity, in an interview with SC Media. And "some of these folks may have access to or be involved with future administrations." SC Magazine

BlackNurse Low-Volume DoS Attack Targets Firewalls
A type of denial of service attack relevant in the 1990s has resurfaced with surprising potency against modern-day firewalls. Dubbed a BlackNurse attack, the technique leverages a low-volume Internet Control Message Protocol (ICMP) -based attack on vulnerable firewalls made by Cisco, Palo Alto, SonicWall and others, according to researchers. TDC Security Operations Center, a security firm that published a technical report (PDF) on BlackNurse this week, said the attack is more traditionally called a "ping flood attack." In this type of assault, traffic volume doesn't matter as much as the type of packets sent, researchers said. Threat Post; CSO

LAW ENFORCEMENT / APPLICATION DE LA LOI

Mental-health workers to join Mounties in cars
Mental-health workers soon will be riding shotgun in some Kelowna police cars. A new policing initiative aims to pair such workers with RCMP officers in a bid to better help street people avoid criminal entanglements, city council heard Monday. Full details of the program, similar to ones already operating in some B.C. cities, will be announced soon, Kelowna RCMP Acting Supt. Brent Mundel told council. Councillors praised the RCMP for trying to work with social service agencies to curb what appears to be a local crime rate that's once again on a worrying rise. "The collaboration you're working on is phenomenal," Coun. Ryan Donn told Mundel. Coun. Gail Given said Kelowna's street population seems to have "grown quite considerably" during the past year. Dealing with challenges that flow from an increasing homeless and drug-involved population is the "top priority" for city council, Mayor Colin Basran said. Daily Courier (2016-11-14)

Former RCMP officer changes plea to guilty on one charge of assault.
Crown agrees to stop process on a second charge of assault plus a charge of uttering a threat. A former P.E.I. RCMP officer has pleaded guilty to assault. Jeffrey Rae Gillis appeared before Chief Judge Nancy Orr this morning in provincial court in Charlottetown where a trial on three charges was scheduled. With his guilty plea, the Crown stayed another assault charge and a charge of uttering a threat. Sentencing was adjourned until Jan. 18, 2017 to give time to prepare a pre-sentence report. While Charlottetown police were at Gillis's home investigating the assault complaint, the officers became aware of multiple weapons stored in the home, and sought a warrant to return to the home, search it, and seize the weapons. It was done, said officers in court, out of concern for public safety and not as part of a criminal process. Gillis will be back in court this afternoon where Judge Jeff Lantz will give a ruling after Gillis's lawyer challenged the validity of that warrant. Guardian

Nia Eastman, father died by murder, suicide: RCMP
Autopsies on seven-year-old Nia Eastman and her father have determined the causes of death were homicide and suicide. In a statement released Tuesday, the RCMP said the specific causes of death will not be released, but there is no evidence anyone else was involved. Adam Jay Eastman was found dead on Nov. 10, the same day RCMP issued an Amber Alert to find seven-year-old Nia Eastman. She was later found dead inside a residence in Choiceland, Sask. Police say no charges will be laid. More to come... CTV News

Suspicious package prompts evacuation of Red Deer RCMP headquarters
Police are investigating after a suspicious package was brought into the Red Deer RCMP's downtown detachment Monday, prompting road closures and a late-night evacuation. A section of 51st Avenue between 46th Street and 47th Street was closed for several hours after a resident discovered the suspicious package and brought it into the downtown headquarters. The explosives device unit was called in, and all non-essential staff were evacuated from the building. Officers canvassed the neighbourhood to advise businesses of the ongoing investigation. Officers "neutralized the device" shortly after 10 p.m. but police say they have yet to determine whether or not it was explosive. No one was hurt in the incident. The incident prompted RCMP to issue a reminder to the public. They say suspicious packages should be reported to police immediately, and should never be moved or touched. CBC News

Window shutter shot at S. Rutland Elementary over weekend
RCMP recovered evidence at South Rutland Elementary School showing damage to a window screen was caused by a small caliber firearm. On Nov. 14, shortly after 8 a.m., the Kelowna RCMP received a mischief report after school official's observed damage to the rear of South Rutland Elementary School in the 200 block of Mallach Road. School officials said the damage occurred sometime over the past weekend, between end of the school day on Thursday Nov. 10 and before the start of the school day of Monday Nov. 14. The damage was contained to a metal rolling shutter, which covers a classroom window at the rear of the school. RCMP made a full examination of the scene, with the assistance of both Police Dog Services and the Integrated Forensic Identification Services and recovered evidence that the damage caused is consistent with a small caliber firearm. Lake Country

Incivility most common complaint about Windsor police

Incivility is the most common complaint received by the Windsor police, which is often necessary given the situations many officers experience, according to Chief Al Frederick. He supports the latest review by the Ontario government, which is looking at how it investigates reports of officer wrongdoing. Frederick recognizes, though, there is no tolerance for officers insulting or demeaning the people they deal with. "Officers are interacting with people at their worst, during crises, and so sometimes they have to raise their voice or use language [that is] not appropriate in other circumstances," Frederick said. "I can live with that, knowing the volatility of situations on the streets." The Attorney General's office has ordered a review of police. The Ontario Independent Police Oversight Review is holding a public meeting held in Windsor on Tuesday. "Trust between a community and its police is a moving target," Federick said. "Yes, the oversight and the review of that oversight is a necessary tool." CBC News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Détenu agressé à Renous
Un détenu avait été victime de voies de fait samedi soir à l'Établissement Atlantique, un établissement fédéral à sécurité maximale situé à Renous, dans la région de Miramichi. Dans un communiqué de presse, Service correctionnel du Canada (SCC) indique que le détenu blessé a été immédiatement évalué par le personnel et transporté à l'hôpital pour y recevoir des soins. Aucune autre information concernant l'agression et l'état de santé de la victime n'ont été dévoilés. Le détachement de Blackville de la Gendarmerie Royale du Canada et l'établissement mènent une enquête sur l'incident. Les agresseurs ont été identifiés et des mesures appropriées ont été prises, avance Service correctionnel du Canada. Acadie Nouvelle

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

London police carding will meet minimal standards, chief says
The chair of London's police board said there are no plans to crack down on the Chief John Pare's plans to roll out street checks under new regulations in January, the board chair said. Jeannette Eberhard said the board supports the "guidelines and regulations" for the controversial practice as laid out by the Ministry of Community Safety and Correctional Services last spring after a round of public consultations across Ontario. "Our board is compliant with our ministry," she said. "I will look to their wisdom in their consultations." Controversy over a receipt that officers will be required to issue when they stop and question people re-ignited calls for a ban in this city -- where the most recent public statistics show that black and indigenous people were three times more likely to be stopped by police than white people -- altogether last week. At Thursday's police board meeting, Pare presented an updated draft of the receipt that will be handed out to people who are subjected to carding by London police. Police had revised the draft to include some explicit information about how citizens can access information about the stop under the Freedom of Information Act, as requested by the board in a motion last month, but decided not to add an area for officers to include the "reason" for the stop. London Free Press

VPD responds to nearly a dozen of opioid ODs in one day
A warning from Vancouver Police and health workers to drug users after a rash of opioid overdoses in the Downtown Eastside. The VPD says there were 11 ODs reported yesterday – luckily no one has died. Police believe fentanyl is to blame; the suspected drug appears to be purple in colour. You're advised not to snort, swallow, or inject drugs alone and call 911 immediately if symptoms, like trouble walking or talking, start to show. News 1130; Global News

Medicine Hat still a safe place, city police stress
Police are assuring local residents that Medicine Hat remains a safe community, despite two homicides occurring barely a week apart. "Having two homicides occur in such a short time frame is tragic and unprecedented in Medicine Hat," said Insp. Brent Secondiak Monday at a Medicine Hat Police Service press conference. Second-degree murder charges were laid against Noah Harrison Bentley, 26, over the death of Brenda Woloski, 53, this weekend. (...) These two incidents bring the number of homicides in

the city up to three for 2016. (…) According to police-reported crime statistics from StatsCanada, the homicide rate for 2015 was 1.68 homicides per 100,000 population in Canada. This is the highest rate since 2011, but remains below average for the previous decade. Medicine Hat News

Crime rides wave of theft
Kelowna's crime rate is up this year, thanks in large part to preventable property crimes. That was one of the conclusions reached during the RCMP's quarterly report to city council Monday. Kelowna's well-documented crime rate jumped in 2015, and acting top cop, Insp. Brent Mundle, said calls for service jumped during the third quarter of this year. Calls for service increased nearly 8.9 per cent – more than 3,900 – over 2015. Mundle said the biggest concern centres around property crime. Castanet

Prince George may act as model in addressing Merritt crime
The city of Merritt is reaching out to Prince George for help fighting crime. Merritt city councilor Mike Goetz was at the Union of B.C. Municipalities meeting this year when he heard how Prince George is using simple city bylaws to deal with suspected criminal activity at local hotels and businesses. CBC News

Twitter rolls out new tools to combat abuse, cyberbullying after months of criticism
Twitter, facing pressure for not doing enough to curb abusive behavior on its platform, said on Tuesday it would upgrade some features to better combat cyber-bullying. The company said it would expand the "mute" option to allow users to block tweets based on keywords, phrases and the content of conversations from a user's notifications .The "mute" option currently allows users to block tweets from accounts. The change will be rolled out to all users in the coming days, Twitter said in a blog post. "Because Twitter happens in public and in real-time, we've had some challenges keeping up with and curbing abusive conduct. We took a step back to reset and take a new approach, find and focus on the most critical needs, and rapidly improve," read the blog post. Global News

'It's just a waste': Refugees lack opportunity to play elite soccer
A local soccer player and coach are concerned newcomers to Winnipeg don't have the opportunity to play elite level soccer, which could pivot some from the draw of street gangs. When Omar Rahimi - an immigrant from Iraq - arrived in Winnipeg in 2001, soccer was the first thing he pursued. He went to Gordon Bell High School and played there, and then went on to play in the premier division for about eight years. The sport transformed his new life in Canada, he says. "Many of my good friends are from soccer. It was the best part of my transition. If not for soccer, I don't think I would be doing this good," he says, adding the sport also makes it easier to cope with stress. Many people who live in neighbourhoods that are hot spots for gangs are newcomers to Canada and their children are often targeted for recruitment, according to Winnipeg police. Rahimi added the sport made it easier to cope with stress. CBC News

Police ask for budget increase, more officers
The Saskatoon Police Service is asking the city for a budget increase to hire more police officers and other staff in 2017. The preliminary police budget calls for a $3.3 million increase to hire four new patrol officers and two detectives. The budget also includes additional medical staff in the detention unit and a lawyer and privacy officer to facilitate freedom of information guidelines. It's a 3.9 per cent increase over the 2016 budget. Mayor Charlie Clark says it's important to find efficiencies within the police service to tackle crime, but there is also a need for more officers as the city grows. CTV News

Police budget requires a balancing act
An editorial states, "Faced with an initial budget projection that would see property taxes rise by 3.97 per cent if newly elected councillors are unable to whittle down the city's spending when they begin deliberations at the end of November, it's understandable that Mayor Charlie Clark and some others might balk at Police Chief Clive Weighill's request to add $3.3 million to the allocation for his department. Granted, it's up to the board of police commissioners to assess and make a recommendation to council about the size of the police budget, which claims by far the largest share of property taxes at around 23 cents of every dollar collected. However, policing costs that continue to rise generate plenty of debate among elected officials, because voters hold them ultimately responsible for the associated property tax

increases. (...) The budget increase of $3.3 million that Chief Weighill seeks — to among other things hire four patrol officers and one officer each for special investigations and cyber crimes — presumably includes the above $2.6 million for inflation, pay raises and other costs. So, if the police commission grants Weighill's request, the additional cost to the city budget will be about $700,000, or an increase of close to 0.34 per cent, bringing the total property tax hike awaiting taxpayers to about 4.3 per cent, according to city officials." StarPhoenix

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Why writer Katherena Vermette searches the Red River
Katherena Vermette joins a volunteer search party on Winnipeg's vast Red River in the new short documentary This River. The organization, known as Drag the Red, routinely conducts searches in the river for clues around the disappearance of Indigenous friends and family. The group formed in 2014, after the body of a teenage girl was discovered in the Red River, inciting public outcry and renewed calls for a national inquiry into missing and murdered Indigenous women. It is believed that as many as 4,000 Indigenous women, men and children have gone missing or been murdered since 1980 in Canada. The documentary features Kyle Kematch, whose sister went missing over five years ago. Kematch and Vermette discuss the despair and frustration of working with police. "We reported [her disappearance]. We didn't get any response the first day. Second day, we went down there and they just kept saying, 'Well, if we find her we don't need to tell you where she is,'" said Kematch, who searches the water almost every day. "Took a couple weeks, but they labelled her as a prostitute and when they label her as a prostitute, that's when everybody stops caring. That's where it's wrong. It shouldn't matter what your race is or what you did or what you are doing. Everybody deserves to live." CBC News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Canopy Growth becomes Canada's first marijuana unicorn, worth $1 billion
Medical marijuana producer Canopy Growth Corp. has become the first Canadian company in the sector valued at more than $1 billion after strong quarterly results sent the stock on a tear. The company was trading hands at $11.16 per share when stock markets closed in Toronto on Monday. That values the company at almost $1.3 billion. As recently as July, the company was worth less than a third of that. But that was before seven U.S. states voted last week to legalize some form of either recreational or medical marijuana. (...) During a conference call to discuss the company's quarterly results, CEO Bruce Linton emphasized the company's efforts to expand its production capacity to keep up with demand. CBC News

CAA wants to prepare the public for stoned drivers
The Canadian Automobile Association is lobbying for a government-funded public education program to warn of the dangers of cannabis-impaired driving before Canada legalizes recreational pot. Police will also need more funding to learn how to recognize and investigate drug-impaired drivers, says the CAA. The Liberal government has promised to introduce legislation legalizing recreational marijuana next spring and a committee report on the process is expected at the end this month. The CAA helped fund a study by the Ottawa-based Traffic Injury Research Foundation that suggests legalization will pose "incredible challenges" for managing pot-impaired drivers. The study is sure to inflame the escalating propaganda war over marijuana's harms and benefits, because it is premised on the assumption that access to legal cannabis will increase traffic accidents. The CAA commissioned a poll that found almost two thirds of respondents are worried roads will become more dangerous after legalization. CTV News (Civilized.life)

PUBLIC SERVICE / FONCTION PUBLIQUE

How politics sabotaged the federal government's grand IT plan, Shared Services Canada
An opinion piece states, "Liseanne Forand really didn't know what to expect. On Aug. 4, 2011 she was making her way on foot to Phase III of the Gatineau office complex known as Place du Portage. A career bureaucrat, Forand had, the day before, been appointed president of Shared Services Canada - a new federal department that would manage the government's email, data centres and telecommunications. Her mandate - representing about one-third of the federal government's $5-billion-a-year technology services budget - was breathtaking in its scope and complexity. She was to simultaneously streamline and modernize the government's electronic backbone, and keep the old gear running. Sixty-three email systems would be collapsed into one. More than 500 data centres were to be decommissioned, to be replaced by a mere handful. Fifty telecommunications networks connecting 3,500 federal buildings were to be upgraded. Forand was to do this with staff cobbled together from 43 different departments. But on this day, she had no office, and the paperwork had been approved for just 1,200 of an eventual 6,000 employees." Postmedia News (National Post)

OTHER / AUTRES

Sodomie: le fédéral veut éliminer un article "discriminatoire" du Code criminel
Toutes les pratiques sexuelles seront désormais traitées sur un pied d'égalité avec l'abrogation d'un article "discriminatoire" du Code criminel qui interdisait partiellement les relations sexuelles anales. C'est ce qu'a plaidé la ministre de la Justice du Canada, Jody Wilson-Raybould, mardi, après avoir déposé le projet de loi C-32 à la Chambre des communes. La mesure législative ne prévoit pas de pardon pour les personnes qui ont été reconnues coupables d'avoir enfreint l'article 159 du Code criminel dans le passé, selon ce qu'a indiqué la ministre. Elle a cependant fait remarquer que la disposition a été jugée "inconstitutionnelle" par plusieurs tribunaux à travers le pays. La Cour d'appel du Québec fait partie du lot. Les représentants de la communauté LGBTQ2 qui assistaient à l'annonce, mardi, au parlement, ont accueilli favorablement le dépôt du projet de loi C-32, qu'ils considèrent comme une avancée. Ils attendent maintenant que le gouvernement bouge dans un autre dossier, celui des excuses aux fonctionnaires et aux militaires remerciés en raison de leur orientation sexuelle. Ce dossier atterrira notamment sur le bureau du député Randy Boissonnault, fraîchement nommé conseiller spécial sur les enjeux de la communauté LGBTQ2 par le premier ministre Justin Trudeau. L'élu albertain, qui est ouvertement homosexuel, n'a pas voulu se prononcer sur un échéancier, mais il a dit avoir l'intention de "rectifier les injustices commises dans le passé". La Presse Canadienne (L'actualité); Canadian Press (Ottawa Citizen, National Post, CTV News); News 1130; International Business Times (2016-11-15; iPolitics; Le Devoir (2016-11-14)

Edmonton Centre MP named special advisor on LGBTQ2 issues
Prime Minister Justin Trudeau has named an Edmonton MP as his special advisor on LGBTQ2 issues. Randy Boissonnault will work with advocacy groups to promote equality for lesbians, gays, bisexual, transgender, queer and two-spirited people - a term used broadly to describe indigenous people who identify as LGBTQ. Boissonnault, who represents the Edmonton Centre riding, will also be tasked with addressing historical and current discrimination against LGBTQ2 people. He will, however, stay on as parliamentary secretary to the minister of Canadian Heritage. The announcement comes as the Liberal government prepares to introduce legislation to repeal a Criminal Code provision on anal intercourse. Canadian Press (CTV News); CBC News

Turkish-Canadian Davud Hanci held in solitary confinement: wife
The wife of a Calgary imam jailed in Turkey says he is being held in solitary confinement and she's worried about his well-being. Davud Hanci, who has Canadian and Turkish citizenship, was arrested in July shortly after a failed coup attempt. Rumeysa Hanci says she has not been able to speak to her husband in more than three months and says it's been like torture for her and their two young sons. She adds Canadian government officials have not had access to him and he has only been able to see his lawyer twice. Canadian Press (Metro News)

INTERNATIONAL

Russian minister held in biggest Putin-era corruption case
Russia detained Economy Minister Alexei Ulyukayev on charges of taking a $2 million bribe to approve a major privatization sale, setting off shock waves as the highest-level official to face such treatment in President Vladimir Putin's 16-year rule. Ulyukayev, 60, was detained on Monday "in the act" of receiving the cash, said Russia's Investigative Committee. He was later charged with demanding the money from Rosneft to allow its purchase last month of the government's 50 per cent stake in regional oil producer Bashneft, the agency said in a statement. The economy minister denies any wrongdoing, his lawyer Timofei Gridnev told Business FM radio. Investigators moved that he be held under house arrest before he arrived for arraignment Tuesday at Moscow's Basmanny Court. Hamilton Spectator

German police raid offices of Islamist group allegedly recruiting youths for Syria
The German government announced Tuesday it had banned an Islamic group, "The true religion," which is suspected of targeting teenagers to radicalize to fight in Syria and Iraq. At the same time, police raided about 190 offices, storehouses, mosques and apartments of members and supporters. In searches in 60 cities in western Germany and in Berlin, police seized documents, hard drives, smartphones and weapons, German Interior Minister Thomas de Maiziere said. Nobody was detained. The group -- also known as "Read!" -- has been distributing German-language copies of the Qur'an across the country. The interior minister said that more than 140 youths had travelled to Syria and Iraq to join fighters there after having participated in the group's campaigns in Germany. Associated Press (CP24; CTV News); Reuters (Reuters; CBC News)

Light sentences for 2 of 3 ISIS conspirators in Minnesota
A Minnesota man who admitted plotting to join the Islamic State of Iraq and Syria (ISIS) has been sentenced to time served by a judge who said he hopes to see the man rehabilitated. Abdullahi Mohamed Yusuf is the first of nine men being sentenced in Minneapolis this week in the plot. The 20-year-old pleaded guilty more than a year ago of conspiring to provide material support to ISIS, and testified against some of the others. U.S. District Judge Michael Davis sentenced Yusuf to the 21 months he's already served in jail, plus 20 years of supervised release. Davis said it didn't make sense to send Yusuf to prison because the government would miss a chance to help him. CBS News

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

RalphGoodale
Profondément perturbé par la haine antisémite visant un rabbin d'Ottawa. Il n'y a pas de place au Canada pour de tels actes exécrables.

cbcdaveseglins
Federal "Green Paper" floats ideas to expand police power to combat online criminals, extremists. Minister @ralphgoodale seeking pubic input

JodieEmery
This is VERY encouraging, @RalphGoodale!
#cdnpoli https://twitter.com/Safety_Canada/status/798251694576508928

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

vicecanada
After 33 days under water, this leaking tug boat is finally coming out: http://bit.ly/2gcgw1o

CBCCanada
$5.3B to flow during Fort McMurray rebuild, says Conference Board of Canada http://ift.tt/2gdm4b6

nafeesakarim
Extremely high tides start this week. What's being done to prevent flooding? I have details on @CTVMorningLive. #kingtides #kingtidesbc

nafeesakarim
Crews from @CityofVancouver are putting down sandbags at Locarno Beach to protect from #kingtides flooding. #kingtidesBC

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

StephanieCarvin
Today I am speaking to #SECU on Bill C-22. 3:30pm Eastern. Here is the audio link: http://parlvu.parl.gc.ca/

cbcdaveseglins
Federal "Green Paper" floats ideas to expand police power to combat online criminals, extremists. Minister @ralphgoodale seeking pubic input

NATIONAL SECURITY / SÉCURITÉ NATIONALE

caparsons
The RCMP's Counterterrorism Center in Ottawa http://www.matthewaid.com/post/152250163076 …

thecribby
How terrorism suspect Aaron Driver hid behind digital encryption http://on.thestar.com/2ezLoHK via @torontostar https://t.co/tMxgKOOf9C

Colinfreeze
Good on @rcmpgrcpolice for engaging with @cbcdaveseglins @thecribby for case studies on "going dark" issues... https://www.thestar.com/news/canada/2016/11/15/top-secret-rcmp-files-show-digital-roadblocks-thwarting-criminal-investigations-in-canada.html … Attn

cforcese
When have time, shall write article re: how, since 18th century, privacy right has *always* been about balance. So this is important debate.

neuwaves
Seems like there'd be some juicy bits in the secret Aaron Driver case file beyond what's in here. Hey @cbcnews can you publish that or nah

Colinfreeze
Subsequent to story received info that RCMP NSJOC has 5.5 full time police personnel assigned. (Let's Assume + 1 CSIS, +1 CBSA +1 CIC +1CSE) https://twitter.com/caparsons/status/798319902478082048

StephanieCarvin
@Colinfreeze @caparsons there is no way NSJOC has access to all of the databases. Not possible. Have no idea where that prof is getting that

StewartBellNP
1/"The increasing potency and reach of terrorist groups ..." http://cs.is/2fuB03h

StewartBellNP
2/ "...and a sense that governments' response to the threat has been inadequate ..." http://cs.is/2fuB03h

StewartBellNP
3/ "...is creating deep political divisions and fueling support for populist solutions." http://cs.is/2fuB03h

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CBCNews
MPs to hear legal, logistical challenges of rescuing Yazidi genocide victims http://www.cbc.ca/1.3850033

courosa
"Ontario teen who called for 'white' Canada has laptop seized by CBSA" http://globalnews.ca/news/3052556/ontario-teen-who-called-for-white-canada-has-laptops-seized-by-cbsa/ … #racism

CP24
Thicker Canada-U.S. border unlikely under Trump: former American security czar http://www.cp24.com/news/thicker-canada-u-s-border-unlikely-under-trump-former-american-security-czar-1.3161645 …

Paul Dewar
This is in our community, in our space we must all stand together with Anna against hate #satndwithAnna #antiracism

CYBER SECURITY / CYBERSÉCURITÉ

motherboard
Spies use Tinder, and it's as creepy as you'd think http://bit.ly/2f0tHQg

VICEAU
NOW on #SBSVICELAND @BMakuch investigates the most significant computer security issues of our time

CTVNews
You can now use Skype without an account with new 'Guest' option http://ow.ly/FhVO306c1p4

amandacconn
"We are undertaking an effort to be able to do offensive cyber operations should we need to," Vance says

amandacconn
"But we aren't there yet," either from an authorization or capability perspective, he says

GlobalNational
Text message fraud cost Canadians half a million dollars so far in 2016 glbn.ca/LXeyMJ

VICELAND_ca
CYBERWAR with @BMakuch is back tonight investigating the fall out from the Ashley Madison hack at 10:30P ET/PT.

LAW ENFORCEMENT / APPLICATION DE LA LOI

TorontoStar
RCMP opened secret files to the Star, CBC to show how digital roadblocks thwart crime cases in Canada http://on.thestar.com/2ftELGh #Investigation

Eric_Szeto
Top-secret RCMP files show digital roadblocks thwarting criminal investigations in Canada http://on.thestar.com/2eA1Pns via @torontostar https://t.co/OMyMtTCCxq

neuwaves
Absolutely mind blowing that the RCMP will release docs on ONGOING CASES when it benefits them, not when it concerns, say, stingrays

neuwaves
Alt headline: The RCMP spoonfed us 10 cherry-picked cases to argue for new surveillance powers https://twitter.com/CBCNews/status/798495883549638656

vicecanada
Toronto police are going undercover to bust men having sex with other men: http://bit.ly/2g8jKD5

HuffPostCanada

CRA investigating dozens of Canadians over tax fraud linked to Panama Papers huff.to/2gblRoW

vicecanada
An Alberta judge hid the identity of a child lurer because he was worried about Creep Catchers: http://bit.ly/2fue7NA

CityNews
Vaughan teen charged with pointing laser at police helicopter, two planes http://ow.ly/8EqD306c1L0 https://t.co/S3UV2jruOa

CTVVancouver
ICYMI: Eye-popping costs have stalled the Vancouver Police Department's body-worn camera program, @ctv_jon reports

CTVNews
RCMP investigation has determined causes of death of Adam Jay Eastman and Nia Eastman were homicide and suicide

JdeMontreal
Allégations d'agressions sexuelles sur des autochtones: aucune accusation contre les six policiers à Val-d'Or. http://www.journaldemontreal.com/2016/11/15/allegations-dabus-physiques-et-sexuels-aucune-accusation-deposee-contre-les-policiers-de-val-dor …

VancouverSun
Fight between Mounties, teens, in Prince Rupert sparks internal probe https://t.co/PYktgbUPxp

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Abbynews
An inmate was airlifted after being assaulted at Matsqui Institution this morning. http://fb.me/1yj2vbGbm

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

620ckrm
Operation Red Nose to kick off in Sask. next week http://bit.ly/2eCazte

KelownaNow
Illegal tobacco rate holds steady in B.C. https://t.co/1dFdpyhylq

rcmpgrcpolice
Domestic violence rates in Shamattawa #MB fall thanks to @rcmpmb proactive, preventive policing. Read more: http://rcmp.ca/-Vui

vicecanada
Toronto police investigating alt-right posters as a hate crime: http://bit.ly/2fcQnup

JimBronskill
UPDATED: Drug decriminalization would bring health benefits, says internal federal study obtained by CP http://ctv.news/ShAHTxh #cdnpoli #hw

motherboard
This tiny plastic implant may disrupt America's opioid addiction problem http://bit.ly/2fC1vkR

HuffPostCanada
Ottawa to study the effects of violent pornography #cdnpoli http://huff.to/2fRcjuK

CBCCalgary
New calls for change follow two more deaths of Alberta children who received government ca… http://ift.tt/2eWTOnO

YQRCrimestopper
We are proud to officially welcome Inspector Davies to our @YQRCrimestopper family. @reginapolice @lnorm45

Justin Trudeau
Heureux d'annoncer que le député @R_Boissonnault sera mon conseiller spécial sur les questions liées aux LGBTQ2 : http://bit.ly/2eBEYry

CBCCanada
Liberals to revamp 'discriminatory' age of consent law for anal intercourse http://ift.tt/2fC0mdk

globalnews
Government announces legislation to repeal sect. 159 of criminal code which prohibits anal intercourse in some cases

CBCKatie
Government has introduced legislation to repeal laws against anal sex, amendment to ensure age of consent is same for all sexual acts.

cmaconthehill
Justice Min Jody Wilson-Raybould will soon announce bill to repeal section 159 of Criminal Code. Pride & trans flags up in foyer #cdnpoli

LoopEmma
I was surprised when I read that Criminal Code section a while ago that it was still in there. Good to see it go.

Justice Canada
#GoC proposes Criminal Code amendment to treat all forms of sexual activity equally #cdnlaw http://ow.ly/R7CW306c5zO

CRCVC
Invitation to participate in national survey into bullying in Canada - https://www.surveymonkey.com/r/bullyingincanada ...

Ottawa Police
Members of our Partner Assault Unit made sure to #wearpurple to #ShinetheLight on #VAW. Follow @OCTEVAW for events throughout November.

Marilyn Gladeau
In the House of Commons in purple, in recognition of the efforts to eliminate violence against women #ShineTheLight #wearpurpleday

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

CBCNews
'I remember them hypnotizing me': Check out Episode 4 of Who Killed Alberta Williams http://www.cbc.ca/missingandmurdered/podcast … #MMIW

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

BCheadle
ICYMI: Canada needs pot-impaired driver education before legalizing, says CAA https://t.co/KWECDVM6nu

vicenews
California just legalized recreational weed and this Canadian company wants to cash in http://bit.ly/2fSLI7S

PUBLIC SERVICE / FONCTION PUBLIQUE

StephanieCarvin
I teach at a school where 90% of my students end up in government. Most just want a non-insane recruitment process and to be paid. #cdnpoli https://twitter.com/CBCOttawa/status/794465491133878273

OTHER / AUTRE

rabbleca
Solidarity with Standing Rock continues to grow in Canada as First Nations see resonances at home #cdnpoli #NoDAPL http://buff.ly/2faNR80

CTVNews
Liberal government to repeal section of Criminal Code on anal intercourse https://t.co/qkfD5OOeXi

OttawaCitizen
Liberals to repeal Criminal Code section on anal sex http://ow.ly/FNIT306bVgS

hscoffield
Liberal government to repeal section of Criminal Code on anal intercourse via @smithjoanna #cdnpoli https://t.co/KfEmWTYYor

rp_browne
Ottawa rabbi wakes up this morning to a swastika and racial slur spraypainted on her front door https://t.co/l0lJ5FkMMq

CBCNews
Canada's special forces shoot first when required in Iraq conflict http://www.cbc.ca/1.3850827

davidpugliese
Canada to spend $348 million countering Russia but with Trump in charge is that money wasted? https://t.co/w4WidIDC4e

smsaideman
I have always scoffed at those who argue that NATO faces existential crisis. Not anymore http://saideman.blogspot.com/2016/11/wither-nato.html ...

CP24
WATCH: Canada's top general testifies at Commons Committee on Iraq involvement, sexual assault reform http://www.cp24.com/now

PostmediaNews
HMCS Vancouver and crew to provide aid to New Zealand town hit by earthquake

INTERNATIONAL

CP24
German police raid offices of Islamist group allegedly recruiting young people for Syrian war http://www.cp24.com/world/german-police-raid-offices-of-islamist-group-alleged-to-be-recruiting-youths-for-syria-1.3161319 ...

StewartBellNP
“Democracy is against Islam,” founder of Islamist group True Religion, banned by Germany, claimed in video. https://t.co/sn7frXQAdW

borealissaves
Minnesota judge grants light sentences to IS wannabes https://t.co/uAFksSChSb

borealissaves
So who is going to "deradicalise" these IS wannabes? https://t.co/uAFksSChSb

vicecanada
Inside Bataclan, one year after the Paris attacks: http://bit.ly/2eVPjgs

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

Today's News / Actualités
November 16, 2016 / le 16 novembre 2016
08:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 08h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Confidentialité des sources: des journalistes réclament une loi fédérale
Le premier ministre Justin Trudeau, qui s'est présenté comme un défenseur de la liberté de la presse, doit joindre la parole aux actes et légiférer afin de protéger les sources confidentielles des journalistes. C'est ce qu'ont réclamé mercredi en conférence de presse au parlement trois journalistes qui ont vu cette liberté entravée, Patrick Lagacé, Ben Makuch et Mohammed Fahmy, ainsi que le directeur exécutif de Journalistes canadiens pour la liberté d'expression (CJFE), Tom Henheffer. Ils ont exhorté le gouvernement à déposer un projet de loi pour protéger les sources, à revoir la façon dont les mandats de

surveillance sont accordés et à abroger des éléments d'une loi fédérale sur la cyberintimidation qui abaisse le seuil de la preuve requise pour l'obtention de mandats. Ils estiment aussi qu'une enquête publique fédérale s'impose afin de déterminer si la Gendarmerie royale du Canada (GRC) et le Service canadien du renseignement de sécurité (SCRS) ont épié des journalistes au cours des dernières années. On a appris en mai dernier que des enquêteurs de la GRC ont pris en filature les journalistes Joël-Denis Bellavance et Gilles Toupin, du quotidien montréalais La Presse, pendant neuf jours en août 2007. Il y a environ deux semaines, le premier ministre Trudeau et son ministre de **la Sécurité publique, Ralph Goodale**, ont affirmé qu'aucun journaliste ne faisait actuellement l'objet d'une surveillance policière. La Presse Canadienne (L'actualité)

ISIS, ISIL or something else? Declassified documents reveal struggle over what to call terrorists
When a federal bureaucrat circulated a map depicting "the Islamic State's regional spread," an email soon followed from the Foreign Affairs Department saying the document had to be changed. "We do not recognize the group as 'The Islamic State' and it is important it not be suggested that we do," read the email, which proposed amending the wording to " 'the global ambitions of ISIL' or something similar." Declassified documents released under the Access to Information Act show how Canadian officials struggled with language as they drafted a key report on terrorism in the age of the Islamic State of Iraq and the Levant. Planning for the latest annual Public Report on the Terrorist Threat to Canada began in April 2015, during the final months of the Conservative government. But the process dragged on for so long it was not released until August 2016. Part of the back-and-forth about its contents concerned how to talk about ISIL. Officials wanted to draw attention to the growth of the terrorist group but wrestled with terminology. There was discussion about whether to use the acronym ISIS or ISIL. That was followed by debate over how to describe the group's origins. The reference to al-Baghdadi as "caliph" was cut and **Public Safety Minister Ralph Goodale** wrote in the final version that because ISIL was "neither Islamic nor a state" the report would instead use the term Daesh, an Arabic acronym. The Integrated Terrorism Assessment Centre's view that the "greatest threat" to Canada, as well as its allies, "comes from individuals inspired and directed by ISIL" never made it into the final report. Nor did a Global Affairs Canada passage about how the RCMP and **Public Safety Canada** were using community engagement to "redirect" those at risk of radicalization. "The purpose of these efforts is to reduce and stop ISIL recruitment in Canada" and discourage support for the group, it said. National Post

TOP STORIES / MANCHETTES

Crown withdraws terrorism peace bond against Toronto man once accused of communicating with ISIL
A part-time Toronto security guard and business student, Abdul Aldabous came to the attention of RCMP national security investigators last April when information surfaced that he was communicating with ISIL terrorists. His online confidants allegedly included the failed Canadian suicide bomber Aaron Driver, an American killed while attempting an ISIL-linked attack in Texas, a prominent ISIL fighter in Syria, and Britain's youngest convicted terrorist. When the RCMP arrested Aldabous on a terrorism peace bond in September 2015, a search of his computer turned up materials, including the Islamic State of Iraq and the Levant handbook, reflecting his support for what a court document called "the radical jihadist cause." But following his arrest, Aldabous went to see a psychologist and began counselling under the guidance of a prominent Toronto imam, Yousuf Badat. Now, fourteen months later, federal prosecutors have ended their case against him. The peace bond was withdrawn at Toronto's Old City Hall courthouse on Tuesday because the Crown felt that, due to the measures Aldabous had taken largely on his own initiative, there were no longer grounds to fear he would engage in terrorism. National Post

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

No reports of damage after earthquake rumbles across southwestern Yukon
Seismologists have upgraded the magnitude of an earthquake that has occurred in a remote area of southwestern Yukon. Earthquakes Canada says the magnitude is now measured at 5.0, up from an earlier estimate of 4.7. It occurred at 6:25 a.m. local time and was relatively shallow at just 2.5 kilometres

underground. It was centred 100 kilometres south of the village of Haines Junction near the Alaska border, and about 180 kilometres southwest of Whitehorse. An online post from Earthquakes Canada says no reports of damage have been received. Canadian Press (660 News)

Broken rail caused Wadena, Sask. train derailment
A broken rail, caused by a defect that went unnoticed, led to a serious train derailment near Wadena, Sask.,according to findings released by the Transportation Safety Board. "The investigation determined that the train derailed when a sudden and catastrophic failure of one of the rails occurred under the train, due to the presence of an undetected defect," said a statement from the TSB on Wednesday. "Poor rail surface conditions had masked the presence of this defect and reduced the effectiveness of visual inspections and ultrasonic inspections." CBC News; 650 CKOM; Global News; StarPhoenix

Wawanesa: We could have done better in Fort McMurray
Wawanesca Insurance has admitted that it could have done things better in its response to the devastating wildfires in Fort McMurray, and will undergo a review of its response to the disaster. "I think there's a lot of learning to do on this. It's tough," Graham Haigh, Wawanesa's vice-president of business development, told CBC News. "It really does kill both us and our staff when we are not producing service at a level that we would want to for our families," he continued. Wawanesa received 4,094 claims following the disaster, it said, and has settled 74% of them. InsuranceBusiness.ca

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Broadcast Media / Médias télédiffusés:

CBC News interviewed RCMP Commissioner Bob Paulson on policing challenges in the digital world and the need for warrantless access to subscriber information. The Public Consultation on National Security was mentioned in this segment. Rough Transcript

The Commissioner of the RCMP is lobbying the Prime Minister's office for new powers to fight criminals and extremists who operate online. He says Canada is lagging behind when this comes to digital investigations. (CBC News, 7:00, 8:00, 9:00; CBC World Radio, 8:00; CBC Radio One, 8:30, 9:00; CBC Radio Two, 9:00)

Crown withdraws terrorism peace bond against Toronto man once accused of communicating with ISIL
A part-time Toronto security guard and business student, Abdul Aldabous came to the attention of RCMP national security investigators last April when information surfaced that he was communicating with ISIL terrorists. His online confidants allegedly included the failed Canadian suicide bomber Aaron Driver, an American killed while attempting an ISIL-linked attack in Texas, a prominent ISIL fighter in Syria, and Britain's youngest convicted terrorist. When the RCMP arrested Aldabous on a terrorism peace bond in September 2015, a search of his computer turned up materials, including the Islamic State of Iraq and the Levant handbook, reflecting his support for what a court document called "the radical jihadist cause." But following his arrest, Aldabous went to see a psychologist and began counselling under the guidance of a prominent Toronto imam, Yousuf Badat. Now, fourteen months later, federal prosecutors have ended their case against him. The peace bond was withdrawn at Toronto's Old City Hall courthouse on Tuesday because the Crown felt that, due to the measures Aldabous had taken largely on his own initiative, there were no longer grounds to fear he would engage in terrorism. National Post

Surveillance watchdog says C-22 not likely to be abused

The man in charge of overseeing Canada's electronics surveillance agency says there is no reason to believe the government would abuse controversial provisions in its national security committee legislation that give ministers the power to refuse to disclose requested information. "I don't see why they would do that unless they are in bad faith, and I assume that everybody is in good faith unless the contrary is proven to me," said Jean-Pierre Plouffe, commissioner of the Canadian Security Establishment. "The fears we have are seldom realized to the same extent we had thought. Yes, it is a restriction, but it is a reasonable one." Bill C-22, currently being studied at the House of Commons public safety committee, would create a nine-member committee of parliamentarians tasked with monitoring and scrutinizing the activities of all government departments and agencies that engage in national security activities. While it would bring Canada up to speed among the Five Eyes intelligence allies (we are currently the only one without such a committee), opposition critics have raised red flags over several key components of the bill. First, the legislation would allow the government to appoint a chair of the committee as well as all of its members rather than allowing parliamentarians to vote to confirm them or allow committee members to elect their own chair. Second, the bill contains what some national security experts have dubbed "potential Mack truck exemptions" when it comes to giving ministers the power to refuse to disclose information the committee has requested. Third, it requires the committee to submit any reports it produces to the prime minister for vetting and requires that the committee scrub the report for issues the prime minister flags as potentially jeopardizing national security before the report can be presented to Parliament. Ian McPhail, chair of the RCMP's Civilian Review and Complaints Commission, was also at the committee and stressed the need for a continued discussion around the balance of privacy and civil liberties, and suggested the committee can play a leading role in leading that conversation for Canadians. "There is a constant tension between our commitment to civil liberties but also to the protection of Canadians in terms of national security issues," he said. "Exactly how that balance should be reached I would see as being one of the key purposes of this committee because the review bodies aren't able to perform that function. The committee, provided there's not undue partisanship, should be able to do so." The committee is working to complete hearings and move to clause-by-clause consideration by November 23. iPolitics

Le juge Jacques Chamberland présidera la Commission d'enquête sur la surveillance des journalistes

C'est le juge Jacques Chamberland, qui a fait carrière à la Cour d'appel, qui présidera la commission d'enquête chargée de lever le voile sur l'écoute policière des journalistes. L'exercice devrait durer un an, selon le mandat qui sera dévoilé aujourd'hui, a appris La Presse. Le nom de Jacques Chamberland avait été évoqué il y a quelques années pour la Cour suprême, il avait aussi été pressenti comme juge en chef de la Cour d'appel. Cette nomination sera saluée par le monde juridique. Il est passablement connu à Québec ; il était passé directement du cabinet Lavery, de Billy au poste de sous-ministre à la Justice sous le gouvernement Bourassa en 1988 - Herbert Marx était alors ministre de la Justice et procureur général. Premier haut fonctionnaire nommé à forfait, son atterrissage avait soulevé un peu de controverse. La Presse

Surveillance chill on writers and journalists Canada

A new survey of some 129 writers and journalists in Canada showed many were concerned about government, police, and corporate surveillance of their work and habits. Many said that changed what they wrote and how they did research, in other words, self-censoring their work. The survey was conducted by the Centre for Free Expression at Ryerson University, in collaboration with PEN Canada and the Canadian Association of Journalists. It showed that about a quarter of writers and journalists reported that they avoid writing about certain topics because of government and corporate surveillance. A fifth said they refrain from conducting internet searches or visiting web sites on topics that may be considered controversial or suspicious. Canada's top police officer is now lobbying the government for more power to access digital data saying they are being blocked in important investigations. Radio Canada International

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Canadian businesses must lobby U.S. to fight protectionism, diplomat says

Douglas George, consul-general in Detroit, says government does not expect 'protectionism and anti-trade sentiment' from U.S. to wane that do business across the Canadian-U.S. border must fight back against American protectionism by lobbying president-elect Donald Trump's White House, one of Canada's top diplomats says. Douglas George, consul-general in Detroit, told the Canadian Council for Public Private Partnerships conference in Toronto on Tuesday that the federal government will work with business to keep the lines of trade open."Protectionism and anti-trade sentiment have been pervasive throughout the election cycle, and we do not anticipate this sentiment will wane as we move forward," he said. (…) Still, Mr. George sounded a note of optimism, arguing that Mr. Trump's election will not destroy the bond between Canada and its largest trading partner. "Yes, there are going to be bumps along the road, but [Canada's ambassador to the United States, David MacNaughton] does not see the fundamentals of our relationship changing," he said. Globe and Mail

Trump team flags Canadian livestock and lumber as targets in NAFTA reset
Transition team memo obtained by CNN points to looming 'aggressive, protectionist approach' by U.S. president-elect, Canadian Chamber of Commerce head says. Canada's softwood lumber and livestock producers are being targeted by Donald Trump's transition team, which is advising the president-elect to extract terms more favourable to the United States in these areas in a renegotiation of the North American free-trade agreement. The head of Canada's largest business group says a transition team memo obtained by CNN suggests Washington is about to embark on an "aggressive, protectionist approach to trade both with Mexico and with Canada." Perrin Beatty, president of the Canadian Chamber of Commerce, said statements Mr. Trump made during the campaign suggest every aspect of Canada-U.S. trade is up for negotiation. Globe and Mail

In Ottawa, TPP's death could open the door to transparent trade dealing
Trade deal talks that take place behind closed doors with little public consultation or review foster a culture of mistrust. Donald Trump's surprise presidential election victory promises to result in an overhaul of U.S. trade policy, including the immediate end of support for the Trans-Pacific Partnership, the controversial trade pact involving 12 Pacific countries, including Canada, the United States and Japan. (…) Their ambivalence was not a function of trade skepticism - the Liberals emerged as enthusiastic backers of the Comprehensive Economic and Trade Agreement (CETA) between Canada and the European Union - but rather stems from the recognition that Canadian interests in the TPP were largely defensive in nature. With agreements already in place with many TPP countries, the agreement offered at best limited benefits for Canada's economy. Globe and Mail

'The American dream moved to Canada': One of Donald Trump's speechwriters sees Canada as a beacon
An opinion piece states, "For millions of Canadians aghast at the election of Donald Trump, the American voters' choice of their next president seemed not just astounding, but entirely foreign-perhaps comfortingly so. While federal Conservative leadership aspirant Kelly Leitch might talk in a Trump-like vein about subjecting would-be immigrants to some sort of values test, she is easily dismissed as an outlier. Our more traditional, well-mannered Tories would never, Canadians might reassure themselves, slide toward the U.S. president-elect's angry brand of right-wing populism. (…)He concludes that a major factor explaining the difference is Canadian immigration policy. Starting in 1962, federal policy emphasized accepting immigrants based on their skills, and in 1967 a "point system" was introduced that rated would-be immigrants on factors including education, occupational skills, employment prospects, age and proficiency in English and French. To this day, Canada accepts a far larger proportion of immigrants than the U.S. does based on the likelihood that they will succeed economically. Buckley calls it "a system Donald Trump would love." Macleans

What happens when the walls go up: Trump has promised to tear up trade deals. How will an open economy like Canada cope?
An opinion piece states, "It's often said, in reference to the economy, that when the U.S. sneezes, Canada catches a cold. Well, in the words of Samantha Bee, the sharp-tongued comedian and former Daily Show correspondent (and Hillary Clinton supporter), U.S. voters "just hoicked up a marmalade hairball." (…) That's obviously not great for Canada, a self-described "trading nation" and a NAFTA member alongside Mexico. More than 75 per cent of our exports head to the United States. Complex

products like automobiles are effectively manufactured in both countries simultaneously, with engine parts and upholstered interior pieces whisked back and forth across the border by trailer truck. No wonder, then, Prime Minister Trudeau last week struck a conciliatory tone by saying "if the Americans want to talk about NAFTA, I'm more than happy to talk about it." (…) "The supply chains that run through Canada, the U.S. and Mexico are unbelievably intricate," Wolf says. "The auto industry is probably the best example. A spider couldn't weave a more interesting web. Look at the Ambassador Bridge in Windsor and how much stuff is moving back and forth." Macleans

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Tips on protecting devices from hackers
Billions of fitness trackers, medical implants, surveillance cameras, home appliances, thermostats, baby monitors and computers in automobiles now are connected as part of a rapidly expanding "internet of things." But many such devices were developed without security considerations. As a result, they are prime targets for hackers. Tips to protect your devices: Associated Press (St. John's Telegram)

Prediction: The Internet Will Get Shut Down Many More Times in 2017
It is a great irony that a system designed to withstand nuclear war falls so easily victim to a stampede of beeping baby monitors and webcams. We're talking about the Internet, of course. In October a number of top websites—Twitter, Amazon, Spotify, and more—were knocked offline when a sprawling botnet attacked New Hampshire-based Dyn DNS, a firm that serves as an Internet switchboard. An army of hijacked Internet of Things devices swarmed this choke point with overwhelming traffic. The result? A massive Internet outage. Now, far from being fixed, the problem compounds each time an unsecured device—surveillance cameras, toasters, and other home appliances—rolls off the production line with a weak default password. With billions of connected "things" entering the grid, it's open season for hackers. Fortune (2016-11-15); Infosecurity Magazine

The Web-Shaking Mirai Botnet Is Splintering—But Also Evolving
Over the last few weeks, a series of powerful hacker attacks powered by the malware known as Mirai have used botnets created of internet-connected devices to clobber targets ranging from the internet backbone company Dyn to the French internet service provider OVH. And just when it seemed that Mirai might be losing steam, new evidence shows that it's still dangerous—and even evolving. Researchers following Mirai say that while the number of daily assaults dipped briefly, they're now observing development in the Mirai malware itself that seems designed to allow it to infect more of the vulnerable routers, DVRs and other internet-of-things (IoT) gadgets it's hijacked to power its streams of malicious traffic. That progression could actually increase the total population available to the botnet, they warn, potentially giving it more total compute power to draw on. Wired (2016-11-15)

LAW ENFORCEMENT / APPLICATION DE LA LOI

Sask. Mounties on the hunt for police impersonators
The Mounties are looking for two people accused of impersonating police officers several weeks ago in east-central Saskatchewan. Two people were spotted outside a rural home in the rural municipality of Bjorkdale, about 180 kilometres southeast of Prince Albert, on Sept. 27. They had allegedly gone into somebody's vehicle when they were confronted by the owner of the property. The man and woman identified themselves as police officers. They were wearing clothing that may have been intended to look like an RCMP uniform. For instance, both were wearing pants with yellow stripes down the side, according to witnesses. CBC News; 650 News

Perquisition à Trois-Rivières: un réseau international de fraude démantelé
C'est un réseau international de fraudes qui a été démantelé mardi, un peu partout dans le monde, menant notamment à une perquisition sur le boulevard Saint-Michel à Trois-Rivières. La centrale d'information policière Europol a révélé mercredi matin que le réseau recrutait notamment des mineurs pour parvenir à ses fins. Au total, 15 personnes ont été arrêtées au cours de perquisitions qui ont eu lieu

simultanément au Canada, en Finlande, en Espagne et au Royaume-Uni. Pour le moment, nous ne savons pas si des personnes mineures ont été arrêtées à Trois-Rivières ou si la résidence visée faisait seulement l'objet d'un mandat de perquisition. Rappelons qu'une autre opération de même nature a aussi eu lieu à Longueuil, mardi. (…) La GRC, qui a participé aux perquisitions au Canada à la demande d'Europol, devrait faire le point un peu plus tard mercredi sur les opérations menées à Trois-Rivières et sur le niveau d'implication des personnes visées par les mandats dans la région. Le Nouvelliste

Les Soldats d'Odin, groupe anti immigration, anti réfugiés, sont maintenant présents au Yukon
Si, sur la scène internationale, le Canada reçoit des éloges pour son ouverture aux réfugiés – le secrétaire général des Nations unies, Ban Ki-moon a même fait l'éloge du Canada en ce sens – voilà que des groupes qui sont contre cette politique canadienne voient le jour un peu partout au pays. Selon la page Facebook du groupe et selon la Gendarmerie royale canadienne, l'organisation « The Soldiers of Odin » est un regroupement de personnes résolument anti immigration – en anglais, les termes utilisés sont « extreme anti-refugee vigilante organization. » On s'attendrait à voir surgir des groupuscules du genre dans les grandes villes, là où l'immigration est la plus présente, mais, au Yukon? En effet, la police fédérale canadienne affirme qu'un tel groupe a été constitué à Yellowknife, capitale du territoire nordique du Yukon. Radio-Canada International

Nunavut RCMP must learn better ways of handling the mentally ill, jury says
The jury that sat on a coroner's inquest into the 2012 death of a Nunavut man with serious mental health issues says the RCMP must find non-violent ways of dealing with people who are mentally ill. The six-member jury in Igloolik heard testimony about the death of Felix Taqqaugaq Nov. 1 to Nov. 10 from about 30 witnesses. Taqqaugaq died March 20, 2012, when an Igloolik RCMP officer shot him three times in the chest. "The [Government of Nunavut's] and the RCMP's goal must be zero shooting deaths for incidents where police interact with individuals with mental illness," one recommendation said. The inquest, which was mandatory because Taqqaugaq died at the hands of police, does not assign responsibility. Nunatsiaq Online

Did Canada's failure to fix policing problems in the North lead to the death Lena Anderson?
On a cold night in Feburary 2013, Lena Anderson tied the drawstring from her pants to a bar in the back of a police truck and hanged herself. Anderson was 23, and a mother. An inquest into the circumstances of her death wrapped up in Thunder Bay, Ont., with 28 recommendations to prevent her tragic death from happening again. A jury of five heard five days of testimony from 12 witnesses, including how Anderson was handcuffed and detained in the back of a Nishnawbe-Aski Police Service (NAPS) truck on Feb. 1, 2013. The police officer on-duty in the First Nations community Kasabonika left Anderson alone in the truck for 16 minutes. Anderson had been struggling with the recent suicides of two loved ones when she died. APTN (2016-11-15)

Kelowna could soon have new top cop
Kelowna is closer to getting a new police chief. The search for a new superintendent began in late September following the sudden resignation of Kelowna's former top cop, Nick Romanchuk. Kelowna Mayor, Colin Basran, said they've whittled the list down to a few candidates. "I believe the shortlist is four. They will all be coming to Kelowna for interviews with RCMP officials and City of Kelowna officials. Afterwards, a decision will be made jointly between the RCMP and the City of Kelowna as to who the new superintendent will be," said Basran. Global News

Rotary Fundraiser Luncheon Focuses On D.A.R.E. Program
The annual South Eastman Rotary fundraiser luncheon for the RCMP Drug Awareness Resistance Education program was held at the Mennonite Heritage Village on Tuesday. Rotary Club President Corny Petkau says when the club was founded in the Southeast they were looking for a good cause to support. He notes the RCMP D.A.R.E. program was a perfect fit for the Rotary Club. "Sometimes you wonder when you are phoning people and asking for funds if it is worth it or not but every time it is done and when we see the results in the kids, the teachers show us what the kids have learned, it is very well worth it and it is a big honour to be involved with that." Steinbach Online

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

No new trial for roommate torturer Dustin Paxton: Alberta Court of Appeal
Convicted roommate torturer, Dustin Paxton's aggravated and sexual assault convictions have been upheld by the Alberta Court of Appeal. The Alberta Court of Appeal released its decision on Wednesday, one month after hearing arguments from Paxton's lawyers and Crown prosecutors. In 2010, Paxton dropped off his victim at a Regina hospital weighing just 87 pounds, disfigured from daily beatings and with permanent brain damage. Paxton, 36, was deemed a dangerous offender and handed an indeterminate sentence in 2012 after being convicted of assaulting his victim and business partner over an 18-month period. CBC News; Canadian Press (Metro News, Global News, News1130, Chronicle Journal)

Man who assaulted teen gets early parole
A man who sexually assaulted an intellectually challenged teen has received day parole 16 months into his five-year sentence. Anthony Leo Gough, 50, of Middle Sackville, pled guilty in July 2015 to the sexual exploitation of a girl he was responsible for at the Social Opportunities and Recreation Society day camp. In a Parole Board of Canada decision, Gough was put on day parole in a community-based residential facility for a six-month term. He was ordered to avoid children and his victim and her family. The board said letters of support from Gough's family had come in, although he did not write on his own behalf. Chronicle Herald, A3

How to Prepare for Prison: Start by cutting your hair
Courtney Hills stole $950,000 from her employer in Calgary and pleaded guilty. As she waits to be sentenced, she meets with a prison consultant, Lee Chapelle, who spent 21 years behind bars. (According to this doc from director Matt Gallagher, rising incarceration rates in North America have turned prison consultancy into a cottage industry.) "So, haircut tomorrow," Lee says to Courtney, who is 20-something, with long hair. "We know why we do this: manageability, potential lockdown, lack of shower time, plus eliminate any chance of somebody being able to use it physically against you, grabbing your hair." In an interview for the camera, Lee explains, "Prison changes people. You put on a mask to survive. You don't cry, you don't smile. As time passes, this is no longer an act. This becomes the person." "I have to become someone I'm not but not lose the person I was," Courtney says. (…) Despite its promising title, this is film is not that. Instead, it decries a system that sends non-violent offenders to prison and then, somewhat cruelly, tries to manufacture suspense about what kind of sentence Courtney and two other accused criminals might get. It should have been called, *I Wish Someone Had Scared Me Straight, But Now It's Too Late*. The documentary *How to Prepare for Prison* aired on TVO Nov. 16. Toronto Star

Sex offender's library access under appeal
Is a public library a community centre? That's one of the issues judges of the province's top court will ponder as they decide whether or not an order that prohibited a Regina pedophile from attending community centres also extends to the Regina Public Library (RPL). The Crown is appealing a lower court decision that acquitted Robert Keith Allaby, 53, of breaching that prohibition order. But Allaby's lawyer says his client was specifically ordered to stay away from "community centres" - not "libraries" - and he so complied. The Saskatchewan Court of Appeal reserved decision after hearing arguments Tuesday. If the Crown's appeal is successful, it wants Allaby tried again. (…) The National Parole Board, which revoked his parole in March 2010, subsequently added a parole condition that expressly forbid him from entering libraries. However, when Allaby moved to Regina in 2014, he was no longer on parole, so wasn't bound by that condition. However, the lifetime prohibition order remains. Leader-Post, A2

Stuck in solitary
A letter to the editor states, "I am more than disgusted by the facts revealed in "1,560 days" (National, Nov. 14) about the treatment of Adam Capay in our prison system, and the excessive use of solitary confinement. How can we be doing this? We wouldn't treat dogs this way! It is reprehensible that the people responsible for this (who seem to all be passing the buck) are not being removed from their positions immediately. How can we call ourselves a progressive and humane country when this kind of thing is occurring? What we are doing is torture, plain and simple!" Macleans

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Intoxication aux opioïdes : 13 Canadiens hospitalisés chaque jour
Le Canada traverse une crise de santé publique en raison de la hausse des préjudices associés aux opioïdes, conclut un nouveau rapport de l'Institut canadien d'information sur la santé (ICIS) et du Centre canadien de lutte contre les toxicomanies (CCLT). Selon le rapport *Hospitalisations et visites au service d'urgence liées à une intoxication aux opioïdes au Canada*, à l'échelle du pays, le nombre d'hospitalisations du genre a augmenté de plus de 30 % entre 2007 et 2015, tandis que les intoxications aux opioïdes entraînent plus de 13 hospitalisations par jour. Les taux de préjudices liés aux opiacés sont plus élevés dans l'ouest du pays, souligne le rapport, notamment en Saskatchewan (20,5 hospitalisations pour 100 000 habitants), en Colombie-Britannique (19,1 hospitalisations pour 100 000 habitants) et en Alberta (18,6 hospitalisations pour 100 000 habitants). Le Québec était la province avec le plus faible taux d'hospitalisations (9,7 préjudices pour 100 000 habitants), et ce, tout au long de la durée de l'étude. Alors que le taux d'hospitalisations liées à une intoxication aux opioïdes a augmenté parmi tous les groupes d'âges, les jeunes de 15 à 24 ans ont affiché le changement le plus marqué, soit une hausse de 62 % par rapport à 2007-2008. Il s'agit également de la tranche d'âge où les intoxications sont majoritairement le résultat d'un geste intentionnel (52 %). Radio-Canada ; CBC News; StarPhoenix; Vancouver Sun

Ottawa would've taken 'greater action' if opioid crisis struck Ontario as it has B.C.: Terry Lake
Would the federal government have taken quicker action if the opioid crisis had struck Ontario with the same magnitude as British Columbia? That's what B.C.'s Health Minister thinks. Speaking from Ottawa at a joint provincial-federal opioid conference, B.C. Health Minister Terry Lake says Ottawa needs to increase RCMP resources, ban pill presses, repeal Bill C2 and establish national surveillance of overdoses. "I don't think it's hit Ontario the way it's hit British Columbia, if it had I think we would see much greater federal action and so we are really pushing the federal government to take greater action than they have to date." He says Ottawa needs to amend legislation and increase resources to tackle the overdose epidemic. "We need more RCMP resources, we need legislation banning pill presses, we need the repeal of Bill C2 which prevents us from setting up safe consumption sites where they are needed, and we need national surveillance of opioid overdoses." CKNW

Hospital stays for opioid overdoses on the rise, warn health researchers
Slow breathing. A lack of oxygen. Blue discoloration. For Ottawa paramedic JP Trottier, the telltale symptoms of an opioid overdose are becoming all too common. "Our paramedics find the patient hypoxic, blue in colour ... they're breathing at four or six breaths a minute, certainly not enough to maintain life," said Trottier. This year Ottawa is on pace to see twice as many opioid-related 911 calls as the previous year, Trottier said. And they aren't the only emergency responders seeing a spike in recent years, if a study published Wednesday is any indication. The rate of opioid overdoses requiring hospitalization is on the rise in nearly every province, according to a new national study by the Canadian Centre on Substance Abuse and the Canadian Institute for Health Information. (...) Seniors age 65 and older had the highest rate of hospitalization, at 20 per 100,000 people, with the most common cause being "accidental" overdoses, due to confusion or misunderstanding about how to take prescribed drugs. The next biggest age group was youth, age 15 to 24. They were hospitalized at a rate of 10 per 100,000, with more than 50 per cent of the cases categorized as "intentional," meaning the person admitted to using the drug to "self-harm." But young people also had the biggest increase in hospital stays as a result of opioid poisoning, up 62 per cent compared with 2007-08. CBC News

Opioid crisis growing here, paramedics warn
Winnipeg paramedics are rushing to more homes where partygoers are daring death by using opioids such as fentanyl. The first report to examine Canada's growing epidemic of the use of synthetic narcotics such as fentanyl was released today, but city paramedics said they don't need statistics - they have seen overdose scenarios that shock veterans of the job. "From a front-line paramedic side, the calls with fentanyl and carfentanil, you don't know who your patients are. You have to assess everyone," said Ryan

Woiden, local 911 paramedics union president. "You walk into a house party and everyone has sunken eyes. They're all very pale, they're all nodding off, walking slowly, talking slowly and you don't know how many patients there are. "When I started, or even a year ago, you'd walk into a house party and there'd be boozing, loud music, someone getting sick in a corner, and you'd know who your patient was," Woiden said. He said he's gone to suburban house parties, including ones with young adults headed out for a night of clubbing. They start off with drugs such as fentanyl or carfentanil, to get a buzz on, not realizing the dangers or knowing what the drugs are. The stronger the buzz, the more deadly it is, Woiden warned. "This is no party drug. This drug will kill you. This drug is going to depress your breathing until you stop breathing," he said. Winnipeg Free Press, 1

VPD issue warning following string of drug overdoses
Vancouver police have issued another warning after 11 overdoses were reported in a single day in the city's Downtown Eastside. The move prompted the province's opposition party to call for more help for addicts and underscored the danger facing drug users ahead of a federal conference on the opioid crisis.Police issued the warning after a series of non-fatal overdoses on Monday, echoing previous notices from police and health officials, who have urged users not to inject when they are alone and to watch for overdose symptoms. Meanwhile, the city's supervised injection site saw 28 overdoses on Monday - none fatal. Federal Health Minister Jane Philpott will host a conference this weekend in Ottawa to discuss a crisis that has killed hundreds in British Columbia alone and resulted in thousands of overdoses, taxing police, fire and emergency health departments. Globe and Mail, S1

Estevan receives funding for officers
The Estevan Police Service (EPS) has received $330,000 in provincial funding for three police officer positions. Police Chief Paul Ladouceur said the money will support EPS community liaison officer Const. Danielle Stephany, as well as their drug and intelligence officer position and one of the EPS officers who are part of the Estevan Combined Traffic Services unit. Estevan Mercury

Police seek $1.2M increase for 2017 budget
City police will ask for a $1.2 million increase to its 2017 operating budget. Thunder Bay city council approved a $39 million 2016 budget for the Thunder Bay Police Service, but the force was unable to work within that budget and are projecing a shortfall of nearly $815,000 for the year, which is about two per cent of its total budget. During the Thunder Bay Police Services Board meeting Tuesday, Chief J.P. Levesque stated that they need more money to cover the increasing legal fees, which he believes will help alleviate the pressures it has felt over the past few years. TB News Watch (2016-11-15)

Halifax sees upswing in homicides
Homicides in Halifax are trending upward again, according to information from Statistics Canada and the Halifax Regional Police. On Tuesday evening, police confirmed Terrance Patrick Izzard, 58, was the city's latest homicide victim. His death brings the total number of homicides in Halifax this year to 11. That's already two more than last year and six more killings than the city saw in 2014. While it's an upward swing, its not a record for the region. According to Statistics Canada, 18 people were killed here in 2011. Former Saint Mary's University president Owen Carrigan sat on both the provincial and municipal task forces on crime and violence in the province. He says it's not possible to know whether the numbers are a new normal or an outlier. A comparison with Canada's national homicide rate between 2006 and 2014, also doesn't put Halifax in a favourable light. Statistics Canada's numbers show that the rate of homicides per 100,000 people in Canada in that period, varied between one and two homicides. Halifax has spent time above and below the national rate. Its highest rate was in 2011 with more than four homicides per 100,000 people. The lowest rate in that period was just over one homicide per 100,000 people in 2014. Global News (2016-11-15)

Bernstein: We asked the Ottawa police for crime stats, but the data are unreliable
An opinion piece states, "Ottawa has experienced a wave of media headlines profiling multiple violent crimes in our downtown core in recent weeks. Based on these stories alone, one might think Ottawa is a dangerous place to live. The reality is that our communities have no clear picture of the crime problem. Where knowledge and evidence should inform action, there is a frustrating lack of reliable data from the city and the Ottawa Police Service regarding crime rates in our neighbourhoods. Ottawa can do better.

The Police Services Board is meeting at the end of the month to review the 2017 departmental budget. They have an opportunity to increase funding of the police service's data capacity, in order to produce better information to direct policing action and to make reliable neighbourhood crime data available to the public. (…) Our search for reliable crime data initially brought us to the ByWard Market Safety and Security Committee and Crime Prevention Ottawa, neither of which had access to data on actual crime rates in our neighbourhood. We then turned to the most logical place for crime numbers – the police. The Ottawa Police Service directed us to two data collections available on their website; both are seriously flawed. The Crime Mapping Tool shows police calls-for-service from the public and displays them on a city map for the previous 15 days. The tool itself is preceded by a page of disclaimers explaining why the data is unreliable. The section of the map covering Lowertown is always crowded with icons, making the area look like a hotbed of crime. However, many of the calls-for-service are reported more than once, and some turn out to be of insufficient severity to actually open a police file. " Ottawa Citizen

Broadcast Media / Médias télédiffusés:

A new report from the Canadian Institute for Health Information says this country is facing a public health crisis over opioids. It says 13 Canadians are hospitalized every day for opioid poisoning. And here's a fact that may surprise you: the majority of them are seniors. (CBC News, 10:20EST)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

B.C. limits on federal probe vex advocates
The B.C. government has issued an orderin-council that some legal advocates fear places new restrictions on the national inquiry into missing and murdered indigenous women. Attorney General Suzanne Anton said the order-in-council confirms the province's support for the inquiry by giving commissioners the power to examine relevant matters within B.C. "It gives them the authority that a provincial commission of inquiry would have," she said. But West Coast Women's Legal Education and Action Fund and the B.C. Civil Liberties Association both expressed concern Tuesday that the B.C. order comes with conditions attached. "I'm happy that they've committed to participating," said Kasari Govender, executive director of West Coast LEAF. "I'm less happy about the additional restrictions they placed on the terms of reference." She said the federal terms of reference already made clear that the inquiry will not reopen specific cases. The B.C. government's additional terms go beyond that by indicating that the commission "may not inquire into any matter respecting the exercise of prosecutorial discretion," she said. Times Colonist, A4

L'Assemblée des Premières Nations accuse Couillard de se trainer les pieds
Le PQ ainsi que l'Assemblée des Premières Nations du Québec et du Labarador (APNQL) réclament une enquête indépendante sur le sort réservé aux femmes autochtones. L'APNQL souhaite cependant que le mandat de cette enquête soit élargi à « tous les aspects des relations entre les services policiers et les Premières Nations ». « Le gouvernement Couillard refuse de faire face à ses responsabilités, la majorité des services policiers étant sous son autorité, a déclaré le chef de l'APNQL, Ghislain Picard. [Le gouvernement Couillard] a plutôt choisi de se cacher derrière l'enquête policière menée par le SPVM. » (…) L'APNQL accuse le gouvernement du premier ministre Philippe Couillard de gagner du temps au détriment des femmes autochtones. « Il [le gouvernement] souhaite également attendre […] les résultats de l'enquête déclenchée par le gouvernement fédéral sur les femmes et les filles autochtones disparues ou assassinées, soit dans deux ou trois ans! » Radio-Canada; CBC News; 98.5FM; Presse canadienne (La Presse)

BC Liberals reach into aboriginal governance ranks for northwestern B.C. candidate
The BC Liberals, for the second time, have reached into the ranks of northwest aboriginal governance for a candidate for next May's provincial election. Wanda Good, the deputy chief councillor for Gitanyow, located north of Gitwangak on Hwy37 North, has been selected as the party's candidate for the Stikine

riding. In a release Good said she was honoured to be a BC Liberal candidate. "Working in collaboration with the province, municipalities, and First Nations, I have been able to bring positive change to northwest BC. Now, I'm ready to step up and be a strong voice in Victoria for the Stikine riding, which has been underrepresented in government for too long," she said in the statement. (…) Good's also been very active in the cause of missing and murdered women along Hwy16 – a cousin, Lana Derrick, a 19-year-old college student, was last seen in Thornhill in the fall of 1995. Terrace Standard

Quebec needs an inquiry into Indigenous/police relations
An opinion piece states, "Quebec crown prosecutors won't be laying charges in 37 abuse complaints by Indigenous women against six Sûreté du Québec police officers in Val d'Or. Stop me if you've heard this one, or something similar, when it comes to a) complaints against police; b) complaints by Indigenous women; c) complaints by women who say they've been sexually assaulted. (…) The Couillard government and native affairs minister Geoff Kelley have tried to sideline the demand by palming it off on the federal government inquiry into Missing and Murdered Indigenous Women, but chief Ghislain Picard, leader of the Assembly of the First Nations of Quebec and Labrador, told *Le Devoir* this week that "we will continue to ask for an investigation. "There is nothing that prevents the government from carrying out an inquiry that is specific to Quebec, even as it feeds into the national inquiry." Quebec, he added, was trying to find comfort by hiding behind the MMIW probe. Indeed, although the mandate of the MMIW will no doubt lead it to examine the role of police in investigating the deaths and disappearances of anywhere from 1,200 to 4,000 First Nations women, a Quebec commission would have a much broader mandate." Cult Montreal

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Medical marijuana user warns about cannabinoid hyperemesis syndrome
Halifax woman say she vomited 'all day long' for eight months until specialist made diagnosis. A Halifax woman says she threw up "all day long" for eight months straight — and her medical marijuana is to blame. It wasn't until a specialist diagnosed Dawn Rae Downton with cannabinoid hyperemesis syndrome, and she stopped taking marijuana entirely, that she says the vomiting finally ended." Vomiting and just a complete malaise, I was bedridden most of the time," she said of the period she took marijuana. The condition, which was first documented in 2004 and has not been widely researched, is characterized by cyclical bouts of nausea, vomiting and gastrointestinal discomfort, said Toronto family doctor Peter Lin. If it occurs often enough, it can lead to things like weight loss, dehydration, and vomiting blood, said Lin, who is also a health columnist for CBC. CBC News

Major Businesses That May Benefit After Canada Legalizes Recreational Marijuana
In October 2015, Canadians elected the Liberal Party of Canada and their leader, Justin Trudeau, as the majority government and Prime Minister, respectively. A campaign promise of Prime Minister Trudeau was to legalize and regulate the use of recreational marijuana in Canada. Medical marijuana was and still is legal in Canada nationwide (with the proper prescription). Unlike the United States, Canada's Criminal Code is federal legislation. (…) Papa John's owns a lot of joint-venture stores in four states, including Colorado. So while we cannot get Colorado-specific numbers from the filing, we can look at how that group of four states did after marijuana legalization and compare it to the company as a whole. In the company's 10-K for the year ended December 28, 2014, the company gave a breakdown of its joint venture stores in four regions, including Colorado. Seeking Alpha

Marijuana stocks trading halted on TSX after massive jumps of up to 44% trip circuit breaker
Stock trading for several Canadian marijuana companies was halted briefly this morning, following massive increases in value in high volume trading. Canada's publicly-traded marijuana companies, including Aphria Inc., Mettrum Health Corp., Organigram Holdings Inc., Supreme Pharmaceuticals Inc., Aurora Cannabis Inc. and Canopy Growth Corp. were all halted for five-minute intervals before 11 a.m. Wednesday morning. The Investment Industry Regulatory Organization of Canada issued halt and resumption notices, giving the reasoning "single stock circuit breaker," for each. Circuit breaks can be triggered when a stock climbs at least 10 per cent in a five-minute period, which appears to be the case with the six marijuana stocks Wednesday. "IIROC can make a decision to impose a temporary

suspension (halt) of trading in a security of a publicly-listed company. Trading halts are implemented to ensure a fair and orderly market," the statements read. Vancouver Sun

Medical marijuana clinic sets its sights on a Rupert office
A medical marijuana company wants to plant seeds in Prince Rupert by opening a clinic by the end of the year. The Medicinal Cannabis Resource Centre Inc. (MCRCI) has been in business for six years and has clinics in Vancouver, Kamloops, Kelowna and Winnipeg. A physician-based medical marijuana clinic would be the first of its kind in the city, and will offer its service to surrounding communities including Haida Gwaii and Terrace. The company set its sights on Prince Rupert after opening the clinic in Winnipeg, said Ron Bell, director of business development for MCRCI. "We got involved in some of the issues around Indigenous peoples, smaller communities and under-serviced areas," he said. When they began to consider northern B.C. as their next site, they found a physician in Prince Rupert who was willing to work with them. Northern News

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Canadian peacekeepers to Mali: deadly possibility
After the previous Conservative government scaled back Canada's peacekeeping missions, the current Liberal government subsequently announced a new commitment to international peacekeeping. In addition to contributing millions of dollars to UN peacekeeping, the announcement indicated Canada would commit some 600 soldiers and additional police to a United Nations mission in Africa. All signs seem to point to a mission to Mali where the Canadian defence minister visited this month and where a Canadian reconnaissance team also visited earlier. That country has been in a state of war and conflict for the past five years, with terrorists and rebel factions having killed some 100 UN peacekeepers since 2013, after French and Mali forces pushed back against radical Muslim forces which had taken over a large area of northern Mali. Some 30 peacekeepers have been killed this year alone. Radio Canada International

INTERNATIONAL

German court rejects opposition's bid for disclosure of NSA spy targets
Germany's highest court has rejected a bid by opposition politicians to make the government disclose spy targets it worked on with the U.S. NSA spy agency to a parliamentary commission investigating the NSA's activities in Germany. Germany began an investigation after news in 2015 that the Bundesnachrichtendienst (BND) foreign intelligence agency had helped the NSA spy on many European companies and politicians. German politicians and other critics also argue that a law passed in October after NSA whistleblower Edward Snowden's disclosures about U.S. spying on Chancellor Angela Merkel, will make oversight of the BND harder. The government says it will do exactly the opposite. Reuters; Deutsche Welle (2016-11-15)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

BCSARA
Update on Announced Funding for SAR in BC http://www.bcsara.com/2016/11/update-on-announced-funding-for-sar-in-bc/ ....

Nova Scotia EMO
Storm surge warnings in place for Digby & Yarmouth counties. Higher than normal water levels & large waves expected. http://weather.gc.ca/warnings/index_e.html ...

Naomi Yamamoto
Free Disaster Response Workshop. Nov 16, 7-9:30pm @NorthShoreEMO @CityOfNorthVan http://bit.ly/2fQLK9k #beprepared

IBC West
#FortMcMurray #ymmfire #wildfire recovery to spur $5.3B in spending: report http://herald.ca/ubC#.WCyMRGXBCI0.twitter ... via @chronicleherald @ibickis @WBEcDev

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Christopher Parsons
AND Canada's is currently having a national security consult ON EACH OF THESE POINTS. How can CBC/RCMP claim 'conversation' not happening?!

The Muslim Lawyer
Less than a month left to provide your input. Canadians should worry more about Bill C51 than Trump. Please...

NATIONAL SECURITY / SÉCURITÉ NATIONALE

CBC News
RCMP Commissioner Bob Paulson 'consumed' with 'inability' to investigate in digital world http://www.cbc.ca/1.3851955

CBC Nova Scotia
RCMP Commissioner Bob Paulson 'consumed' with 'inability' to investigate in digital world

Christopher Parsons
Pleading the Case: How the RCMP Fails to Justify Calls for New Investigatory Powers christopher-parsons.com/pleading-the-c...

Christopher Parsons
I have a hard time believing that the CBC is just reproducing the RCMP's own documents, with no 3rd party analysis, as facts on the ground

Christopher Parsons
Absent in CBC/TorStar pieces is the RCMP GOT a raft of lawful access powers just a few years ago. Not everything. Now they're back for rest

PACC
The argument for/against law enforcement gaining greater investigatory powers: what's at stake christopher-parsons.com/pleading-the-c... #privacy #security

Open Media
Another privacy scandal strikes Canada: RCMP used data from police + social media to track down Aboriginal activists ow.ly/v888306eBaL

ishmael n. daro
RCMP lobbying federal government for more surveillance powers, including warrantless access to subscriber info on.thestar.com/2fg2cjj

Nora Loreto

The @TheCurrentCBC's segment on expanding arrest and surveillance powers of the RCMP is on the anniversary of the NWMP hanging Louis Riel.

Jordan Pearson
the RCMP's line hasn't changed in years. can we stop reporting it over and over and over like this. cbc.ca/news/politics/...

The Vancouver Sun
Swastika, slur spray-painted on Glebe Jewish prayer centre http://ebx.sh/2f3wh83

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

The Vancouver Sun
Has the federal government dropped the ball in preventing the import of synthetic fentanyl into B.C.? Weigh in: ow.ly/Btbw306eJqB

The Telegram
C.B.S. man arrested by Canadian Border Services on fuel theft charges https://goo.gl/4Zo72k

NTV News
Newfoundland Man Accused of Stealing 170,000 Liters of Diesel Caught by Canada Border Services - http://ntv.ca/newfoundland-man-accused-o...

CBC News
John McCallum says Mexican visa could be 'reimposed' if refugee claims spike after Trump victory cbc.ca/1.3851904

Kim Allen
Changes to Express Entry system will attract global talent to Canada https://t.co/E7jpEHB0wP

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

CTV News
Appeal denied for man who tortured, starved, assaulted his roommate ow.ly/hUWa306eEux

CP24
Appeal denied for man who tortured, starved, assaulted roommate cp24.com/news/appeal-de...

Jason Godin
Looking forward to being a guest speaker this evening with RCMP members @CanadaMPPAC to share our experiences in building UCCO-SACC-CSN

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

BC Government News
In addition to firearms & replicas, explosives & ammo were turned in during October's Amnesty, http://ow.ly/F2Z7306a78o #StopGunsGangsBC

Canadian Red Cross
Congrats to our team in Alberta for receiving the Inspiration Award for their bullying prevention work: http://bit.ly/2fgRWHv #BAW2016

Ottawa Citizen
The Lowertown Community Association wanted crime stats on their area, but couldn't get reliable data from police https://t.co/cm40veNSoK

VICE Canada
Canada is repealing its law criminalizing anal sex, but it won't pardon anyone: http://bit.ly/2eCCUzB

Nicholas Keung
Veteran York educator blasts board on racist, anti-Muslim incidents http://on.thestar.com/2ggX3M5 @njaved @krushowy @TorontoStar

Google News
Emergency department visits for opioid poisoning higher in Alberta than Ontario

Pamela Fayerman
B.C. has 2nd highest hospitalization rate for opioid painkiller poisonings, Sask. the worst: today's CIHI report. vancouversun.com/news/local-new…

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

APTN National News
"Joanne was loved. We want justice..." #MMIW #MMIWG #JoanneNeepin aptn.ca/news/?p=65950

PUBLIC SERVICE / FONCTION PUBLIQUE

TBS Canada
Thanks to everyone who sent feedback for our assessment of Canada's #OpenGov Plan 2014-16. http://ow.ly/9Lt9306epmI #OpenGovCan

Ottawa Citizen
She's caught in a firestorm of controversy

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

Today's News / Actualités
December 3, 2016 / le 3 décembre 2016
11:00 - 18:00 ET

This collection contains news items that appeared online between 11:00 a.m. and 6:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 11h00 et 18h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

L'immigration irrégulière au Canada décortiquée en 5 questions
La question des immigrants illégaux est un enjeu majeur aux États-Unis. Durant la campagne, Donald Trump a promis d'expulser les 11 millions de sans-papiers. Qu'en est-il au Canada? L'immigration irrégulière est-elle un problème?... 4. Que fait le gouvernement? Si le nombre d'expulsions a fortement diminué au cours des dernières années, il n'y a pas de raison de s'inquiéter, croit l'ASFC, qui soutient que la priorité est accordée « au renvoi des personnes qui constituent une menace pour la sécurité

nationale [en raison d'actes terroristes, de crimes de guerre ou d'atteintes aux droits humains] et des personnes qui sont impliquées dans le crime organisé ou qui ont commis des actes criminels. » Le syndicat des douaniers pense plutôt que cette baisse est le résultat des compressions budgétaires du gouvernement Harper qui ont entraîné la suppression d'un millier de postes. Jean-Pierre Fortin, président national du Syndicat des douanes et de l'immigration, soutient qu'il est pressant d'agir parce que le nombre de migrants irréguliers ira en augmentant si rien n'est fait. Le gouvernement de Justin Trudeau veut agir en amont, en diminuant le nombre de personnes qui restent au pays illégalement. **Le ministre de la Sécurité publique et de la Protection civile, Ralph Goodale**, a déposé en juin dernier un projet de loi qui vise, entre autres, à identifier les étrangers qui demeurent au Canada après l'expiration de leur visa. L'ASFC aura la tâche de recueillir « les données biographiques » de tous les voyageurs à leur sortie du Canada. ***« Lorsque le projet de loi sera adopté, le Canada saura à quel moment et à quel endroit une personne est entrée au pays, et à partir de quel moment et de quel endroit elle a quitté le pays »,*** indique le communiqué du **ministère de la Sécurité publique.** Radio Canada

TOP STORIES / MANCHETTES

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Plus de 10 000 foyers toujours privés d'électricité dans la région de Québec
Quelque 200 équipes d'Hydro-Québec s'affairent toujours à rétablir le courant pour plus de 10 000 résidences qui sont privées d'électricité dans la région de Québec, samedi, au surlendemain de la première vraie bordée de neige de l'hiver. Sur le coup de midi samedi, 10 028 clients étaient toujours privés de courant, près de 50 heures après la tempête. Le poids de la neige et les branches tombées sur les fils électriques sont à l'origine des pannes… Les secteurs de Stoneham-et-Tewkesbury, Saint-Gabriel-de-Valcartier et la MRC de Portneuf sont particulièrement touchés. Radio Canada

Sinkhole shuts down Highway 4 east of Ucluelet Junction
People living in Tofino and Ucluelet are virtually cut off from the rest of Vancouver Island due to a washout on Highway 4. The portion of the highway near Kennedy Lake, about five kilometres east of Ucluelet Junction, has been shut down since Friday afternoon. According to people in the area, the road was initially open to a single lane, alternating traffic. However a sinkhole apparently expanded and closed down the highway completely. It's believed to be more than nine metres deep. A Geotech assessment was scheduled for Saturday morning. CTV News; Canadian Press (Vancouver Sun); CBC News

STARS, emergency personnel dispatched to school bus rollover carrying 25 kids
Dr. Myron Thiessen, the Chief Medical Officer for Interlake Eastern Regional Health Authority, confirmed a school bus carrying 25 children rolled over near Matheson Island, roughly 235 kilometres north of Winnipeg. Six ground units are on the way to the scene. STARS ambulance was also dispatched. Thiessen said there are other life flight units on standby to assist if necessary. CTV News

Rescuers in northwestern B.C. search remote highway for missing U.S. man
A search was underway along a remote northwestern B.C. highway for a 70-year-old Alaska man who was last seen on the route Monday. A news release from the RCMP says family members report Tony Adevai was driving from Oregon to his home in Alaska when he disappeared… They say it's possible that Adevai was picked up by another driver, but dog teams and search volunteers are scouring the Iskut area, where Adevai's truck was found. Canadian Press (Vancouver Sun)

Nelson House teacher believed to have fallen through ice: Chief
A Nelson House teacher who has been missing since Thursday, is believed to have fallen through the ice while riding his snowmobile… Moody told CTV there are snowmobile tracks leading to a hole in the ice.

He said a local search team is ready to be deployed, but due to freezing rain and mild temperatures, they can't set out… Moody said he's waiting for an RCMP dive team out of Winnipeg to help locate MacDonald. The RCMP Underwater Recovery Team is expected to be in the community on Monday to help with the search efforts. CTV News

More than 100 people join search for missing Bryan Balong
With piles of posters and a set plan, more than 100 people took to the streets around Winnipeg searching for 33-year-old Bryan Balong. Balong has been missing since Nov. 22. His brother Brad organized the searched with the help of family and friends. "I am hopeful, everybody is here. We are just going to keep searching," Brad Balong said. CBC News; CTV News

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Le Canadien kidnappé en Libye raconte son histoire
Lorsque ses bourreaux l'ont conduit dans le désert de la Libye et lui ont dit de s'agenouiller dans le sable, le Canadien Frank Poccia croyait que ses sept semaines de captivité prenaient une fin tragique. Assis par terre et entouré d'individus armés jusqu'aux dents, M. Poccia s'est dit que la fin était proche. Il s'attendait à mourir. Mais au lieu de cela, le Canadien de 52 ans et deux autres otages italiens ont été transportés dans un autre véhicule qui s'est dirigé vers l'aéroport, où ils ont été libérés 47 jours après avoir été kidnappés par des hommes armés alors qu'ils se rendaient au travail à Ghat, en Libye. En ce moment, un mois après que le gouvernement italien eut annoncé la libération des trois hommes, M. Poccia a confié à La Presse canadienne qu'il se sentait chanceux d'avoir pu s'échapper pour retrouver sa famille à Montréal (…) Bien que plusieurs groupes terroristes rodent dans la région, M. Poccia ne croit pas qu'il avait affaire à des terroristes. Les individus fumaient, priaient rarement et n'étaient pas violents avec eux, ce qui concorde davantage avec l'hypothèse d'une organisation criminelle. «Ils voulaient nous garder en santé et alertes pour collecter une rançon ou quoi que ce soit d'autre», a-t-il soutenu, ajoutant qu'il avait craint qu'ils soient vendus en otage à Daech (groupe armé État islamique) ou à al-Qaïda. Il est tout aussi incertain sur la possibilité qu'une rançon ait été payée et sur l'implication des gouvernements canadien et italien. La Presse Canadienne (La Presse)

Captive in the jungle
Marites Flor first realized John Ridsdel had been murdered when she saw one of their captors cleaning his blood off a machete… Months later, on June 13, the militants struck again, this time beheading another hostage, Canadian Robert Hall. The 66-year-old was Flor's fiance. Now, months after her own release, Flor gave her first wide-ranging interview to VICE News over Skype, shedding light on the harrowing ordeal she and the hostages who did not make it endured. She revealed new details of just how close the Philippine military was to the Abu Sayyaf camp — at one point, the gunfire exchange between the militants and the army was so close, Flor could smell the smoke — and a $1 million ransom offer by the Ridsdel family that fell short of the captors demands. A Filipina woman, Flor was an afterthought in Canadian media coverage of the hostage situation that began on Sept. 21, 2015, when she, Ridsdel, Hall, and Norwegian Kjartan Sekkingstad were captured at gunpoint at a Philippine resort in the Mindanao region. But during her time in captivity, Flor played a crucial role, becoming the go-between translator and advocate for the three foreign hostages. They pinned their hopes on newly-elected Prime Minister Justin Trudeau, who stood firm on Canada's policy of not paying ransom demands to terrorists. After witnessing horrors and starving in the jungle, Flor is now back to a healthy weight and is getting support from a therapist. What follows is her account of the nine months she spent in captivity. Vice News

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

La carte Nexus en quelques questions faciles
On aurait bien envie de l'avoir entre les mains lorsqu'on se heurte à une file d'attente interminable aux douanes américaines, mais on n'est pas tout à fait certain de ce qu'elle représente. La carte Nexus vous est ici expliquée en 8 points, grâce aux informations fournies par l'Agence des services frontaliers du Canada. Canoe (TVA Nouvelles)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Donald Trump Advised to Train 100,000 Hackers to Protect the US
US President-elect Donald Trump should train and hire around 100,000 hackers whose main purpose would be hacking but also defending the country from cyberattacks, a commission including top security experts, including former NSA director Keith Alexander and MasterCard CEO Ajay Banga, said in a report. The panel of security experts pointed out that cybersecurity should become a priority during Donald Trump's tenure at the helm of the United States, and recommended the President-elect not only to train hackers and be prepared for any cyber threat, but also to propose international norms for hacking that would guarantee better protection. Softpedia

Enter 'The Glass Room,' Where Privacy Goes To Die
The line of people moving down Mulberry Street in Manhattan's SoHo district on Tuesday night could've easily been confused for a product launch. It was pouring rain, and the mostly-young crowd was slowly shuffling past designer handbag stores and into a shiny, brightly-lit storefront reminiscent of Apple's trademark retail destinations. Unbeknownst to them or anyone casually passing by on the street, their smartphones were being tracked. An array of cylindrical Yagi antennas pointed outward from the storefront's windowed entrance, recording the positions and unique MAC addresses of every WiFi-enabled device that wandered by—a setup reminiscent of the "Stingray" fake cell tower devices secretly used by police to track cellphones en-masse. Inside, a huge screen displayed a map of those devices as their owners sauntered about the space, consuming hors d'oeuvres and cocktails with cheeky cyber-themed names like "The Firewall." The "store" isn't actually a store, of course. This was the opening party for The Glass Room, a pop-up digital privacy space that's free and open to the public through December 14, courtesy of Mozilla, makers of the Firefox browser, and the Tactical Technology Collective, a Berlin-based activist group known for interventions in online security and digital rights. Motherboard

LAW ENFORCEMENT / APPLICATION DE LA LOI

Threat called into Air Tindi ruled a hoax by RCMP
All of Air Tindi's planes landed safely Friday after a threat was called into the airline. The details of the threat have not been released, but in a press release, RCMP say it was a "hoax and all leads are being followed up by the police." Alasdair Martin, the president of Air Tindi, says four planes were in the air at the time of the threat, which happened around 12 p.m. Friday. "We are going through a process now on following up with the passengers as well to see if people have any concerns with people getting on the aircraft afterwards," he said. RCMP investigated on and near the Air Tindi site Friday afternoon and quickly concluded the threat wasn't real. No locations were evacuated, they say. CBC News

Waycobah man faces multiple drug and weapon charges after RCMP search his home
The Inverness Country District RCMP and Victoria Country District RCMP say they are continuing to investigate after they arrested a 51-year-old man. The Mounties say that while executing a search warrant on Friday night they found a quantity of marijuana, oxycodone and a set of brass knuckles. Kenneth John Googoo, 51, of Waycobah will face charges for possession for the purpose of trafficking oxycodone, possession for the purpose of trafficking cannabis and possession of a prohibited weapon. Metro News

RCMP searching for man in Nanaimo armed robbery
RCMP say a man armed with a handgun robbed a 7-Eleven in Nanaimo on Friday. A cashier was working alone just before 4 a.m. when a man entered the store, pointed a gun at the teller and demanded cash and cigarettes. Police say the cashier complied, and the man fled the store on foot. He has not been located, and police are trying to identify the man described as Caucasian, 6-feet tall with a thin build and dirty blond curly hair. Canadian Press (CTV News)

N.S. RCMP request public assistance after gas station robbery
RCMP in New Minas, N.S. are asking for the public's assistance in a gas station robbery investigation. Around 3:00 am Friday, a man entered a New Minas gas station and demanded money and cigarettes from the clerk. The man threatened to use a knife, though the clerk didn't see one. The man got away in dark coloured two-door vehicle with a quantity of cash and cigarettes. The clerk wasn't injured. The suspect is described as being five-feet 10 inches tall, 320 pounds, and wearing dark clothing. Kings District RCMP have not made an arrest. Anyone with information about the incident is asked to call RCMP or Crime Stoppers. CTV News; Metro News

Cops trying to save lives with CPR or naloxone won't be investigated
British Columbia's police watchdog will no longer investigate police officers who have provided life-saving measures resulting in someone's death. The Independent Investigations Office says that while it is tasked with investigating in-custody deaths, officers who use CPR or the overdose-reversing drug naloxone to save someone's life will not be subjected to an investigation. Spokesman Marten Youssef says the change was brought in on Friday, a week after an overdose victim died in Surrey while an RCMP officer was administering naloxone... He says some police departments have been reluctant to provide officers with naloxone because of concerns over investigations if someone dies, but that will no longer happen. Canadian Press (CTV News)

Amber Alert for nine-year-old girl concluded, girl still missing: police
Niagara police have concluded an Amber Alert for a missing nine-year-old girl; however they will continue looking for her, classifying the search as a missing persons case. Police first issued the alert for Layla Sabry on Friday night and the broadcast order ended at around 3 a.m. on Saturday, as per protocol. "The Amber Alert is not cancelled. What happened is the broadcast gets cancelled automatically after five hours," Staff Sgt. Paul Rogers told CP24. "We are still actively looking for this young lady and her mother. There is a court order that we will be enforcing to apprehend the child for now and sort all of this out." CP24; Canadian Press (CBC News; National Post; Huffington Post); CBC News

RCMP searching for missing 14-year-old girl
RCMP are searching for a missing 14-year-old girl from Ahtahkakoop First Nation. Rachel Isnana was last seen at her home at 3:30 a.m. CST Sunday morning. Her mother reported her missing at approximately 6:45 a.m. Isnana resides on the Ahtahkakoop First Nation, but may also be on the Beardy's First Nation. CBC News; StarPhoenix; Global News

Alvarenga Alert Cancelled: Missing girl found
An amber alert has been cancelled after Manitoba RCMP say the missing eight-year-old girl, Luisa Alvarenga, was found safe in Winnipeg. An AMBER Alert was issued for 8-year-old late Friday afternoon. RCMP confirmed that the girl was found safe just after 6 p.m. CT during a media briefing. Canada Journal; Canadian Press (Calgary Herald)

Body found on White Rock beach
Global News reports that a body has been found on the beach near White Rock Pier this morning. The man's body has not yet been identified by RCMP, but officials told Global the death doesn't appear suspicious. They also said the body has been in the water for some time. CKNW News

Vernon RCMP Supt. responds to 'RISK IT OUT'
A letter by Vernon RCMP Superintendent McNamara states, "Editor, I am concerned by significant inaccuracies that could compromise both officer and public safety, in the November 30th Infonews article by Charlotte Helston on RCMP staffing in Vernon.To set the record straight, I do not believe chronic

under staffing is leaving our police officers or the public in danger. Ms. Helston's article is largely based on information from anonymous sources. Unfortunately anonymous sources, or those not working within our environment, don't have to account for misinformation they're providing. When she contacted me with questions on staffing, overtime and leave I provided her with detailed, factual answers. She literally used less than ten words from what I gave her…" Infonews

Editor's Note in response to allegations from Vernon RCMP Supt. Jim McNamara
An editor's note in response to Vernon RCMP Superintendent McNamara's letter states, "Editor's note:• Watch shifts at the Vernon detachment have fallen as low as three roadable officers.• The department suffers from chronic understaffing.• Sources, who we trust and who have knowledge of the situation, say understaffing is creating dangerous work conditions for officers on the road.That's what our first story on chronic understaffing at the Vernon RCMP detachment alleged. They remain entirely unaddressed by Supt. Jim McNamara statement yesterday or by the City of Vernon in its response Thursday.Supt. McNamara alleges 'significant inaccuracies' in our story. We have found one error in our reporting, specifically the number of roadable officers... Supt. McNamara provided plenty of information, some of which we intended and still intend to use in further reporting on the subject. However, much of the information he has supplied did not aid our efforts to understand the issue facing his officers and the community of Vernon. He refused all requests for interviews for this story. We share Supt. McNamara's concern for officer and public safety. We look forward to returning to the discussion this story has provoked." Infonews

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

NIL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Missing persons cases in Winnipeg continue to soar with 7.3k reports this year
The number of people reported missing in Winnipeg continues to soar with more than 7,335 missing persons reports since January. Detective Sgt. Shauna Neufeld, head of the Winnipeg Police Service's Missing Persons Unit, says the figure is in line with previous years, which saw record numbers. In 2015, 8,894 people were reported missing in the city — a 29 per cent increase over 2014. Those numbers are high but a lot of those numbers are quickly resolved throughout the year," Neufeld said, adding this week has been noticeably busy. As of Monday, there were 99 "short-term" active missing persons with roughly 70 per cent involving youth, she said. CBC News

Contrer l'alcool au volant : augmentation des contrôles routiers en Alberta
Des centaines d'agents de la Gendarmerie royale du Canada (GRC) et d'autres forces de l'ordre augmenteront le nombre de contrôles routiers en Alberta au cours de la fin de semaine. La GRC indique au public qu'elle veut renforcer la sécurité routière afin de combattre la conduite en état d'ébriété lors de la période du temps des fêtes, selon un communiqué. Le Service de police de Calgary a lancé sa campagne annuelle contre l'alcool au volant « Checkstop » vendredi soir… La GRC indique que plus de 1600 suspensions immédiates de permis ont été émises en 2016. Radio Canada

More than 1/3 of fatal crashes in N.B. involve impaired driving
More than a third of the fatal traffic crashes this year on roads patrolled by the New Brunswick RCMP have involved impaired driving. The force says 20 of the 55 fatal crashes involved drugs or alcohol. Those 55 crashes killed 60 people. As recently as the weekend of Nov. 12, Moncton's Codiac Regional RCMP arrested seven people for impaired driving. All of those drivers were arrested after checkstops, and RCMP will be out in full force Saturday with a similar initiative, but this time it will be province-wide. As part of National Safe Driving Week from Dec. 1 to 7, the provincial RCMP are participating in National Impaired Driving Enforcement Day. CBC News

Sask. RCMP using social media to curb drunk driving
Saskatchewan RCMP took a new approach to addressing drunk driving Saturday, sharing their stories on social media. It's part of National Impaired Driving Enforcement Day. At 11 a.m. they began posting stories from their members about their experience with drunk drivers. 650 CKOM; CTV News

Ridge Mounties continue holiday tradition
Ridge Meadows RCMP continue with the tradition of spreading good will amongst members of the community. Local police will go to senior care homes and events and perform Christmas carol sing-a-longs. Police will also visit a number of elementary schools in Maple Ridge and Pitt Meadows to meet students, and offer sweet treats. Maple Ridge News

Prince George Mounties hope to pack police cars with donations
The Prince George RCMP are looking to give to the Prince George Council of Seniors this holiday season. Today, they'll be holding their first ever 'Pack A P.C.' Event, with a goal of filling up police cars entirely with non-perishable food items. "We're not sure what to expect," says Corporal Craig Douglass. "We will have the van and that'll be interesting to see how much because it'll take more than a regular police car. Then other locations will have regular police cars." At each of the four Save-On-Foods locations in the city, RCMP are encouraging grocery shoppers to pick up something extra for their cause. My Prince George

Mayor Iveson thinks Fentanyl crisis needs to be met with compassion, not judgement
Mayor Don Iveson believes the opioid crisis facing our country needs to be met with compassion, not judgement. He said Edmonton is watching with great interest with how Vancouver is dealing with it as the problem seems to be moving west. "It came to Edmonton sort of through Calgary, so we had the benefit of watching public health responses and we don't have it licked by any stretch." Iveson said Vancouver is way ahead in harm reduction with its needle exchanges and safe injection sites. "The science gives us lots of guidance on what to do, the public needs a lot of conversation about why this is not only the compassionate thing to do but also from the public policy point of view the most cost effective approach. Even if it's not what people come to naturally because of assumptions that they make." AM 770

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Never Blame the Victim says YWCA Canada's Rose Campaign
YWCA Canada recently launched its annual Rose Campaign to end violence against women on Parliament Hill with a call for Canadians to #NeverBlameTheVictim of sexual assault. Through the Rose Campaign, Canada's oldest and largest women's multi-service association supports the wave of change on sexual assault working to end victim blaming and rape culture and adopt a consent culture... "NWAC is currently dedicated to seeking accountability from the Inquiry on Missing and Murdered Indigenous Women and Girls as they attempt to address the systems that contribute to the plague of violence upon Indigenous women here in Canada," says Francyne Joe, Interim President of the Native Women's Association of Canada. "Speaking at the press conference to launch the Rose Campaign 2016 and the 16 Days of Activism Against Gender-based Violence gives me a unique chance to speak not only for the Indigenous women of Canada but to draw attention to the need for more protection for Indigenous women worldwide." The Suburban

57th Six Nations elected council sworn in
Six Nations elected council scored a lot of achievements for the community in the past three years, but the new one has a number of challenges to keep the territory on a wave of growth and prosperity, re-elected Chief Ava Hill told more than 50 people at a swearing in ceremony. Standing in a community room in the Six Nations Tourism hall on Friday evening, Hill told an upbeat gathering to witness the 57th council take their oaths of office that she was proud the last council had brought the water treatment plant to completion... Council also must keep looking for ways to advance the issue of missing and murdered

indigenous women and children, Hill said, noting that Six Nations has its own cases right in the community. Brantford Expositor

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

NIL

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Quebec Mohawk chief vows civil unrest if B.C. pipeline moves forward
A Quebec Mohawk chief is promising a coordinated campaign of civil disobedience if recently approved pipeline construction encroaches on aboriginal territory in British Columbia. The actions could range from demonstrations and rail blockades to people occupying government offices across Canada, according to Kanesatake Grand Chief Serge Simon. "I've always said my favourite form of action is civil disobedience," said Simon, in an interview with the Montreal Gazette. "If the government insists on ignoring its commitment to First Nations, we're looking at unrest in many areas of the country, not just in British Columbia." The chief's comments come as Natural Resources Minister Jim Carr suggested Friday that the federal government will consider deploying military forces in response to non-peaceful forms of protest. Gazette (Ottawa Citizen)

Expect to see CF-18 fighter jets operating out of Ottawa for a couple of days
Two Royal Canadian Air Force CF-18 Hornet fighter jets from 3 Wing Bagotville, Quebec, will operate out of the Ottawa Macdonald-Cartier International Airport for a military exercise in New York State. The exercise started December 2 and runs until Dec. 4. The CF-18s are taking part in Dissimilar Air Combat Training (DACT) with U.S. F-16 Fighting Falcons in New York State, just south of Ottawa, the RCAF noted in a news release. "DACT exposes RCAF CF-18 pilots to fighter aircraft that they do not interact with on a regular basis to provide more realistic training," the release added. Ottawa Citizen

Proposed bill would guarantee coverage for B.C. first responders: MLA
A B.C. MLA wants the provincial government to declare post-traumatic stress disorder a "presumptive illness" for emergency workers in order to guarantee coverage for health services. B.C. NDP MLA Shane Simpson says there is concern the British Columbia government isn't doing enough to help firefighters, police officers and paramedics suffering from post-traumatic stress disorder. CTV News

INTERNATIONAL

Morocco arrests suspect tied to thwarted French attack plot
Moroccan police have arrested a "dangerous element" who allegedly served as a liaison between the Islamic State group's external operations and members of a French cell that was dismantled last month while allegedly planning an attack. The state-run MAP news agency reported on Saturday that the arrested man allegedly met on the Turkish-Syrian border with emissaries of the Islamic State group who provided instructions that were to be communicated to the group in France. MAP didn't name the suspect or say when or where he was arrested. Associated Press (CTV News)

Found at an Islamic State training camp: bunk beds, weapons manuals, steroids
The bunk beds that fill the rooms sleep more than 80 Islamic State recruits. On the walls, posters detail the components of Russian Kalashnikovs and American assault rifles. One sign reminds the trainees that

victory comes from long fights and pain — rewards come later: "Remember that we didn't come for this life, we came for the afterlife." Spread across several large houses, the "Sheikh Abu Samaya Ansari Camp" was discovered this week by Iraqi forces as they pushed deeper into the northern city of Mosul, which Islamic State militants have been fighting bitterly to retain. It is the first military training center that the Iraqi forces have found in the city since they began an offensive to retake it just more than six weeks ago. Washington Post

US cautions crackdown in Myanmar could radicalize Muslims
It's a scene straight out of Myanmar's dark past: a military offensive waged beyond world view that forces ethnic minority villagers from the smouldering ruins of their homes. The U.S. government, a key sponsor of Myanmar's democratic transition, says a security crackdown that has displaced tens of thousands of Rohingya Muslims and left an unknown number dead risks radicalizing a downtrodden people and stoking religious tensions in Southeast Asia. The military moved in after armed attacks by unknown assailants on police posts along the border with Bangladesh in October. The attacks in Rakhine State were a possible sign that a small number of Rohingya were starting to fight back against persecution by majority Buddhists who view them as illegal immigrants although many have lived in Myanmar for generations. Associated Press (Metro News)

North Korea's Government Sanctioned Operating System Can Be Hacked Remotely
Today a group of hackers found a new vulnerability in Red Star OS—North Korea's government sanctioned operating system—which allows it to easily be hacked remotely. The hermit kingdom's linux-based OS has never exactly been known for its security features and significant vulnerabilities have been exposed on numerous occasions since it leaked to the rest of the world last year. The latest vulnerability, exposed by the information security company Hacker House "to mark Red Star's anniversary leak," allows a hacker to remotely access users' computers simply by getting them to click on a hyperlink. Motherboard

'It's just a ploy': North Dakota protesters reject help from officials to leave as winter descends
The head of North Dakota's emergency management services says the state is prepared to respond to Dakota Access pipeline protesters who may need help during a winter storm or some other crisis. But some protesters on their way to the site are rejecting those calls, saying it's "just a ploy" to get them out. Speaking with CBC News near Standing Rock, Sam Deering and Sean Kristopher Tremblay of the group U.S. Vets for Standing Rock said the pledge by officials to help protesters leave the site on the basis of safety is disingenuous and proof that the movement is gaining momentum. CBC News

UK to double armed drone fleet in deal with US Predator manufacturer
The United Kingdom will double its fleet of armed drones, defense secretary Michael Fallon announced on Saturday, under a $125m (£100m) development deal with US arms manufacturer General Atomics. eneral Atomics, makers of the Predator and Reaper drones used widely by the US, will provide 10 drones to the Royal Air Force, bringing the fleet from 10 to 20. Fallon described the drone expansion as a major addition in terms of firepower, imaging and intelligence gathering. For the past two years, the UK's drone arsenal has been centered on fighting Islamic State in Iraq and Syria. Guardian (UK)

Police criticized after using 'fake news' in sting aimed at California gang
Police investigating a notorious gang in a city on California's central coast issued a fake press release that the chief credited with saving two men by deceiving gang members who wanted to kill them, but the ruse was criticized by news organizations who reported it as fact. Santa Maria Police Chief Ralph Martin defended the rare tactic this week when it came to light, saying he had never done such a thing in his 43-year career, but he wouldn't rule out doing it again. Associated Press (Global News)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

IBC
Get the facts. Contact your rep. Be #EQready. http://bit.ly/1HDyXOg

Prince George SAR
Two members of PGSAR and two from Nechako Valley are in attendance with 20 others from across the province.

RadioCanadaInfo
Plus de 10 000 foyers toujours privés d'électricité dans la région de Québec http://bit.ly/2gA4YU4

theprovince
Rescuers in northwestern B.C. search remote highway for missing U.S. man http://theprov.in/2gNlpKC

CTVVancouver
People living in Tofino and Ucluelet are cut off from the rest of Vancouver Island due to a washout https://t.co/eOQKxduoCg

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

OpenMedia
Second round of of National Security consultations are happening TODAY in #Vancouver! Join @OpenMediaOrg and pls RT! #YourNatlSec

NATIONAL SECURITY / SÉCURITÉ NATIONALE

CSIS Canada
Proud to support International Day of Persons with Disabilities 2016 #AccessibleCanada #BreakingBarriers

NCCM
Visit us 2day as young Calgarians find ways 2 counter #Islamophobia thru storytelling w/amazing line-up / talent! contact aelghawaby@nccm.ca

OpenMedia
Cellphone providers may soon be able to know when police is snooping on their networks, research shows: http://ow.ly/CqH7306J7pa #Stingrays

Craig Forcese
And as much as I respect their efforts, reporters who are parachuted into this area btwn assignments are simply unable to follow threats /5

Craig Forcese
There are only a handful of journalists who do the nat'l security best in Cda /2

Craig Forcese
Just read @imacnewser leaving @OttawaCitizen. Ian's departure real lose to nat'l security reporting in Cda /1 https://twitter.com/imacnewser/status/802203770767675392 …

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

InSight Crime
Cream Cocaine Latest Innovation by Drug Traffickers http://ow.ly/tFrl306KUZu

LAW ENFORCEMENT / APPLICATION DE LA LOI

Infonews Kamloops
Vernon RCMP Supt. responds to 'RISK IT OUT' https://goo.gl/v64zUn

CPAC
Should the RCMP have enhanced digital surveillance powers to fight crime? Outburst asks Canadians this & more, next on CPAC

CTVNewsVI
RCMP searching for man in Nanaimo armed robbery https://t.co/4WABHwuaU7

CTVVancouver
Cops trying to save lives with CPR or naloxone won't be investigated: Watchdog http://ctv.news/84fj9rf

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

APTNNews
"More than 3/4 of indigenous offenders were sent to medium or maximum security institutions." #cndpoli #Canada http://aptn.ca/news/?p=66529

MacleansMag
The UN would call Adam Capay's treatment torture. In a Canada, he was just another inmate in segregation: https://t.co/YYmYUFGsDx

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

OVC Ontario
Do you know someone who deserves recognition for their exemplary work with victims of crime? Consider nominating them for #AGsAwards!

Women in Canada
We must not normalize gender-based violence in society. Your #ActionsMatter

BC Civil Liberties
In response to BC's overdose crisis, policy change by police watchdog encourages police to step in to save lives.

Rabble.ca
ICYMI: Carding: An open letter to the City of #Toronto from Black intellectuals, writers, organizers #TOPoli http://buff.ly/2qiALpN

AngelaSterritt
Missing persons cases in Winnipeg continue to soar with 7.3k reports this year https://t.co/7mH5OBU6wJ

OTHER / AUTRES

CF Operations
#HMCSEdmonton helped the @USCG to disrupt over 2 tonnes of cocaine during #OpCARIBBE Bravo Zulu! http://bit.ly/OperationCARIBBE ...

Postmedia News
Expect to see CF-18 fighter jets operating out of Ottawa for a couple of days

CTVNews
Proposed bill would guarantee coverage for B.C. first responders: MLA https://t.co/Ms9t2kwsQ2

INTERNATIONAL

Craig Forcese
Canadian Journalist's Detention at U.S. Border Raises Press Freedom Alarms

motherboard
North Korea's government sanctioned operating system can be hacked remotely: http://bit.ly/2gTlwmX

CBCNews
North Dakota officials pledge 'humane' help for protesters as 'winter begins to take hold'
http://www.cbc.ca/1.3880276

FreedomofPress
Families who sheltered Edward @Snowden in Hong Kong say NSA whistleblower 'gave them hope'
https://t.co/Z1x0ymHMWu

GuardianUS
UK to double armed drone fleet in deal with US Predator manufacturer https://t.co/USv8LX3fa0

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

Today's News / Actualités
December 6, 2016 / le 6 décembre 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

La tuerie de Polytechnique est soulignée sobrement

L'école Polytechnique de Montréal avait choisi de souligner sobrement, mardi, le 27e anniversaire de la tuerie qui avait fait 14 morts — toutes des femmes — le 6 décembre 1989. Un bouquet de 14 roses blanches a été déposé devant la plaque commémorative en l'honneur des femmes tombées sous les balles de Marc Lépine ce jour-là. Les drapeaux étaient aussi en berne sur le campus mais aussi sur le toit de certains édifices montréalais mardi. Peu après midi, le premier ministre Justin Trudeau et 10 de ses ministres — toutes des femmes — ont déposé des roses blanches devant la Flamme du centenaire, à

Ottawa, sous le regard de six de leurs collègues masculins. La courte cérémonie s'est déroulée dans le silence, alors que la ministre de la Santé, Jane Philpott, pleurait à chaudes larmes. Sa collègue Mélanie Joly a réussi à refouler les siennes, avec difficulté. Invitée à dire après la cérémonie ce que son gouvernement pouvait faire pour adoucir le 6 décembre, la ministre Joly a répondu qu'il fallait «le commémorer»....En matinée, M. Trudeau, la ministre de la Justice, Jody Wilson-Raybould, et la ministre de la Condition féminine, Patty Hajdu, ont tous trois publié des communiqués pour souligner le 6 décembre, sans toutefois faire allusion au contrôle des armes à feu. «Aujourd'hui et chaque jour, nous réaffirmons notre engagement à trouver des solutions qui aideront à prévenir les actes de violence dans l'avenir», peut-on lire dans le communiqué du premier ministre. M. Trudeau insiste sur l'intention de son gouvernement d'augmenter le nombre de refuges et de maisons de transition pour les femmes victimes de violence familiale. «J'encourage tout le monde à réfléchir au fait que leurs propres gestes comptent. Pour commencer, joignez-vous à la conversation en ligne au moyen du mot-clic #GestesComptent», a-t-il également offert... En sortant de la réunion du cabinet, mardi après-midi, **le ministre responsable de ce dossier, Ralph Goodale**, a voulu calmer les doutes de Mme Rathjen. ***«Il y a toute une série d'amendements sur lesquels nous travaillons, a-t-il assuré. Nous présenterons un projet de loi dans les semaines et les mois à venir.»*** **Le ministre Goodale** a ensuite voulu souligner **qu'il** est à revoir la composition du comité consultatif sur les armes, groupe que les conservateurs de Stephen Harper avaient peuplé de membres du lobby pro-armes. **Il a promis** un comité mieux équilibré ***«très bientôt»***. Mais **il ne sait pas** si cela se fera avant janvier. ***«Nous travaillons très fort sur tous ces éléments et nous avons l'intention de les présenter aussitôt que nous aurons aligné nos flûtes»***, a insisté **le ministre de la Sécurité publique**, mais toujours sans offrir un quelconque échéancier. «C'était des choses assez faciles à faire. Ils ne les ont toujours pas faites», a critiqué le chef néo-démocrate Thomas Mulcair. Presse Canadienne (Journal Métro)

Spies should not be allowed to keep innocent people's data, privacy czars say
Canada's spy agencies should destroy the data trails of innocent people they incidentally collect during terrorism investigations once the actual targets have been cleared of suspicion, say Canada's privacy watchdogs. The declaration Tuesday from privacy commissioners across the country came after a judge recently ruled the Canadian Security Intelligence Service violated the law by keeping potentially revealing electronic data about people who were not under investigation. The message was part of a joint submission signed by federal, provincial and territorial privacy czars that urged the Trudeau government to strengthen protection of personal information as it revamps the national security regime. Rather than expand state powers and reduce individual rights, it is time to beef up legal standards and oversight to prevent repetition of mistakes, said federal privacy commissioner Daniel Therrien, flanked at a news conference by counterparts Brian Beamish from Ontario and Jean Chartier of Quebec. They urged the government to learn lessons from the information-sharing blunders that led to the overseas torture of Maher Arar following 9/11 and the current uproar over surveillance of journalists in Quebec... Just last month a Federal Court judge said CSIS broke the law by holding on to electronic data, over a 10-year period, about people who were not considered a danger to national security... **Public Safety Minister Ralph Goodale said** Tuesday the joint submission would help the government redraft security policy. ***"We have two critical objectives to achieve: No. 1, keep Canadians safe, and at the same time ... make sure that Canadian rights and freedoms are respected, along with the open, generous and inclusive nature of our democratic society."*** Canadian Press (Metro News)

Don't expand police spying powers, watchdogs say
Privacy watchdogs from across the country have come together to challenge proposals to expand police and intelligence agencies' powers. Federal Privacy Commissioner Daniel Therrien told a press conference Tuesday that state spying and investigative powers have "already been significantly increased" in recent years. The RCMP have recently undertaken a public push for more powers to investigate online crime, arguing privacy-protecting software and laws are preventing them from catching criminals. But Therrien suggested that the balance is actually tipped in police agencies' favour, and argued for greater legal safeguards to protect Canadians' privacy. "In my view, this is not the time to further expand state powers and reduce individual rights," Therrien said in a statement (...)In a joint submission to the federal Liberals with provincial and territorial privacy commissioners, Therrien questioned a number of proposals outlined in **Public Safety Minister Ralph Goodale's** discussion paper on Canada's national security framework. More strict rules should be brought in on accessing Canadian

metadata, for instance. Metadata is often described by police as innocuous "phone book information" — telephone numbers, IP addresses, residential addresses, and so on. Toronto Star

Trudeau cabinet expected to debate renewed Ukraine mission
The Liberal government signalled to its allies that it is prepared to extend Canada's military training mission in Ukraine, CBC News has learned. A series of senior Ukrainian government officials visited Ottawa over the last few weeks, warning of the dangers of warming frosty relations with Russia. But they have also lobbied for renewed Canadian assistance beyond March 2017, when the current deployment is set to expire. Several sources, with knowledge of the file who could not speak publicly, said there is a clear intention for Canada to remain, but the size, scope and composition of the force is yet to be determined and the federal cabinet has yet to give its blessing (...) Ukraine Interior Minister Arsen Avakov met on Monday with **Public Safety Minister Ralph Goodale,** where the two discussed Canada's commitment to police training and judicial reform, among other things. In an interview with CBC News, Avakov would not confirm if he and **Goodale** spoke about the military training commitment — or the reasons Canada has discontinued a program of providing satellite images of eastern regions where Russian-back separatists have been fighting a low-grade war of attrition (...) Avakov did, however, put a major proposal in front of **Goodale,** requesting training for Ukrainian national guard units and police forces. Canada seems anxious to remain involved in the building of institutions, such as the national police force where a partnership is being formed with the RCMP, he said (...) Both he and **Goodale** also spoke extensively about the daily cyberattacks that have hit Ukraine, and in some cases caused disruptions to important infrastructure including the country's power grid and major airport. Public Safety is the lead in Canada when it comes to cyber-defence and Avakov asked for the department's assistance, specifically access to analytical programs used by the federal government, ones "that analyze huge masses of information" known as metadata. Avakov also told **Goodale** he would like to see more Canadians involved as ceasefire observers through the Organization for Security and Co-operation in Europe (OSCE). CBC News

TOP STORIES / MANCHETTES

Liberals to announce $3-billion search and rescue aircraft contract — Airbus named as winner
The Liberal government will announce the winner of a multi-billion dollar program for new search and rescue aircraft on Thursday, even as industry sources say aerospace giant Airbus has won the deal. The announcement was planned for Winnipeg on Thursday but at the last minute was changed to the Canadian Forces base at Trenton, Ont., sources say. The Airbus C-295 was selected over the C-27J built by the Italian firm, Leonardo. National Post

Privacy watchdogs urge caution with encryption laws
Privacy watchdogs from across Canada warned the government on Tuesday to "proceed cautiously" before passing encryption legislation — a move that would have the potential to undermine the security of everything from financial transactions to online communication. The warning comes at a time when government and law enforcement agencies have been seeking the ability to access encrypted information, the lack of which they see as a growing investigative problem... The government is currently soliciting feedback and holding public consultations on this and other national security issues, as part of its pledge to to repeal the "problematic elements" of Bill C-51. In a submission to **Public Safety Canada**, Canada's Privacy Commissioner Daniel Therrien and his colleagues warned against introducing any legislation aimed squarely at encryption, as well as other proposed powers that police do not currently have... One particularly divisive issue is the matter of encryption — cryptographic protections that prevent attackers and police alike from eavesdropping on messages as they travel across the internet, or from accessing files on a password-protected device. ***"There is currently no legal procedure designed to require a person or an organization to decrypt their material,"*** according to **Public Safety Canada's** "***National Security Green Paper,"*** which was released in September to ***"prompt discussion and debate about Canada's national security framework."*** Both law enforcement and government agencies have increasingly characterized encryption as an impediment to investigations, a problem they refer to as "going dark." Canada's police chiefs, for example, recently called on the government to

introduce legal measures that deal with encryption, and the US Senate introduced a draft bill addressing encryption earlier this year. CBC News; IT World Canada

Surveillance: les commissaires à la vie privée demandent un meilleur encadrement de la police
Citant les révélations d'Edward Snowden et les cas de journalistes surveillés au Québec, les commissaires à la protection de la vie privée du pays mettent le gouvernement Trudeau en garde: au lieu de donner de nouveaux pouvoirs aux corps policiers, Ottawa doit plutôt mieux encadrer les pouvoirs policiers existants en matière de surveillance. Dans le cadre de la consultation du gouvernement Trudeau pour moderniser le cadre de sécurité nationale, le commissaire à la protection de la vie privée du Canada Daniel Therrien ainsi que tous ses homologues provinciaux demandent à Ottawa de ne pas hausser les pouvoirs policiers en matière de surveillance... «Sans vouloir faire comparaison» avec les services de renseignement des ex-républiques de l'Europe de l'est, le commissaire Daniel Therrien rappelle toutefois une décision récente de la Cour fédérale dénonçant le fait que le SCRS a conservé de façon illégale pendant plusieurs années des métadonnées de citoyens canadiens (le SCRS interprétait la loi différemment et s'est plié à la décision de la Cour fédérale). «Nous parlons ici de retenir des données de citoyens ordinaires. Je ne crois pas que c'est le type de société dans laquelle [les Canadiens] veulent vivre», dit le commissaire Daniel Therrien... Le gouvernement Trudeau a lancé a lancé cette année une consultation sur la modernisation du cadre de sécurité nationale. Les commissaires à la protection de la vie privée ont déposé aujourd'hui un mémoire commun. La Presse ; Globe and Mail

Police haven't made case for more digital spying powers
The federal privacy commissioner says he's not convinced Canadian law enforcement agencies have made their case for greater powers to access Canadians' online information, and urged the federal government not to grant new ones unless police can prove they're needed. "It's not as though there's an absence of tools," said Daniel Therrien Tuesday at the National Press Theatre, where he released a joint submission to the government's national security consultations that had been co-signed by all of Canada's provincial and territorial privacy commissioners. "We remain to be convinced. We do not think they have made their case." Launched in September, the government's national security consultations run until December 15, are aimed at getting Canadians to share their ideas and "will help inform future changes to national security tools," according to its website. The consultations come at a time of intense debate about how best to balance the privacy rights of law-abiding citizens with the need for security, and following two high-profile cases where the Canadian Security Establishment and the Canadian Security Intelligence Service were found to be failing to live up to their responsibilities. In January, the CSE held an unprecedented technical briefing to announce it had stopped its metadata sharing program with international intelligence partners because the data was not being properly scrubbed of information that could identify Canadians... More recently, some have accused the RCMP of using the media to create "moral panic" after they granted security clearances to two reporters from the CBC and the Toronto Star to view pre-vetted files on cases officials claimed had been running into digital roadblocks. One of those cases was that of Strathroy terrorist Aaron Driver, which RCMP said had been obstructed by encryption for more than a year. iPolitics

RCMP officers copied contents of Ismael Habib's laptop in 2014
The RCMP obtained a warrant to go into Ismael Habib's home, take his computer, replicate its contents and replace it while he was in Sault Ste. Marie, Ont., seeing a woman, a Quebec court heard Tuesday. Habib is charged with attempting to leave Canada to commit terrorist acts and giving false information to obtain a passport. The trial is being heard by Quebec Court Judge Serge Délisle at the Montreal courthouse. CBC News

City of Surrey and Surrey RCMP launch City Centre Response Plan
The City of Surrey and Surrey RCMP have launched their City Centre Response Plan to address the public safety and public health concerns for both the homeless and the community in the 135A area. The plan will address three key areas: 1. Enhanced Outreach and Presence on 135A. 2. Emergency Housing. 3. Engagement and Education. “As is the case with all municipalities in the region, Surrey is facing increased challenges related to homelessness, mental health issues and fentanyl use,” said Surrey Mayor Linda Hepner. “With the City Centre Response Plan, we are taking tangible, concrete action on addressing the public safety issues that area businesses and residents are faced with on a regular basis,

while addressing the public health challenges that affect the vulnerable who are easily preyed upon and exploited." Voice Online; CKNW NEWS AM 980

Violence against women has touched us all, Wynne says on anniversary of Montreal Massacre
Ontario Premier Kathleen Wynne placed roses in a vase at a ceremony in Toronto in memory of 14 women killed in Montreal 27 years ago. Wynne, along with Toronto Mayor John Tory, spoke at Women's College Hospital about the deaths at l'École Polytechnique on Dec. 6 in 1989. On this day in 1989, 14 women were shot and killed at the engineering school by a gunman professing to hate feminists. CBC News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Liberals to announce $3-billion search and rescue aircraft contract — Airbus named as winner
The Liberal government will announce the winner of a multi-billion dollar program for new search and rescue aircraft on Thursday, even as industry sources say aerospace giant Airbus has won the deal. The announcement was planned for Winnipeg on Thursday but at the last minute was changed to the Canadian Forces base at Trenton, Ont., sources say. The Airbus C-295 was selected over the C-27J built by the Italian firm, Leonardo. National Post

Thousands of pounds of food collected in two hours by Chilliwack emergency responders
The Chilliwack Fire Department along with Chilliwack Search and Rescue (SAR) and Emergency Social Services (ESS) cruised around the city last night and collected approximately 13,000 food items (15,000 pounds) and $2,500. Chilliwack Times

Duo awaiting rescue keep cougar at bay
Two Campbell River men stranded on the shore after capsizing near Elk Bay had to ward off a prowling cougar while trying to attract attention from passing boats Saturday night. "A couple of guys were out doing some fishing in Elk Bay, there, and they ended up sinking their boat and had to swim for shore," said Ron Boucher, Officer in Charge of the Canadian Coast Guard vessel Cape Palmerston which is based in Campbell River. Campbell River Mirror

Health ministry investigators didn't understand Ottawa ambulance system, paramedic chief says
An opinion piece states, "Ottawa objects to several findings in a report from the Ministry of Health that said the city's paramedic service violated several policies and service agreements in one August shift, potentially harming patients, says Anthony Di Monte, Ottawa's acting general manager of emergency services. But in a long interview Tuesday, he didn't reject a ministry finding that paramedics frequently didn't tell their dispatchers they'd handed patients over to hospitals -- which cost Ottawa's ambulance system hours of work on one night in August and left people with new emergencies waiting..." Ottawa Sun

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Privacy watchdogs urge caution with encryption laws
Privacy watchdogs from across Canada warned the government on Tuesday to "proceed cautiously" before passing encryption legislation — a move that would have the potential to undermine the security of everything from financial transactions to online communication. The warning comes at a time when government and law enforcement agencies have been seeking the ability to access encrypted information, the lack of which they see as a growing investigative problem... The government is currently soliciting feedback and holding public consultations on this and other national security issues, as part of its pledge to to repeal the "problematic elements" of Bill C-51. In a submission to **Public Safety Canada**, Canada's Privacy Commissioner Daniel Therrien and his colleagues warned against introducing any legislation aimed squarely at encryption, as well as other proposed powers that police do not currently

have... One particularly divisive issue is the matter of encryption — cryptographic protections that prevent attackers and police alike from eavesdropping on messages as they travel across the internet, or from accessing files on a password-protected device. ***"There is currently no legal procedure designed to require a person or an organization to decrypt their material,"*** according to **Public Safety Canada's** "***National Security Green Paper,"*** which was released in September to ***"prompt discussion and debate about Canada's national security framework."*** Both law enforcement and government agencies have increasingly characterized encryption as an impediment to investigations, a problem they refer to as "going dark." Canada's police chiefs, for example, recently called on the government to introduce legal measures that deal with encryption, and the US Senate introduced a draft bill addressing encryption earlier this year. CBC News; IT World Canada

Surveillance: les commissaires à la vie privée demandent un meilleur encadrement de la police
Citant les révélations d'Edward Snowden et les cas de journalistes surveillés au Québec, les commissaires à la protection de la vie privée du pays mettent le gouvernement Trudeau en garde: au lieu de donner de nouveaux pouvoirs aux corps policiers, Ottawa doit plutôt mieux encadrer les pouvoirs policiers existants en matière de surveillance. Dans le cadre de la consultation du gouvernement Trudeau pour moderniser le cadre de sécurité nationale, le commissaire à la protection de la vie privée du Canada Daniel Therrien ainsi que tous ses homologues provinciaux demandent à Ottawa de ne pas hausser les pouvoirs policiers en matière de surveillance... «Sans vouloir faire comparaison» avec les services de renseignement des ex-républiques de l'Europe de l'est, le commissaire Daniel Therrien rappelle toutefois une décision récente de la Cour fédérale dénonçant le fait que le SCRS a conservé de façon illégale pendant plusieurs années des métadonnées de citoyens canadiens (le SCRS interprétait la loi différemment et s'est plié à la décision de la Cour fédérale). «Nous parlons ici de retenir des données de citoyens ordinaires. Je ne crois pas que c'est le type de société dans laquelle [les Canadiens] veulent vivre», dit le commissaire Daniel Therrien... Le gouvernement Trudeau a lancé a lancé cette année une consultation sur la modernisation du cadre de sécurité nationale. Les commissaires à la protection de la vie privée ont déposé aujourd'hui un mémoire commun. La Presse ; Globe and Mail

Police haven't made case for more digital spying powers
The federal privacy commissioner says he's not convinced Canadian law enforcement agencies have made their case for greater powers to access Canadians' online information, and urged the federal government not to grant new ones unless police can prove they're needed. "It's not as though there's an absence of tools," said Daniel Therrien Tuesday at the National Press Theatre, where he released a joint submission to the government's national security consultations that had been co-signed by all of Canada's provincial and territorial privacy commissioners. "We remain to be convinced. We do not think they have made their case." Launched in September, the government's national security consultations run until December 15, are aimed at getting Canadians to share their ideas and "will help inform future changes to national security tools," according to its website. The consultations come at a time of intense debate about how best to balance the privacy rights of law-abiding citizens with the need for security, and following two high-profile cases where the Canadian Security Establishment and the Canadian Security Intelligence Service were found to be failing to live up to their responsibilities. In January, the CSE held an unprecedented technical briefing to announce it had stopped its metadata sharing program with international intelligence partners because the data was not being properly scrubbed of information that could identify Canadians... More recently, some have accused the RCMP of using the media to create "moral panic" after they granted security clearances to two reporters from the CBC and the Toronto Star to view pre-vetted files on cases officials claimed had been running into digital roadblocks. One of those cases was that of Strathroy terrorist Aaron Driver, which RCMP said had been obstructed by encryption for more than a year. iPolitics

NATIONAL SECURITY / SÉCURITÉ NATIONALE

'He's been freed, thank God,' says mother of former Canadian soldier detained after fighting ISIL
A Canadian military veteran who had been detained by Iraqi authorities after spending six months fighting against ISIL has been released, his mother said Tuesday. "He's been freed, thank God," Kay Kennedy said shortly after her son Michael Kennedy phoned home from Erbil to say he was no longer being held. "I

am so happy you couldn't imagine."... Ottawa has discouraged Canadians from taking up arms against ISIL but has not stopped them from travelling or arrested them upon their return, although some have been questioned by the RCMP. National Post

RCMP officers copied contents of Ismael Habib's laptop in 2014

The RCMP obtained a warrant to go into Ismael Habib's home, take his computer, replicate its contents and replace it while he was in Sault Ste. Marie, Ont., seeing a woman, a Quebec court heard Tuesday. Habib is charged with attempting to leave Canada to commit terrorist acts and giving false information to obtain a passport. The trial is being heard by Quebec Court Judge Serge Délisle at the Montreal courthouse. CBC News

"Lock up the agitators"

Conservative party leadership contender Kellie Leitch wants to crack down on and surveil those who interfere with natural resource development projects in Canada... Leitch outlined a five-point plan to quash "violence and/or vandalism" against Energy East and other natural resource projects. Perhaps most striking is her plan to create a "new task force" made up of "specialized components" of the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS), Canada's main spy agency, the Canadian Revenue Agency, and Global Affairs Canada. Government surveillance of Indigenous and environmentalist protesters is not new, but is always controversial. CSIS and the RCMP have been chastised for infiltrating, tracking, and surveilling peaceful activists. The spy agency came under fire for preparing national security plans in case peaceful Indigenous protests "escalated." And last month it was revealed that the RCMP was conducting surveillance on 89 Indigenous activists for their involvement in environmental efforts. Leitch's proposals would clearly turn up the dial on that sort of surveillance. Vice News

Broadcast Media / Médias télédiffusés :

CBC News Network's Power & Politics interviewed Federal Privacy Commissioner Daniel Therrien regarding the retention of data and the expansion of powers for police and intelligence agencies. Rough Transcript

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Bridge Labour Stalemate Into Third Week

The strike by 47 employees at the Blue Water Bridge, now into its third week, was raised in the House of Commons Monday. Windsor West MP Brian Masse says drivers are using the privately owned Ambassador Bridge, resulting in lost revenue for the federal government. Toll collectors, currency exchange personnel, custodians and maintenance staff represented by Local 501 of the Public Service Alliance of Canada (PSAC) walked off the job November 21. Blackburnnews.com

Feds Beef Up Security on NORTHERN Border...To Keep Dems IN or Canadians OUT?

Despite the surge of illegal aliens into the U.S. from the south, U.S. Customs and Border Patrol (CBP) is offering hiring bonuses and advertising to shore up border security in Minnesota and North Dakota. Are they trying to keep Disgruntled Democrats in, or keep Conservative Canadians out? MRCTV

Port authority watches over 'Detroit's $300M forgotten economy'

Detroit is home to a port that's tied to some 15,000 jobs and generates nearly $300 million in state and federal taxes as part of the Great Lakes St. Lawrence Seaway System. And yet many are completely unaware of its existence. To make his point about the Port of Detroit being an afterthought -- if even that -- the head of the authority watching over the $300 million economy likes to use a story of border patrol agents being unaware of its existence. "There is a crewman who comes into the port (from Canada), and when he gives the customs agent his reason for coming, the agent says: 'There's no port here,'" said John Loftus, executive director of the Detroit/Wayne County Port Authority, about general unfamiliarity with the Port of Detroit. M Live

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Mydemocracy.ca poses privacy risks for Canadians in small towns: professor
If Canadians using the government's new electoral reform consultation website don't disclose detailed demographic information, their input won't be included in the study's results - raising privacy concerns for those in small communities, according to University of Ottawa law professor Michael Geist. In a short blog post published Tuesday, Geist highlights a few sentences in the Mydemocracy.ca privacy policy that got missed in the coverage of the site's launch Monday. iPolitics

LAW ENFORCEMENT / APPLICATION DE LA LOI

A Look at Canada's 12 Most Wanted Fugitives
Despite having an international image of being a country purportedly full of angels, Canada has its fair share of unscrupulous transnational fugitives running amok and thwarting international law enforcement agencies. With consultation from RCMP and Interpol databases, we've compiled a list of the country's most wanted, a group of alleged gang bangers, murderers, pedophiles, bikers, and other crooks currently at large in a series of unsolved criminal cases. 1. David MacDonald "Wolf" Carroll. At 64 years of age and after 15 years on the run, Nova Scotian-born David MacDonald Carroll has proven he's a difficult man to trace. Vice News

No charges approved after RCMP investigation into death of aboriginal teen Paige Gauchier
The Criminal Justice Branch of B.C. (CJB) has announced no charges will be laid against police officers or paramedics who failed to tell Ministry of Children and Family Development (MCFD) officials about an incident with Paige Gauchier before the aboriginal teen died of a drug overdose... The CJB has concluded, based on available evidence, that there is no substantial likelihood that the officers or paramedics would be convicted of the offence recommended by the RCMP. CBC News

Ban Donald Trump and save breakfast cartoon characters: Notable petitions sponsored by federal MPs
Free the AR-15 - The AR-15 rifle — the much-maligned civilian variant of the M-16 — is classified as "restricted" in Canada. Just as it is with handguns, this means that the AR-15 can only be fired on a licensed gun range. The AR-15 doesn't shoot more or faster bullets than many non-restricted Canadian hunting rifles, but it made the restricted list largely because of its military appearance and violent cultural mystique. Calling the gun the "most versatile hunting rifle in the world," Newfoundlander Marc Bennett started this petition to once again get Canadians shooting non-paper things with their AR-15s. His efforts earned a pretty definitive "no" from **Public Safety Canada**. Or, as they put it, ***"the Government has no intention of using section 117.15 of the Criminal Code to change the classification of the AR-15."*** Vancouver Sun

Prince District RCMP advises of increased presence
Checkpoints were established in Tignish, Alberton, O'Leary, West Devon, Lennox Island and Borden, and the RCMP also partnered with police forces in Kensington and Summerside to conduct checkpoints in those municipalities. Journal Pioneer

Prolific offender caught in Beaumont Dec. 5
Submitted by the Beaumont RCMP. On December 5 at approximately 8 p.m. Leduc and Beaumont RCMP responded to a report that stolen property was being sold in the McDonald's parking lot in Beaumont. Police attempted to apprehend the suspect when he proceeded to ram two police vehicles with a stolen pickup truck in an attempt to evade police. Devon Dispatch

Charges laid against 2 after seizure of weapons, drugs and counterfeit cash
A list of drug and weapons-related offences have been laid against two people, after an Edmonton home was searched last month. Strathcona County RCMP began an investigation in October in relation to stolen property and drug possession and on Nov. 24, Edmonton police assisted with a search warrant in Edmonton. CKNW News AM 980

5 people wanted in connection to 1998 homicide of Tania Marsden, Manitoba RCMP say
Manitoba RCMP are on the lookout for three men and two women in connection to a homicide nearly two decades old. Tania Marsden was last seen alive on her 18th birthday on Sept. 9, 1998. Her body was found partially submerged and weighed down with a cement block, in the Assiniboine River on Sept. 29., nearly three weeks after she was last seen. Global News; CBC News; Postmedia Network (Ottawa Sun, Edmonton Sun, Toronto, Sun, Winnipeg Sun)

RCMP Report: National Impaired Driving Day was on Dec. 3
Clearwater Traffic Services issued two three-day immediate roadside prohibitions for alcohol and one 24-hour driving prohibition (under Section 215 of the Motor Vehicle Act) on National Impaired Driving Day, Dec. 3. Clear Water Times

RCMP CounterAttack in full force
With the holiday season in full swing, Kamloops RCMP are reminding drivers that roadblocks will be set up around the city for the next four weeks. According to the Ministry of Transportation, 66 people die every year from alcohol-related crashes with 35% of those right in the Interior. CFJC Today

RCMP share their drinking and driving enforcement experience
The public is used to hearing about stories from those impacted by drinking and driving. Those include stories from victims and their families, as well as from those dealing with the consequences of their decisions to drink and drive. But there aren't as many stories told about the impact on law enforcement responding to such instances. That's about to change. In Regina on Friday, Sgt. Al Hofland, acting officer in charge of traffic services in Saskatchewan, announced a social media campaign by the RCMP to tell the stories of police officers who have dealt with drinking and driving incidents. Battlefords News-Optimist

Shot fired at parked vehicle in Yorkton
RCMP are investigating after a parked vehicle was damaged by gunfire in Yorkton. Around 10:30 p.m. Monday, residents reported hearing a loud bang on the north end of First Avenue near York Road. CTV News

Drug busts in northern Manitoba
RCMP say they made two significant drug arrests in northern Manitoba this week. The north district Crime Reduction Enforcement Support Team, along with RCMP emergency response and police dog services, busted up two alleged drug operations in Grand Rapids on Friday and another in Chemawawin the following day. Winnipeg Sun

Man convicted in 2011 shooting death, disappearance of Cold Lake man
A 30-year-old man has pleaded guilty in the shooting death of a Cold Lake man almost six years ago. Tyler Arsenault of Cold Lake received a 23-month conditional sentence and a 10-year firearms prohibition Monday after pleading guilty in Court of Queen's Bench in St. Paul to careless handling of a firearm and offering an indignity to human remains, RCMP said in a news release. The victim, Dennis Cardinal, 40, was reported missing by friends and family to Cold Lake RCMP in December 2011 after having allegedly not been seen since Christmas 2010. An initial investigation was unable to locate him or explain his disappearance. Edmonton Journal

Two from Red Deer charged after allegedly trying to flee checkstop
A man and woman face criminal charges after allegedly fleeing an RCMP checkstop in a stolen vehicle and causing a serious injury collision in Red Deer on Saturday. As well over the weekend, RCMP charged eight impaired drivers during weekend checkstops and roving patrols. Red Deer Advocate; CBC News

N.B. RCMP investigating after firearms stolen from Canadian Tire
The RCMP are searching for a suspect, or suspects, after a number of firearms were stolen from a Canadian Tire in Riverview, N.B. Police say one or more individuals broke into the Pinewood Road store around 5:10 a.m. Saturday, causing damage to the main door. CTV News

Yukon RCMP has a new commanding officer
Scott Sheppard, a 27-year veteran with the RCMP, has taken over as head of Yukon's police force. The territorial government made the announcement Tuesday. CBC News

Cougars & Prince George RCMP team up to engage local youth
The Prince George RCMP are excited to announce a partnership with the Prince George Cougars Hockey Club. The Prince George Cougars will be providing police officers from the local Detachment with hockey cards to give out to youth in our community. WHL; Prince George Citizen

Toy drive continues at White Rock RCMP
The first of two three-hour efforts organized by White Rock RCMP to collect toys for the Salvation Army all-but-filled a police cruiser Sunday. "We loaded the back seat up to the ceiling and the front passenger seat," Const. Chantal Sears told Peace Arch News of the afternoon toy drive at Central Plaza. Peace Arch News

Police union head remains troubled by modest budget bump
Officials with the Winnipeg Police and police board are dismissing union concerns that a small percentage increase in the police budget for next year will result in longer wait times for 911 calls. Maurice Sabourin, president of the Winnipeg Police Association, told reporters Tuesday he remains troubled by the 1.3 per cent increase in the police budget for 2017. Winnipeg Free Press

Un Winnipegois accusé de pornographie juvénile
Le Service de police de Winnipeg a procédé à l'arrestation mardi d'un Winnipegois de 59 ans. Il fait face à des accusations de possession et de distribution de matériel de pornographie juvénile. Les policiers, qui ont mené une perquisition en octobre dernier, ont saisi du matériel informatique pour analyse. Des centaines de vidéos et des milliers d'images de pornographie juvéniles ont été récupérées. Radio-Canada ; CBC News

Ottawa's crybaby cops
An editorial states, "My, what a fragile, sensitive lot some Ottawa police are. When the deputy chief recently suggested there were patrol officers not pulling their weight, several took offence at her phrasing. One inspector described it as "shocking." What could have so dismayed the hardened men and women who take down criminals, help quell unruly protests and regularly interact with low-life scum? The offensive vocabulary, it turns out, consisted of the phrase "canine fornicators" - a euphemism uttered by Deputy Chief Jill Skinner during a November talk to frontline officers..." Ottawa Citizen

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Inmate serving indeterminate sentence for murder dies at Regional Psychiatric Centre
A 65-year-old inmate serving an indeterminate sentence for second-degree murder died in custody at the Regional Psychiatric Centre on Sunday. According to assistant warden Tim Krause, Xavier Batoche was receiving palliative care. According to a news release issued Tuesday by Correctional Service Canada, Batoche was also serving time for impaired driving, driving while disqualified and obstructing a peace officer. He began serving his sentence in March 1985. StarPhoenix; CBC News

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

City of Surrey and Surrey RCMP launch City Centre Response Plan
The City of Surrey and Surrey RCMP have launched their City Centre Response Plan to address the public safety and public health concerns for both the homeless and the community in the 135A area. The plan will address three key areas: 1. Enhanced Outreach and Presence on 135A. 2. Emergency Housing. 3. Engagement and Education. "As is the case with all municipalities in the region, Surrey is facing increased challenges related to homelessness, mental health issues and fentanyl use," said Surrey

Mayor Linda Hepner. "With the City Centre Response Plan, we are taking tangible, concrete action on addressing the public safety issues that area businesses and residents are faced with on a regular basis, while addressing the public health challenges that affect the vulnerable who are easily preyed upon and exploited." Voice Online; CKNW NEWS AM 980

Violence against women has touched us all, Wynne says on anniversary of Montreal Massacre
Ontario Premier Kathleen Wynne placed roses in a vase at a ceremony in Toronto in memory of 14 women killed in Montreal 27 years ago. Wynne, along with Toronto Mayor John Tory, spoke at Women's College Hospital about the deaths at l'École Polytechnique on Dec. 6 in 1989. On this day in 1989, 14 women were shot and killed at the engineering school by a gunman professing to hate feminists. CBC News

'We have to keep reminding people:' Montreal Massacre remembered in Charlottetown
Islanders gathered Tuesday to remember the victims of the Montreal Massacre 27 years ago and to renew calls for an end to violence against women. Dec. 6 is the anniversary of the 1989 massacre at École Polytechnique in Montreal in which 14 female students were gunned down because they were women. CBC News

Halifax remembers Montreal's École Polytechnique victims
Red human-sized silhouettes of two Nova Scotia murdered women stood before a mostly female crowd who gathered in downtown Halifax Tuesday to remember the 14 women killed at Montreal's École Polytechnique 27 years ago. Doreen Bernard, a Mi'kmaq elder from the Sipekne'katik First Nation, prayed for the women's families and for missing and murdered Indigenous women, men and children across Canada. CBC News

Restorative Justice program success continues
Volunteers in Williams Lake have been facilitating restorative justice for almost 20 years. Getting its start in 1997 as a response to Williams Lake being the auto theft capital of Canada, the local committee has grown from a handful of volunteers to fluctuating between 35 and 45 active volunteers handling almost 50 files a year. In November, the group invited guests to its monthly meeting held at the Pioneer Complex, including some of the people responsible for starting the program. One of those original members was retired RCMP officer Jacques Drisdale who was trained in restorative justice with the RCMP in eastern Canada. Williams Lake Tribune

Opioid crisis wearing officers down
Police will have to train additional officers for its clandestine drug-lab team to prevent burnout from dealing with the growing opioid-overdose problem. The Winnipeg Police Board heard Tuesday about the strain on resources stemming from the often-deadly consequences of people abusing fentanyl and other opioids. Following the meeting, police chief Danny Smyth told reporters he was concerned there aren't enough members on the drug lab team. Winnipeg Free Press

La police recherche des témoins d'un crime haineux
La police d'Edmonton recherche un homme qui aurait approché deux femmes portant un hidjab avec un noeud coulant, en leur disant « C'est pour vous ». L'incident s'est produit vers 20 h 30, le 8 novembre, à la station de l'Université de l'Alberta du service de train léger sur rails. Radio-Canada

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Broadcast Media / Médias télédiffusés :

CBC News Network's Power & Politics discussed the inquiry into Missing and Murdered Indigenous Women with Minister of Indigenous and Northern Affairs Canada, Carolyn Bennett. Rough Transcript

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

NIL

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

NIL

INTERNATIONAL

Powerful 6.8-magnitude earthquake strikes off the coast of Indonesia
An earthquake with a magnitude of 6.8 has struck 130km southeast of Banda Aceh in northern Sumatra, Indonesia, the United States Geological Survey says. No tsunami warning was immediately issued and the extent of the damage caused is as yet unclear. The quake struck at a depth of 33 kilometres at 5.03am local time (9.03am AEST), the USGS said. Daily Mail UK

Read the Full Transcript of President Obama's National Security Speech
President Obama gave what is expected to be the final national security speech of his tenure on Tuesday, discussing his administration's accomplishments in spheres like battling al Qaeda and killing Osama bin Laden, as well as counterterrorism recommendations for the ongoing struggle against ISIS and other extremist groups. Time

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

RalphGoodale
On Parliament Hill with @JustinTrudeau & Cabinet remembering the 14 precious lives lost on this day in 1989 #ActionsMatter

RalphGoodale
Sur la colline avec @JustinTrudeau et le cabinet aujourd'hui, on se souvient des 14 vies précieuses perdues ce jour en 1989.

Ralph Goodale
Le message que j'ai envoyé à tous les employés dans mon portefeuille de sécurité publique: https://www.securitepublique.gc.ca/cnt/bt/lttr-mnstr-20161206-fr.aspx …

Ralph Goodale
The message I sent today to everyone working in my PS portfolio: https://www.publicsafety.gc.ca/cnt/bt/lttr-mnstr-20161206-en.aspx … #ActionsMatter

UkrEmb_inCanada
Ministers @RalphGoodale and @AvakovArsen discussed future and current cooperation. #Canada is ready to assist #Ukraine in further reforms.

YWCARegina
Are we making progress on #VAW, gun control? Maybe, maybe not. #notokay @RalphGoodale

Polysesouvient
Call on @JustinTrudeau & @RalphGoodale to Fulfill Election Promise to Strengthen Gun Control goo.gl/6T6vbb #cdnpoli #December6

Polysesouvient
Demandez à @JustinTrudeau & @RalphGoodale de remplir promesse électorale de renforcer contrôle des armes goo.gl/Hs9rnq #6décembre

DanBrienPS
@JustinTrudeau, @RalphGoodale, & cabinet. Remembering December 6, 1989 / En souvenir du 6 décembre 1989.

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

nationalpost
Liberals to announce $3-billion search and rescue aircraft contract — Airbus named as winner natpo.st/2hfclrO pic.twitter.com/VGgp53NPgH

ChilliwackTimes
Thousands of pounds of food collected in two hours by Chilliwack emergency responders @ChilliwackSAR ow.ly/7byx306SinI

NATIONAL SECURITY / SÉCURITÉ NATIONALE

JimBronskill
Spies should not be allowed to keep innocent people's data, privacy czars say metronews.ca/news/canada/20... #cdnpoli #hw

CKOMNews
Spies should not be allowed to keep innocent people's data, privacy czars say. ow.ly/gLF3306SqeP #ckom

CBCTechSci
Privacy watchdogs urge caution with encryption laws ift.tt/2he5013 pic.twitter.com/82op8B1cHD

VincentBP
Surveillance: les commissaires à la vie privée demandent à Ottawa un meilleur encadrement des forces policières lapresse.ca/actualites/nat...

PnPCBC
.@PrivacyPrivee Daniel Therrien says no new police powers needed & more oversight needed to protect privacy.

ipoliticsca
Police haven't made case for more digital spying powers. Our @amandacconn reports. ipoli.ca/2hel07i #cdnpoli pic.twitter.com/9MLKdgciwy

nationalpost
RT @StewartBellNP: 'He's been freed, thank God,' says mother of Canadian veteran detained in Iraq after fighting ISIL. https://t.co/4A44G9b…

CBCMontreal
RCMP officers copied contents of Ismael Habib's laptop in 2014 ift.tt/2gOh3VY pic.twitter.com/8kAltV75ft

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

BlackburnSarnia
The strike by 47 employees at the Blue Water Bridge, now into its third week, was raised in the House of Commons Mon blackburnnews.com/sarnia/sarnia-...

CYBER SECURITY / CYBERSÉCURITÉ

PACC_CCAP
It gets better: Demographic info is optional; but opinions will only be counted if demographic details are divulged ipolitics.ca/2016/12/06/myd… twitter.com/Water_Steve/st…

LAW ENFORCEMENT / APPLICATION DE LA LOI

VICE
RT @vicecanada: A look at Canada's 12 most wanted fugitives: bit.ly/2gOTQD8 pic.twitter.com/vaYFf2tmdL

MiyoungLeeCBC
No charges approved after RCMP investigation into death of aboriginal teen Paige Gauchier ift.tt/2h4kica #CBC

RedDeerAdvocate
Two arrested after fleeing #reddeer checkstop, crashing into and injuring another driver reddeeradvocate.com/news/two-from-…

CBCNorth
Yukon RCMP has a new commanding officer ift.tt/2gPlJuN pic.twitter.com/WExs0hXXTd

icimanitoba
Un Winnipegois accusé de pornographie juvénile rc.ca/MqN1sz

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

TheStarPhoenix
Inmate serving indeterminate sentence for murder at Regional Psychiatric Centre dies ebx.sh/2gO9GNY pic.twitter.com/c9Q6YGqEjD

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Femmes_Canada
Se conscientiser. Se souvenir. S'engager. Vos #GestesComptent ow.ly/ScpR306wht0 pic.twitter.com/RSDWaps6li

CBCToronto
Violence against women has touched us all, Wynne says on anniversary of Montreal Massacre bit.ly/2h3iTQV #december6 pic.twitter.com/43MEOfxk49

CBCPEI
'We have to keep reminding people:' Montreal Massacre remembered in Charlottetown ift.tt/2hem9HY #pei pic.twitter.com/TyZM6wnLeT

CBCNS
Halifax remembers Montreal's École Polytechnique victims ift.tt/2g78vdr pic.twitter.com/pFXVilrTea

icialberta
La police recherche des témoins d'un crime haineux rc.ca/MqMkcN

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

PnPCBC
.@Carolyn_Bennett says gov't could have done better job anticipating 'latent' period getting MMIW inquiry underway.

OTHER / AUTRE

CBCPolitics
Trudeau cabinet expected to debate renewed Ukraine mission ift.tt/2gNKild #hw #cdnpoli pic.twitter.com/DjQES5HTso

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

Today's News / Actualités
December 9, 2016 / le 9 décembre 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

No concrete timeline for prison farm decision
Kingston and the Islands MP Mark Gerretsen told members of the Prison Farm Co-op last night that he has no news for them yet on the possible return of the farms. "I was really hoping to hear from the **minister's office** on what their decision was prior to the holidays, but they informed me two or three weeks ago they wouldn't have a decision before then," Gerretsen told the Whig-Standard on Friday afternoon before heading to the meeting. The decision on whether to reopen the prison farms rests with **Public Safety Minister Ralph Goodale**..."My intention tonight is to update everybody as to what I've done over the last year with respect to it, just to make sure I've been continuing to talk to **the minister**

and his office about the next steps," Gerretsen said. "And we're going to make sure the public consultation and information that was received from it is respected and utilized to make a decision."... Last month, Correctional Service Canada released a report from a survey on its website gauging Canadians' opinion on reopening the farms in some form or another... "My understanding, from what I've been told by **the minister's office**, is that they are currently reviewing the findings," Gerretsen said. Gerretsen said he doesn't have a timeline on a decision from **the minister's office**. "Not that I haven't been asking," he said. "I've been continually asking **the minister's office** for an update, but I haven't received anything to date."... Gerretsen said the challenge will be to combine the prison farm co-op plans along with plans from CSC and the **minister's office.** Whig-Standard

TOP STORIES / MANCHETTES

Ismael Habib a-t-il dit aux agents d'infiltration ce qu'ils voulaient entendre?
La Couronne a terminé sa preuve au procès du présumé sympathisant djihadiste Ismael Habib, à Montréal. L'avocat de la défense a tenté de soulever des doutes au sujet de la crédibilité de l'opération d'infiltration menée par la police. Habib aurait-il tout fait pour plaire aux agents d'infiltration afin qu'ils l'aident à retrouver sa famille? Pendant près de six mois avant son arrestation en février dernier, Habib était entouré de policiers de la Gendarmerie royale du Canada (GRC) qui formaient une fausse organisation criminelle. Le dernier témoin du ministère public était le cerveau qui élaborait les scénarios d'infiltration au sein de la GRC. En tant qu'agent couvreur, c'est lui qui donnait des directives aux agents d'infiltration. Il a expliqué que pendant l'opération, la police pouvait compter sur l'aide d'un « agent civil », un commerçant prénommé Lyes qui avait la confiance d'Ismael Habib. Radio Canada ; CBC News

Border agent charged in smuggling tobacco probe at Peace Bridge
The RCMP says a Canada Border Services Agency officer has been charged in a smuggling investigation. The Mounties say the arrest came as part of a joint forces investigation that focused on a criminal organization that was allegedly smuggling truckloads of contraband tobacco into Canada from the United States. They allege the group's smuggling activities were facilitated by a CBSA border services officer working at the Peace Bridge in Fort Erie, Ont. Investigators say arrests and seizures were made simultaneously in Canada and the U.S. but gave no other details. Police say 37-year-old Chad Gale of Welland, Ont. is charged with breach of trust by a public officer. CBSA southern Ontario regional director Rick Comerford called it a very serious matter. "It is an isolated incident and in no way reflects the integrity and professionalism of the thousands of dedicated CBSA officers who carry out their duties each day in an exemplary manner," Comerford added. Canadian Press (CP24, Globe and Mail, CTV News, Global News, Metro News, Toronto Star); CHCH

Investigation clears Alberta RCMP officers of any wrongdoing in shooting death
An investigation has cleared Morinville RCMP officers of any wrongdoing in the 2015 shooting death of a man with a "history of significant mental illness and conflict with the law." In a detailed report released Friday, the Alberta Serious Incident Response Team found the officers involved were "acting lawfully and the use of force was reasonable and justified in all the circumstances." Edmonton Journal; AM 630 CHED; CBC News

Lawyers, judge concerned about RCMP's handling of video evidence
A Yukon territorial judge has raised concerns over the RCMP's handling of video evidence. Judge Michael Cozens acquitted John Lavallee of impaired driving on Nov. 2 but criticized the RCMP for losing the video from the police cruiser's onboard camera. "The preservation of police audio and video recordings is of great assistance to a court in determining the actual circumstances of an arrest or the nature of any interaction between an accused person and the police," Cozens wrote. Yukon News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

UPDATE: Winnipeg company 'ecstatic,' intends to maintain new search-and-rescue planes in city
A multibillion-dollar deal to purchase a new fleet of search-and-rescue planes will likely see a maintenance hub created in Winnipeg. On Thursday morning, the federal government announced it is purchasing 16 Airbus C-295W planes. The $4.7-billion deal also includes the creation of a training centre in British Columbia and includes a subcontract with PAL Aerospace, a company owned by Winnipeg's Exchange Income Corporation, to help with maintaining the new fleet. CBC News; Bloomberg News (Calgary Herald)

$4M boost for Coast Guard headquarters in St. John's
The Canadian Coast Guard Atlantic headquarters in St. John's is getting $4 million in federal cash for upgrades. The work includes removing sediment near the dock to create deeper water, so Coast Guard's larger vessels can use the wharf adjacent to the headquarters. CBC News

B.C. gives OK to drone pilot project for search and rescue in two communities
Drones will be used by search-and-rescue crews in two communities in British Columbia as part of a one-year pilot project. The drones will be used in Coquitlam and Kamloops with the blessing of Emergency Management B.C. Canadian Press (Vancouver Sun)

EMO meets with Sydney homeowners to discuss disaster relief details
Owners of 18 Sydney homes deemed uninhabitable after the Thanksgiving Day floods are in the process of learning what compensation they will receive from the province. On Thursday, the homeowners began individual meetings with officials from the Nova Scotia Emergency Management Office at a downtown Sydney hotel. Cape Breton Post

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Ismael Habib a-t-il dit aux agents d'infiltration ce qu'ils voulaient entendre?
La Couronne a terminé sa preuve au procès du présumé sympathisant djihadiste Ismael Habib, à Montréal. L'avocat de la défense a tenté de soulever des doutes au sujet de la crédibilité de l'opération d'infiltration menée par la police. Habib aurait-il tout fait pour plaire aux agents d'infiltration afin qu'ils l'aident à retrouver sa famille? Pendant près de six mois avant son arrestation en février dernier, Habib était entouré de policiers de la Gendarmerie royale du Canada (GRC) qui formaient une fausse organisation criminelle. Le dernier témoin du ministère public était le cerveau qui élaborait les scénarios d'infiltration au sein de la GRC. En tant qu'agent couvreur, c'est lui qui donnait des directives aux agents d'infiltration. Il a expliqué que pendant l'opération, la police pouvait compter sur l'aide d'un « agent civil », un commerçant prénommé Lyes qui avait la confiance d'Ismael Habib. Radio Canada ; CBC News

Trudeau must face facts on Iranian regime
An opinion piece states, "The Trudeau government is quietly working to strike a deal with the Islamic Republic of Iran. After becoming Prime Minister, Trudeau lifted virtually all economic sanctions against Iran. During the UN General Assembly meeting in September, Foreign Affairs Minister Stephane Dion met with regime officials to discuss the status of Canada-Iran relations... Besides the safety of our diplomats, there are many other reasons why Canada cut ties with Iran. Its elite military unit – the Iranian Revolutionary Guards Corp – is listed as a terrorist entity under Canada's Criminal Code. Iran openly funds and trains other terrorist groups, including Hamas, Hezbollah and the Taliban..." Toronto Sun

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Border agent charged in smuggling tobacco probe at Peace Bridge
The RCMP says a Canada Border Services Agency officer has been charged in a smuggling investigation. The Mounties say the arrest came as part of a joint forces investigation that focused on a criminal organization that was allegedly smuggling truckloads of contraband tobacco into Canada from the United States. They allege the group's smuggling activities were facilitated by a CBSA border services officer working at the Peace Bridge in Fort Erie, Ont. Investigators say arrests and seizures were made simultaneously in Canada and the U.S. but gave no other details. Police say 37-year-old Chad Gale of Welland, Ont. is charged with breach of trust by a public officer. CBSA southern Ontario regional director Rick Comerford called it a very serious matter. "It is an isolated incident and in no way reflects the integrity and professionalism of the thousands of dedicated CBSA officers who carry out their duties each day in an exemplary manner," Comerford added. Canadian Press (CP24, Globe and Mail, CTV News, Global News, Metro News, Toronto Star); CHCH

Ambassador Bridge company responds to Supreme Court decision
The Ambassador Bridge company says it's looking forward to resolving a dispute with the City of Windsor over the fate of several dozen rotting homes on the city's west end. The company was responding to Thursday's Supreme Court of Canada decision, siding with the municipality over the issue of jurisdiction. The court ruled that the issue should be heard in Windsor's superior court, rather than federal court, where the bridge wanted the matter decided. Windsor Star

Asbestos ban to be announced by federal government next week
The federal government plans to announce a comprehensive ban on asbestos in Canada next week, CBC News has learned. The country currently allows imports of construction products and automotive parts that contain the toxic fibre, even though Canada no longer exports the material. CBC News

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

Investigation clears Alberta RCMP officers of any wrongdoing in shooting death
An investigation has cleared Morinville RCMP officers of any wrongdoing in the 2015 shooting death of a man with a "history of significant mental illness and conflict with the law." In a detailed report released Friday, the Alberta Serious Incident Response Team found the officers involved were "acting lawfully and the use of force was reasonable and justified in all the circumstances." Edmonton Journal; AM 630 CHED; CBC News

Dead man left police no choice, final witnesses tell inquest
An inquest into the 2008 police shooting death of an indigenous man in Winnipeg - the first in Manitoba to specifically consider the role of racism - heard from its final witnesses Friday. Two officers responsible for use-of-force training with the Winnipeg Police Service and the RCMP said the police who shot Craig McDougall acted appropriately and that bias-free police training wouldn't have changed the outcome. Winnipeg Free Press

Widow of slain Mountie makes plea for Wynn's Law
The widow of murdered St. Albert RCMP Const. David Wynn vowed Friday to "fight a lifetime" to see a bail-reform bill become law. "I will fight a lifetime for this to pass if I have to," Shelly MacInnis-Wynn told a news conference organized by St. Albert-Edmonton MP Michael Cooper. CBC News

RCMP investigation of Winnipeg police HQ remains active
The RCMP investigation into Winnipeg's police headquarters remains active as the two-year anniversary of the criminal probe approaches. Winnipeg Mayor Brian Bowman said the Mounties recently contacted the city to request additional information pertaining to their investigation of the $214-million police-HQ project, which was completed this summer after three years of delays, $79 million worth of cost overruns and two external audits. CBC News

Time to saddle up: A new graduate for the RCMP's Musical Ride talks about horses, tradition and Canada's 150th birthday
The RCMP Musical Ride held its graduation ceremony, known as "Passing-Out," on Friday. Among the new graduates is Const. Mathieu Crousset, who says he's "very humbled to have this opportunity to represent the RCMP." The Musical Ride is based on cavalry drill movements. The riders and their horses are invited to perform at about 50 events a year in Canada and abroad. Last May, they performed at the Queen's 90th birthday celebrations. The equitation course, which teaches horsemanship, is the second-longest RCMP course, with only recruit training in Regina taking longer. As the newest graduates, these riders will be among the official riders in the Canada 150 tour. We asked Const. Crousset a few questions: Q: Tell us a little about yourself. A: I was born in Langley, B.C. I'm a second generation RCMP member and my father was posted in Surrey, B.C. Our family was transferred to Ottawa when I was a year old, and I grew up in Gatineau. Ottawa Citizen

Lawyers, judge concerned about RCMP's handling of video evidence
A Yukon territorial judge has raised concerns over the RCMP's handling of video evidence. Judge Michael Cozens acquitted John Lavallee of impaired driving on Nov. 2 but criticized the RCMP for losing the video from the police cruiser's onboard camera. "The preservation of police audio and video recordings is of great assistance to a court in determining the actual circumstances of an arrest or the nature of any interaction between an accused person and the police," Cozens wrote. Yukon News

RCMP renew call for help in cold case murder
RCMP are looking for the public's help for tips in the 2007 murder of a Portage la Prairie grandmother. Mounties renewed their plea Friday less than three weeks after issuing a press release asking for people to come forward with information in the 2007 death of Charlene Ward. Winnipeg Sun; CBC News

Drug ring shut down
A large drug ring, allegedly operating out of West Kelowna, has been shut down by RCMP. Following what police call a "significant" two-month investigation, RCMP say they gained enough information on the West Kelowna operation to indicate it had been supplying drug dealers and drug houses, primarily in Kelowna. Castanet.net; Global News

Red Deer woman charged in counterfeiting scheme
RCMP has laid charges against a Red Deer woman and is looking for another woman and a man in connection with a counterfeit cash scheme in Drumheller. In mid-November, police were called by a local business that a pair of women came into their store and bought a large amount of merchandise with counterfeit U.S. cash. CTV News

'Stuff the Cruiser' to collect donations for Christmas Amalgamated
Kamloops RCMP's annual 'Stuff the Cruiser' event takes place tomorrow. RCMP, BC Sheriffs and community volunteers will be at Walmart and Toys-R-Us between 10:00 a.m. and 3:00 p.m. collecting new toys and other items to go towards families in need this Christmas. CFJC Today

RCMP dog handler describes how he and his dog tracked suspect
An RCMP dog and his handler followed a scent that started near a Cornwall break-in to where the alleged "screencutter" parked his car, a judge heard Friday in provincial court. That was part of the testimony during the fourth day of Richard Joseph Arsenault's trial before Chief Judge Nancy Orr in Charlottetown. Charlottetown Guardian

Thieves use key to access mail in Surrey townhouse complex
While mail theft is a common problem across Metro Vancouver, you don't usually see perpetrators casually opening up mailboxes with a key. But that's exactly what happened Saturday morning at a townhouse complex in Surrey, where two suspects managed to make off with a veritable Santa's sack of stolen mail. Fortunately, the entire thing was caught on the complex's surveillance camera... The RCMP said it is investigating the theft, and that officers already have a pair of suspects in mind. No one has been arrested yet, however, and no charges have been laid. Canada Post also confirmed its security team is working with Mounties on their investigation, but the agency would not comment further. CTV News

Cinq suspects arrêtés dans deux opérations anti-tabac
Deux opérations policières visant des présumés contrebandiers de tabac ont permis l'arrestation de cinq suspects, mercredi, en Montérégie. Dans un premier temps, à Saint-Anicet, les policiers ont arrêté trois hommes et une femme, âgés de 20 à 25 ans, soupçonnés de faire partie d'un réseau de contrebande de tabac opérant dans le secteur. La perquisition menée au cours de la journée a permis la saisie de plus de 1,2 tonne de tabac en vrac... L'opération, à laquelle participaient la Sûreté du Québec et la Gendarmerie royale du Canada, a été rendue possible grâce à des informations fournies par le public. La journée de mercredi a donné lieu à une deuxième opération policière en matière de tabac illégal. Agence QMI (TVA Nouvelles)

Indigenous Val-d'Or residents face racial profiling, systemic discrimination, study suggests
A report released today suggests that police in Val-d'Or are racially profiling Indigenous people. Researchers Céline Bellot from l'Université de Montréal and Marie-Eve Sylvestre from the University of Ottawa conducted the study. They looked at how law enforcement and homelessness intersect in the city 600 kilometres northwest of Montreal. CBC News

Peel police chief subject of $21M lawsuit alleging interference
CityNews has learned Peel Regional Police Chief Jennifer Evans has been named in a $21-million lawsuit alleging interference in a controversial police shooting. In March 2015, Peel police responded to a neighbour dispute in Mississauga. A suspect was shot and killed. But a stray police bullet hit an innocent woman in the back as she was standing in her kitchen. 680 News

Beanbag bullets the latest crime-fighting tool in Amherstburg
Amherstburg police is the first in Ontario to introduce the "sock gun" to all its officers. The latest crime-fighting tool fires beanbag-type bullets designed for use when someone is out of reach of a Taser. CBC News

Saskatoon teacher Rhett Lundgren facing child porn, child sex charges after police investigation
A 39-year-old teacher at a Saskatoon high school is facing child pornography charges following an investigation by the Saskatchewan Internet Child Exploitation unit. Rhett Jeffrey Lundgren, 39, has been charged with two counts of arranging to commit a sexual offence against a child and one count of attempting to access child pornography, Saskatoon police announced Friday. Lundgren appeared Friday in Saskatoon provincial court, where he was released on several conditions. StarPhoenix

Jonathan Bettez surveillé sans relâche par la SQ au cours de la dernière année
Jonathan Bettez a été traqué, littéralement, par les policiers de la Sûreté du Québec, dans l'année précédant son arrestation du 29 août dernier. Une surveillance qui s'est intensifiée à partir du 11 décembre 2015. Quelques jours plus tard, les policiers ont installé un dispositif sur son véhicule, un Infiniti G35, leur permettant de suivre ses allées et venues durant plus de sept mois. C'est ce qu'a pu apprendre Radio-Canada dans les dénonciations des policiers de la SQ, qui ont servi à son arrestation, le 29 août dernier. Il fait face à 6 chefs d'accusations de possession et de distribution de pornographie juvénile. Radio Canada; La Presse

London Police - Carding Q&A with Chief John Pare
Ontario is banning carding as it's now practised. London politicians want it scrapped entirely. London police disagree. As new rules on carding begin Jan. 1, police Chief John Pare weighs in on the

crackdown on randomly stopping and questioning people not under investigation. Jennifer O'Brien sat down with the chief. Police board chair Jeanette Eberhard was also there and spoke to some of the issues. London Free Press

Boy, 16, arrested after online threat puts 50 Ontario schools into 'hold and secure'
Provincial police have arrested a 16-year-old boy after a threat was made via Twitter on Friday morning involving the Trillium Lakelands District School Board in central Ontario. As a result, all Trillium Lakelands schools – both elementary and secondary – in Kawartha Lakes, Haliburton County, and Muskoka were put into a hold and secure… The hold and secure was lifted at the approximately 50 schools after about two hours. Canadian Press (Global News)

Avant d'offrir un drone à Noël, quelques précautions s'imposent
L'utilisation de drones doit s'entourer de règles élémentaires de sécurité et les responsables de l'aviation civile internationale ont mis en garde vendredi les parents avant qu'ils ne déposent leur cadeau au pied du sapin de Noël. Faire voler un drone «peut constituer une menace» à la fois pour les avions ou les hélicoptères en vol, mais surtout pour les personnes ou les biens au sol, a rappelé l'Organisation de l'aviation civile internationale (OACI), basée à Montréal. Agence France-Presse (Journal de Montréal, Journal de Québec)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Lockdown continues at Grand Valley Institution with ongoing contraband search
Family visits to the Grand Valley Institution for Women may be cancelled this weekend as corrections staff continue to search the facility for contraband. The institution was locked down at 11:30 a.m. Wednesday and visits were suspended at that time. CBC News

Jacques Delisle: la défense complète sa plaidoirie
Les avocats de Jacques Delisle ont exhorté le juge Benoit Moulin de libérer leur client, un homme qui a perdu «son honneur, sa réputation, sa liberté» après avoir passé quatre ans emprisonné dans une «cage de verre sous prétexte que la preuve de la Couronne ne soulevait aucun doute et qu'on devait la croire». Les plaidoiries se sont entamées vendredi à l'enquête sur cautionnement de l'ex-juge Jacques Delisle, qui tente de retrouver sa liberté le temps que la ministre fédérale de la Justice détermine s'il a été condamné à tort ou non pour le meurtre prémédité de son épouse. Agence QMI (TVA Nouvelles)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Recovering opioid addict pushes province to reconsider detox in Nova Scotia
After being in and out of detox programs multiple times, Danielle Noade says she didn't stop injecting drugs until she went to jail six months ago. Noade, 24, says the confines of a locked cell at the Central Nova Correctional Facility in Dartmouth, N.S., forced her to decide it was finally time to focus on recovery. CBC News

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Trudeau still faces huge challenges if he wants to help indigenous Canadians
An editorial states, "The Kitigan Zibi Anishinabeg Algonquin band in West Quebec has filed suit against the federal and Ontario governments and the National Capital Commission over title to the land that includes the Parliament buildings and LeBreton Flats. It's the latest challenge facing Prime Minister Justin Trudeau as he works to improve the lot of indigenous Canadians… Consider the forest of pledges he made even before winning office: fixing chronic underfunding of education; preserving languages and

cultures; rebuilding schools; launching a public inquiry into murdered and missing indigenous women, enacting all 94 recommendation of the Truth and Reconciliation Commission; renewing the "nation to nation" relationship. None of these carries easy fixes... Earlier this week, the prime minister explicitly promised an Indigenous Languages Act. And while there has been early grumbling, the Inquiry into Missing and Murdered Indigenous Women and Girls is underway..." Ottawa Citizen

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

NIL

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Montreal lawyers urge Ottawa to help asylum-seekers who housed Snowden
The lawyers have launched a Canadian organization named For the Refugees to raise money for the families and to lobby the Canadian government to give them sanctuary as they come under pressure in Hong Kong. Globe and Mail

INTERNATIONAL

ISIS leader linked to Charlie Hebdo attack killed in Syria airstrike: U.S. military
U.S. military officials say an Islamic State leader linked to the 2015 attacks at the French satirical newspaper Charlie Hebdo was killed in a U.S. airstrike in Syria. Officials say Boubaker el Hakim was killed in Raqqa on November 26. He is believed to have played a role in IS attack planning. The officials weren't authorized to discuss the strike publicly and spoke on condition of anonymity. Associated Press (Global News); Postmedia Network (Calgary Sun, Ottawa Sun, Edmonton Sun)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

ccrweb
Join @ccrweb in calling for an end to the #immigration detention of #children ccrweb.ca/en/detention-c… … #cdnpoli #cdnimm @RalphGoodale

itootill
Well @RalphGoodale, you know one thing that needs to be done for sure... scrap #C51

ihsaan
New counter-radicalization office head could be named before Christmas by @amandacconn http://ipolitics.ca/ via @iPoliticsca

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

CBCNL
NEW | $4M boost for Coast Guard headquarters in St. John's cbc.ca/1.3889413 pic.twitter.com/ylAsacOSIC

VancouverSun
B.C. gives OK to drone pilot project for search and rescue in two communities ebx.sh/2gKcOro pic.twitter.com/u0cB4XT7WQ

NATIONAL SECURITY / SÉCURITÉ NATIONALE

icimontreal
Ismael Habib a-t-il dit aux agents d'infiltration ce qu'ils voulaient entendre? rc.ca/Mrcjn8

cforcese
Amdmnts bill c-22 creating nat'l sec cmmttee of parl now reported to House. http://www.parl.gc.ca/ Vast expansion of access to info

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

MetroNewsCanada
RCMP charge border officer in Canada-US tobacco smuggling investigation ow.ly/dOHy306Z0yG

TheWindsorStar
Ambassador Bridge company responds to Supreme Court decision windsorstar.com/news/local-new… pic.twitter.com/724KFuLCvJ

LAW ENFORCEMENT / APPLICATION DE LA LOI

CBCManitoba
RCMP investigation of Winnipeg police HQ remains active ift.tt/2gmgMdR pic.twitter.com/qdMJEmXl7A

OttawaCitizen
A new graduate for the RCMP's Musical Ride talks about horses, tradition and Canada's 150th birthday ow.ly/XGxH306ZsMj

winnipegsun
RCMP renew call for help in cold case murder dlvr.it/MrcH5M

CBCEdmonton
Widow of slain Mountie makes plea for Wynn's Law cbc.ca/news/canada/ed… pic.twitter.com/cYlwWZVcpN

CBCAlerts
Less than 10% of Val D'Or, Quebec's population is Indigenous; study finds they got 76% of tickets issued by police. https://t.co/25g7XSAJMc

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

CBCKW891
Lockdown continues at Grand Valley Institution with ongoing contraband search ift.tt/2gJXmvp pic.twitter.com/RoBalzrEN8

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

CBCNS
Recovering opioid addict pushes province to reconsider detox in Nova Scotia ift.tt/2hv8Kvd pic.twitter.com/VvcWCJhGIm

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

APTNNews
"It was confirmed by the RCMP that we do have a national crisis… Aboriginal women are targeted…" #cndpoli
http://aptn.ca/news/?p=66928

PUBLIC SERVICE / FONCTION PUBLIQUE

OttawaCitizen
PIPSC union and federal government close in on deal https://t.co/80s5ul0Pkz

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

Today's News / Actualités
December 9, 2016 / le 9 décembre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

New counter-radicalization office head could be named before Christmas
The list of candidates to lead the government's new Office of Community Outreach and Counter-Radicalization is down to the final two, and an announcement naming the new head could be made before Christmas. ***"It's down to a shortlist of two and they're both excellent,"*** said **Public Safety Minister Ralph Goodale** in a scrum with reporters outside of the House of Commons public safety committee, where he spoke on supplementary estimates. "***It's very hard to make the choice. I'm hoping to make the announcement, if not before Christmas, then very early in the new year of this individual***." The creation of the new office, aimed at supporting community efforts to tackle radicalization,

formed part of the Liberals' 2015 campaign platform. In the 2016 budget, the Trudeau government earmarked $35 million over five years for the new office, with $3 million of that coming in its first year and ongoing funding of $10 million a year after that. But while the pledge earned praise from researchers and community advocates working on the front lines of counter-radicalization, few details have been made public about how the office will actually operate. **Goodale** shed some light on that before the committee Wednesday evening, saying that the government has been and will continue to deliver funding to counter-radicalization projects through an arm of the office called the Community Resilience Fund; a federal contribution to the recent UNESCO conference on radicalization held in Montreal this fall was the first grant approval through the fund. ***"That's the only initiative so far that's been taken,"*** said **Goodale**. ***"For the vast majority of the future funding I want to have the benefit of the Special Advisor that we are recruiting***." iPolitics

La liberté de presse, une valeur fondamentale!
Un article d'opinion par le député Matthew Dubé note, « En octobre dernier, La Presse a révélé que le journaliste Patrick Lagacé s'était fait surveiller par la police de Montréal. Ces révélations extrêmement troublantes nous rappellent que le gouvernement fédéral n'est pas sans blâme en ce qui concerne la surveillance des journalistes. En 2007, le journaliste de La Presse Joël-Denis Bellavance a été filé par la GRC. En effet, depuis 2003, une directive ministérielle fédérale demande aux forces policières de porter une « attention spéciale » au statut des médias dans le cadre d'enquêtes sur la sécurité nationale. Ces attaques à la liberté de presse s'ajoutent au cas du journaliste de Vice, Ben Makuch, qui risque la prison parce qu'il refuse de divulguer ses sources à la GRC. J'ai interpelé le ministre de la Sécurité publique, Ralph Goodale, à plusieurs reprises lors de la période des questions à Ottawa ainsi que dans le cadre d'une conférence de presse en partenariat avec la Canadian Journalists for Free Expression et les journalistes Ben Makuch, Mohamed Fahmy et Patrick Lagacé. » Chambly Matin

TOP STORIES / MANCHETTES

Canadian border worker charged with smuggling tobacco from the U.S.
A Canadian border worker at the Peace Bridge is charged with helping to smuggle tobacco from the U.S. The RCMP says he was caught during a joint forces investigation into contraband tobacco being brought into Canada by the truckload. Thirty-seven year-old Chad Gale of Welland has been charged with breach of trust. Others are under arrest but no names have been released. CHCH

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

North Shore Rescue urges outdoor adventurers to stay safe
Fresh snow has many outdoor adventurers looking lustily towards the North Shore mountains — but North Shore Rescue is urging people to stay safe if they attempt backcountry excursions. Mike Danks, coordinator of the volunteer-run operation says his team has been busy preparing, but has not yet been busy with calls, which is good news. CBC News

Search for missing Murray Harbour man scaled back
The search for a missing 68-year-old Murray Harbour, P.E.I., man who has been missing since Wednesday has been scaled back. Alan Richards's 2013 Ford Escape was located in the Cape Bear area of Kings County, where police, about 50 volunteers and helicopter from the Joint Rescue Coordination Centre in Halifax were searching on Thursday on the water and the shore. RCMP Cpl.
Alexis Triantafillou said the volunteers, with P.E.I. Ground Search and Rescue, have stopped their search. CBC News

Three new search and rescue aircraft coming to 14 Wing Greenwood
The federal government announced the purchase of 16 new search and rescue aircraft that will replace Canada's fleets of CC115 Buffalo and legacy CC130 Hercules aircraft… Of the 16 aircraft, three will be stationed at 14 Wing Greenwood. Three other aircraft will be going to each of the other three airforce bases in Canada – Trenton, Winnipeg and Comox – and an additional two new planes going to the

operational training unit in B.C. The final two planes will serve as "floaters," Fraser said, meaning they will backfill those aircraft when maintenance is required. Western Star; Norwester

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

RCMP paid for info from civilian source during Habib investigation
While investigating Ismael Habib in late 2015, the RCMP was paying a Montreal clothing store owner who was well-connected in the Muslim community to feed them information. The man was described as a practising Salafist, a strict interpretation of Islam, who operates a second-hand clothing store on Jean-Talon St. Montreal's Muslim community gravitated around the store, an RCMP officer testified at Habib's trial on Friday. The officer said the man, in his mid-40s, acted as a mentor to young Muslims in the city and was used to build trust between Habib and the undercover RCMP agents investigating him. Habib is on trial for trying to leave Canada to commit terrorist acts abroad and giving false information to obtain a passport. In late 2015, he was involved with several undercover RCMP agents pretending to be an underground crime ring capable of obtaining falsified passports and getting people out of the country by boats leaving from the Port of Montreal. On Friday, defence lawyer Charles Montpetit cross-examined an RCMP officer who oversaw the sting operation. e officer said the store owner wasn't technically part of the operation, but was paid every time he handed over information on Habib. Montpetit questioned whether the man had his own motives, given that he wasn't paid if he didn't have new information. Montreal Gazette

Quebec terror trial adjourned until Jan. 23 for Mr. Big arguments
The Crown has rested its case at the trial of a Quebecer charged with attempting to leave the country to participate in the activities of a terrorist group. Ismael Habib is also charged with giving false information in order to obtain a passport. The trial is now adjourned until Jan. 23, when lawyers will argue whether the judge should disregard some of the evidence. Habib's lawyer intends to challenge the admissibility of a confession extracted by undercover agents, suggesting it was obtained in a Mr. Big operation, in which officers pose as criminals. A Mountie who designed the elaborate scenarios involving the undercover agents was the final prosecution witness.

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Canadian border worker charged with smuggling tobacco from the U.S.
A Canadian border worker at the Peace Bridge is charged with helping to smuggle tobacco from the U.S. The RCMP says he was caught during a joint forces investigation into contraband tobacco being brought into Canada by the truckload. Thirty-seven year-old Chad Gale of Welland has been charged with breach of trust. Others are under arrest but no names have been released. CHCH

Suspect in 2010 Scarborough homicide located in Malaysia, returned to Toronto
A suspect in a 2010 vehicular homicide that occurred in Scarborough six years ago was recently located in Malaysia and has been brought back to Toronto to face a second-degree murder charge. On March 13, 2010 at 3:11 a.m., police said they were called to 1641 Pharmacy Avenue in Scarborough for a report of a fail to remain collision. Twenty-five-year-old Nanthi Eashan Dharmaratnam was pronounced dead at the scene. Investigators allege he was deliberated struck and killed by a man driving a car. A post-mortem investigation found Dharmaratnam died as a result of blunt head trauma and injuries to the torso. A warrant was issued for a suspect identified as Seran Kasilingam, 28. He was wanted for second-degree murder. It was believed at the time that he fled Canada. A video appeal for witnesses was released to the

public in Feb. 2016. On Aug. 26, authorities located the suspect in Kuala Lampur, Malaysia. RCMP and Canada Border Services agents made arrangements to return him to Toronto. CP24

Toronto Police seize $2.5 million in counterfeit goods as holiday season starts
As the holiday season approaches, Toronto Police are warning the public to be vigilant with their gift-giving after they seized $2.5 million in counterfeit goods. In the investigation, Project Lucky Chan, the police executed four search warrants around the city. The first warrant was executed at the main floor of a hotel, which happened to be hosting an international anti-counterfeiting conference, Det. Rob Whalen said in a news conference, Friday morning. (…) Hock Chan, 46, of Mississauga has been arrested and charged with one count of possessing property obtained by crime, possessing property obtained by crime with the purpose of trafficking, fraud over $5,000 and passing of wares. In addition, two illegal immigrants who were assisting in the sale of these products were arrested and detained by Canadian Border Services, investigators said. Toronto Star

DNA barcoding could help end food fraud
Eating bread with eggs, butter or jam for breakfast is a ritual at Ryerson student Monica Mejia's household. But her four-year-old nephew is gluten intolerant and can't join in. "Knowing that he won't be able to do that, it's heartbreaking," Mejia, a fourth-year global management student and volunteer at Ryerson's Good Food Centre, said. "So we have to find alternatives for him to replace that." (…) While CFIA sets the regulations and policies for imports, the Canada Border Services Agency (CBSA) shares the responsibility for enforcing them during their initial inspection of food, agricultural inputs and agricultural products at entry points. The Eyeopener

Striking Blue Water Bridge workers reach tentative deal
Workers at the Blue Water Bridge have reached a tentative deal with their employer after nearly three weeks of job action. Members of the Public Service Alliance of Canada walked off the job Nov. 21, saying the federal bridge corporation was trying to slash their benefits in the latest contract negotiations. Union officials representing the 47 workers said they reached the tentative agreement Thursday evening after a full day of talks. The union met with workers Friday morning to review the details of the proposed deal. CBC News

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Obama demande une enquête sur le piratage de l'élection présidentielle
Barack Obama a demandé aux agences américaines du renseignement d'ouvrir une enquête sur le piratage informatique et sur l'intervention de puissances étrangères dans le déroulement de la campagne présidentielle aux États-Unis cette année. Le président américain a souhaité qu'un rapport lui soit remis sur ce sujet avant qu'il quitte la Maison-Blanche le 20 janvier, a déclaré Lisa Monaco, conseillère à la sécurité intérieure, vendredi. Radio Canada; Agence France-Presse (La Presse); Politico

Canadian Cyber Threat Exchange ready to start membership push
After months of planning the country's first national IT threat service has issued its first threat report to a few early members and is ready to launch a campaign to expand its numbers, including lowering its fee for small businesses… Directors of the exchange come from some of the country's biggest enterprises including Air Canada, Bell Canada, Canadian National Railway, Manulife, Telus, TD Bank and Royal Bank. While many CISOs and infosec pros already get information from vendors, blogs and some threat data from vendors and services they subscribe to, the not-for-profit CCTX hopes to show value by tailoring reports and threat feeds for Canadian customers who don't want to know about the latest malware sweeping other parts of the world. The exchange also differs from other threat intelligence groups set up by industry associations and limited to verticals such as the healthcare or financial sectors by having a broad audience. The cross-industry appeal of the exchange has drawn the admiration of Rick Howard, chief security office of Palo Alto Networks, who was one of the keynote speakers at Wednesday's symposium and who believes the CCTX is the first national threat exchange in the world. IT World Canada

Ransomware Jumps Threefold in 2016
Ransomware attacks on businesses grew threefold this year to reach one every 40 seconds by October, according to new data from Kaspersky Lab. The Russian AV firm claimed that attacks came once every two minutes at the start of the year. For individuals it was even worse, with Kaspersky Lab calculating one attack every 10 seconds by Q3, up from once every 20 seconds at the beginning of the year. Some 20% of organizations worldwide suffered an IT incident as the result of a ransomware infection this year, and the same percentage of small businesses never got their files back even after paying up. That chimes with separate research from Trend Micro from earlier this year which claimed that one in five UK firms it polled were left without a decryption key after they paid the ransom. While Kaspersky Lab was at pains to point out there's no such thing as a low-risk sector, education was worst hit, accounting for 23% of all attacks, while retail and leisure (16%) was least affected. Infosecurity Magazine

Yahoo fixes flaw allowing an attacker to read any user's emails
Yahoo has fixed a severe security vulnerability in its consumer email service that could have allowed an attacker to read a victim's email inbox. The cross-site scripting (XSS) attack only required a victim to view an email in Yahoo Mail. The internet giant paid out $10,000 to security researcher Jouko Pynnonen for privately disclosing the flaw through the HackerOne bug bounty, In a write-up, Pynnonen said that the flaw was similar to last year's Yahoo Mail bug, which similarly let an attacker compromise a user's account. Yahoo filters HTML messages to ensure that malicious code won't make it through into the user's browser, but the researcher found that the filters didn't catch all of the malicious data attributes. He explained that sending a specially crafted email could have trigged malicious JavaScript to be immediately executed. Pynnonen said in an email that exploiting the flaw was "rather easy," but finding the bug was difficult. ZD Net; Security Week

US government seeks more data on Apple customers
Apple has seen a sharp year-over-year increase in the number US government demands for customer data. The company's first biannual report this year covers how many demands were made from global law enforcement and intelligence agencies -- including the US government -- for data it stores. Apple said it reviewed 4,822 demands for device data from US authorities, affecting 10,260 devices, an increase of 26 percent on the same period a year earlier. The company said that it was compelled to turn over data in over three-quarters of all cases. Additionally, the company received 1,363 demands from US authorities, the top requesting country, affecting 9,090 accounts. Apple turned over data in 84 percent of those cases. ZD Net

Government spies surveil phones in flight, report says
Turns out the skies are not so friendly after all, at least as far as privacy is concerned. American and British intelligence agencies have been surveilling cell phone use on commercial flights since 2005, according to a new investigation by Le Monde based on documents leaked by former NSA contractor Edward Snowden. As journalist and digital media teacher Dan Gillmor tweeted, it's "another good reason to use airplane mode when you're on the plane." But just turning on your phone when the plane is above 10,000 feet reveals your location to the NSA, according to 2010 internal NSA newsletter posted by Le Monde... Le Monde goes on to explain how the spy agencies can extract information like email addresses and Skype and Facebook ID data and then correlate it with flight and passenger data to pinpoint a particular user. They can also reportedly see what you're doing on your phone, be it looking through email or using a travel app. CNET; CSO Online; Le Monde

Russian cyberspies likely behind DNC breach move on to German election
A group of suspected Russian cyberspies blamed for interfering in the U.S. election is also attempting to influence the upcoming vote in Germany, according to the country's domestic intelligence agency. The Russian hacking group known as Fancy Bear or APT 28 has been targeting political parties in the country, Germany's Federal Office for the Protection of the Constitution (BfV) intelligence agency said in a statement Thursday posted online by Politico. The hacking activities have led to a surge in spear-phishing email attacks directed at German politicians, the agency said. CSO Online

Georgia Tech's $17 Million Rhamnousia Project and the Difficulty of Attribution

The Georgia Institute of Technology, Georgia Tech, has been awarded a $17.3 million contract to develop a scientific method for cyber attack attribution. Dubbed Rhamnousia after the ancient Greek spirit of divine retribution, the project will use machine learning (ML) technology to discover the groups behind different cyber-attacks. Security Week

How the Cyber Kangaroo can help defend the Internet of Things
What are Australia's policy options for responding to the internet threats of 2022? This question was explored in the 360° Cyber Game conducted jointly by RAND Corporation and the National Security College (NSC) at the Australian National University (ANU) in Canberra on Thursday. ZD Net

LAW ENFORCEMENT / APPLICATION DE LA LOI

From Standing Rock to Trans Mountain, dissent is in the pipeline
Melina Laboucan-Massimo, a Lubicon Cree, grew up in Alberta's oil country. Since the age of 7, she has joined blockades and protests aimed at protecting her community's traditional lands from resource development. "I was born into it," she said in an interview. "It's my inheritance." (…)Now, some indigenous leaders are pledging to use the tactics of Standing Rock to block the two pipeline projects approved last week by the Liberal government: the bitterly fought expansion of Kinder Morgan's line that runs to Vancouver Harbour, and Enbridge's lesser-noticed plan to rebuild and expand its Line 3, a main oil export line from Alberta to the U.S. Midwest. (…)Now, some indigenous leaders are pledging to use the tactics of Standing Rock to block the two pipeline projects approved last week by the Liberal government: the bitterly fought expansion of Kinder Morgan's line that runs to Vancouver Harbour, and Enbridge's lesser-noticed plan to rebuild and expand its Line 3, a main oil export line from Alberta to the U.S. Midwest. (…)At a symposium last month in Ottawa, security experts from government, law enforcement, industry and academia gathered to discuss "the challenges of dealing with natural-resource development projects and activism." Several speakers at the closed-door session spoke on emerging threats from the indigenous community. An RCMP document from 2015 tracked the aboriginal protest events – largely against natural-resource projects – and identified 313 individuals who had participated in them. Of those, 89 were judged to have some propensity toward criminality, and their names are being kept in a data base. "Some of these individuals advocate unlawful, and at times, violent protest tactics and techniques, yet there is no known evidence that these individuals pose a direct threat to critical infrastructure, the RCMP's "Project Sitka" report concluded. (…) "The situation at Standing Rock is going to be brought to a head and it's going to get real ugly," Mr. McConachy predicted. If he's right, Canada will be looking for new lessons to draw from the Sioux standoff. Globe and Mail

RISK IT OUT: Chronic understaffing a longstanding challenge at Vernon RCMP detachment
Chronic understaffing isn't a new problem for Vernon RCMP detachment — it has plagued the department for years, and it's not the only detachment facing the dilemma. Back in 2013, former Supt. Reg Burgess said the North Okanagan detachment, which includes Vernon and outlying communities, consistently faced 15 to 20 long term absences at any given time for the past several years. At the time, Burgess, who retired in 2015, said the detachment was operating with between 19 and 27 resources unable to perform duties at any given time. "This high percentage of non-operational resources often puts us short of the minimal resource levels in any of our areas resulting in excessive overtime, insufficient vacation time, compounded fatigue and stress which in turn contribute in part to our medical absences. Shortages affect sufficient developmental training time for members. They also significantly reduce our ability to conduct proactive policing such as undercover operations and high visibility random patrols," Burgess said in a report to Vernon councillors. Sources say those same issues continue to impact the detachment today, with chronic understaffing leaving some watches running short of the minimum manpower needed for officer safety. At times, watches are as low as three officers in the City of Vernon due to difficulty filling shifts, sources say, forcing remaining officers to 'risk it out' when they go on shift. InfoTel

Mounties ditch bodycam plans
Canada's Mounties might always get their man, but they're not going to be using body cameras to help their crime detection rates. The Royal Canadian Mounted Police (RCMP) said earlier this week that after

a feasibility study, it would hold fire on buying and deploying body cameras across 750 detachments "until such time as available technology can meet its specific operational requirements". While studies such as one carried out across some 2,000 police officers in the US and the UK by the University of Cambridge's Institute of Criminology have found that there's a sharp drop in the number of complaints against police – the Cambridge study said the drop was 93% – privacy campaigners have long disliked the trend for police officers to use body cameras. The Mounties seem mostly to be concerned about the quality of the tech and its fitness for purpose with the cameras they looked at, saying: "The RCMP needs to have confidence in the product and ensure that the choice of technology justifies the investment of taxpayers' money." However, they also noted the privacy issues, adding: "The RCMP will continue to work closely with the Office of the Privacy Commissioner to ensure privacy considerations are assessed when body worn cameras are deployed in operational settings." Naked Security

Calgary man wanted in organized crime bust surrenders to police
A man who was the subject of a Canada-wide warrant in connection with a major organized crime investigation has turned himself in to Calgary police. Andrew McGuire, 41, was one of 10 Calgarians implicated in the year-long probe that culminated late last month. The investigation by the Alberta Law Enforcement Response Teams (ALERT) netted 111 charges against the 10 men — related to drugs, firearms and organized crime. (…) The investigation involved the help of RCMP in Vernon and Sicamous, B.C. It also involved Public Prosecution Services Canada, Combined Forces Special Enforcement Unit British Columbia, Canada Border Services Agency, Criminal Intelligence Service Alberta, and Financial Transactions and Reports Analysis Centre. CBC News

Creep-catching crusade comes to Richmond
"We just want these creeps off the street." The leader of the Richmond and Vancouver chapter of Creep Hunters Canada, Brendon Brady, explained his group's motivation after they managed to lure a 36-year-old man to a McDonald's, where the suspect believed he was meeting a 15-year-old girl he'd been chatting with online. The confrontation and "catch" two weeks ago at McDonald's on Alderbridge Way was the group's first in Richmond and led to the man in question being arrested at the scene by the police for suspected child luring. Brady, 31, and a fellow Creep Hunter member handed over their online evidence and video footage to police at the scene and, according to Richmond RCMP, the man has been released on strict conditions while the police continues its investigation. (…) However, the RCMP also stated that it does not condone or recommend vigilantism. "Obtaining proper evidence required for this type of crime is very specific," said Richmond RCMP's Cpl. Dennis Hwang. "When individuals choose to bypass law enforcement to take matters in their own hands, investigations can be jeopardized, key evidence may become lost, and the individuals may jeopardize their personal safety and that of others." Richmond News

Hells Angel testifies he strung along police informant over cocaine shipment
A member of the Hells Angels says he never intended to ship cocaine from Ontario to Saskatoon but strung along a police informant because the man was his sole source of drugs for his back pain. Rob Allen, 36, testified Wednesday at his trial for cocaine trafficking, charges laid under the RCMP's Project Forseti, which saw 19 locations raided across Alberta and Saskatchewan. Noel Harder, the Crown's only witness in the case, has testified police instructed him to continue working on a plan to see Allen organize the movement of cocaine between the provinces. Allen testified that Harder pestered him constantly about using his contacts with Hells Angels in Ontario to get cocaine. Under questioning from the Crown, Allen insisted he never had any way of actually getting cocaine delivered to Saskatoon, but said he strung Harder along in order to avoid losing his source of OxyContin, which he became hooked on after injuring his back. Canadian Press (CFJC Today)

Alberta Mounties poring over new documents in little girl's death
Alberta RCMP are now going through thousands of pages of new information as they investigate the death of a 4-year-old girl who had been placed in kinship care. Serenity died in hospital of a massive brain injury in 2014, with her guardians saying she fell off a swing, but there are reports she was malnourished with signs of physical and sexual abuse. There have been calls for Alberta's Human Services minister to step down over how long it took the Mounties to get the new information they were

looking for, but Inspector Gibson Glavin says they did not ask for the documents until this summer, received them on Nov. 22 in a format they were unable to open, and got them open on Dec. 6. iNews880

Crime Stoppers tip line is back in Yukon
Five years after Yukon's last Crime Stoppers program folded, the tip and reward program is back in operation in the territory. Officials with the RCMP, the Yukon government, and the Yukon Community Crime Stoppers Association, held an event on Thursday to launch the program. "It is an effective tool," said RCMP Insp. Brian Jones, who is head of criminal operations with the Yukon force. "The anonymity that the program provides is critical to the success of that program, and that anonymity is respected throughout the program." CBC News

2 men handed lengthy prison sentences in J-Tornado drug case
Two Saint John-area men arrested as part of the RCMP's Operation J-Tornado in 2014 have both been handed lengthy prison sentences for their role in a criminal organization and cocaine-trafficking ring. Shane Williams, 34, of Smithtown, was sentenced to nine years and 11 months, while Joshua Kindred, 40, of Saint John, received six years. Williams, as the head of the criminal organization, deserved to get a serious sentence, Court of Queen's Bench Justice William Grant said on Friday. Kindred was not as culpable because he was not a member of the criminal organization; he operated in association with it, Grant said. The two men, who were both convicted in September, showed little reaction to their sentences, which work out to approximately six-and-a-half years and two-and-a-half years respectively with time already served in custody taken into account. (…) During the 65-day trial, the court heard the RCMP used a paid agent to distribute BlackBerry smartphones to drug suspects and lead them to believe the phones were immune to police surveillance. Instead, emails from the smartphones were routed directly through RCMP servers, with more than 30,000 messages intercepted and analyzed by police. CBC News

Four stores owned by local couple raided by RCMP, Revenue agency
Investigators with the Canada Revenue Agency, backed by RCMP officers, raided a string of convenience stores owned by a local couple Thursday. The first raid appeared to be at the Glebe Smoke Shop on Bank Street near Fifth Avenue Thursday morning. About half a dozen officers were in the 24-hour convenience store which stocks a large selection of magazines and tobacco products, according to an employee who answered the phone. The employee said the agents had not told him why they were in the shop, which recently reopened after a renovation, and deferred all comments to the store's owner. Agents were seen handling what appeared to be a hard drive, examining books and rifling through shelves. As well, RCMP officers and CRA investigators raided three Zesty Markets, one on Elgin Street and two on Rideau Street. Ottawa Sun

Broadcast Media / Médias télédiffusés:

Radio-Canada a diffusé l'émission Enquête qui tente de comprendre ce qui a motivé l'un des premiers groupes de jeunes québécois à partir pour le Syrie en 2012 et pourquoi certains d'entre eux sont revenus au Canada. Transcription

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Marijuana seized at Atlantic Institution in Renous, N.B.
Corrections officials say they seized a large quantity of marijuana at the Atlantic Institution in New Brunswick. In a statement today, Correctional Service Canada says officials found a package with 65 grams of marijuana at the maximum security institution on November 29th. It doesn't reveal how the contraband was seized, saying only that it uses scanners and drug-detector dogs. Canadian Press (Global News)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Kelowna Council to review 2017 budget
Kelowna City Council will receive an overview presentation of the 2017 Financial Plan at the Dec. 12 regular meeting, where staff will recommend a 4.40 per cent tax increase. Deliberation of the provisional plan will take place during an all-day public meeting Thursday, Dec. 15. Previous years' budgets include commitments that impact the 2017 Financial Plan, such as contractual obligations, the Police Services building project and the annualization of six new RCMP positions approved in 2016. These previous commitments account for more than 2.2 per cent of the proposed 4.40 per cent tax increase. (…)Community safety continues to be a significant part of the City's budget, with requests in 2017 for two new RCMP members, ongoing RCMP contract costs, new firefighters, a new fire truck, two Bylaw Enforcement positions, continued work on the Police Services Building, Glenmore Firehall upgrades, needle sterilization and disposal and a safety coordinator, in addition to additional resources to address homelessness. InfoTel

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Alberta pot tourism hanging in the balance as feds mull legislations
Although not clear how pot legalization will go down, Albertans are already planning to piggyback business on the marijuana economy. In Colorado, when pot was decriminalized in the state, their local tourism board didn't touch the stuff – because it's not federally legal. Yet if you plan a trip to the toking state, there are many services purporting to be 420 friendly. And according to Minister of Justice and Solicitor General Kathleen Ganley, because of the state's restrictions on smoking outside, and of course, in restaurants, they quickly found the edibles market exploding. That one legislative example can give you an idea of how many different scenarios could play out for small businesses, depending on how the government legalizes weed. There are still a lot of unknowns: whether regular businesses will be able to carry pot products, or if it will take a specialized license for weed dispensary type shops. Metro News

There's Been No Bait-And-Switch On Cannabis Legalization
An opinion piece states, "Prime Minister Justin Trudeau recently expressed frustration around the current cannabis landscape, explaining, "Until we have brought in the proposed system... the current prohibition stands," and encouraging police to enforce the law, particularly as it pertains to the continued expansion of medical cannabis dispensaries in major cities across Canada. The response has been one of uniform frustration from many angles, but I don't believe Justin Trudeau actually lied about the Liberal party's intentions on the cannabis file. From the very beginning, the emphasis has always been on restricting and regulating access to cannabis. In September 2015, Trudeau said he would not like to see cannabis sold at corner stores. In 2014, Trudeau said his government would legalize and make it more difficult -- not easier -- for children to get their hands on marijuana (which implies more regulation). As early as 2013, he was quoted saying, "Our government has no interest in seeing any of these drugs legalized or made more easily available to youth," and more recently he has been reaffirming the intention that, "our approach on legalizing marijuana is not about creating a boutique industry or bringing in tax revenues." The budget did not even include any mention of marijuana." Huffington Post

PUBLIC SERVICE / FONCTION PUBLIQUE

PIPSC union and federal government close in on deal

The federal government and the union representing professionals working in the public service wound up three days of contract talks early Friday morning with what some say are the makings of a tentative deal that could boost salaries by five per cent over four years. The Professional Institute of the Public Service of Canada, which had publicly resolved to have a contract deal by the end of the year, appears to have broken the logjam that has dogged negotiations for more than two years. Union and Treasury Board negotiators met until early Friday morning, when they wrapped up discussions for three of the union's bargaining groups. Two other groups return to bargaining today for another session. The government and 18 unions have been negotiating for months but spinning their wheels on two big issues — money and sick leave. The unions signed a solidarity pact vowing not to make concessions on the existing sick leave regime. PIPSC refused to comment with negotiations still underway but sources say the the latest wage offer is a 1.25 per cent a year increase over four years. Ottawa Citizen

Phoenix jitters affects federal United Way campaign
The federal government hopes to close in on its $19 million goal for this year's United Way workplace campaign despite employees' jitters about using the fickle Phoenix payroll system for their campaign donations. William Pentney, deputy minister at Justice and the campaign's chair, said apprehensions about Phoenix reduced the number of employees using payroll deductions for their donations this year, but they didn't put as much of a damper on the campaign as organizers had feared. The federal workplace campaign is the biggest in the country, with 80 per cent of donations typically come from payroll deductions. This year, that slipped to 70 per cent. About $14.6 million has been raised so far. "Seven out of 10 using payroll deduction is a bit of drop but I might have thought it would have been more dramatic than that," said Pentney in an interview. Public servants can also donate using credit cards, PayPal, cash and e-pledges, but contributions have tended to be more generous when they can be extended over 26 pay cheques. The problem is Phoenix has worked so erratically that public servants could be afraid to risk making deductions for fear of fouling up their pay. Pentney said the campaign could fall short of its target but he is hopeful it will climb to the $19 million mark as donations continue to roll in before the campaign closes at the end of December. He said 25 of 101 departments have reached their goals. Ottawa Citizen

OTHER / AUTRES

Russia threatens retaliation over latest round of Canadian sanctions
Canada has quietly imposed additional sanctions on Russian nationals over the annexation of Crimea and Moscow's ongoing support for separatists in eastern Ukraine. The new measures, including asset-freezing and a prohibition on business dealings, were passed by the Liberal cabinet on Nov. 28 and released, without much fanfare compared with the former Conservative government, on the Global Affairs Canada website the same day. There are 15 individuals named in the regulation, which was to be formally posted Thursday in the Canada Gazette, the government's official publication of record. Six of the people are members of Russia's national assembly — known as the Duma — who were elected from Crimea in September in the first vote since the takeover. (…) The additional measures may have been discreet and garnered little public attention in Canada, but they have prompted a fierce reaction from both the Kremlin and the media in Moscow. Russian Foreign Ministry spokeswoman Maria Zakharova says her country regrets Canada's decision and "this unfriendly action" will not go unanswered. CBC News

Anti-corruption group calls for more disclosure on owners of Canadian companies, trusts
The federal government should require all companies and trusts in the country to identify their beneficial owners, according to recommendations contained in a new report from the Canadian division of Transparency International, a global anti-corruption organization. The government should then publish the collected information in a central registry that is accessible to the public in an open data format, TI Canada said in its report, which was released Friday. The lack of ownership disclosure makes Canada's real estate market attractive to those looking to invest the proceeds of crime, the group said. CBC News

INTERNATIONAL

Un «suspect terroriste» arrêté à Rotterdam
Un «suspect terroriste» de 30 ans a été interpellé mercredi dans une habitation de Rotterdam et est «soupçonné d'avoir préparé un crime terroriste», a annoncé vendredi le parquet national néerlandais dans un communiqué. La police a saisi une kalachnikov AK-47, deux chargeurs remplis ainsi que quatre boîtes de «pièces illégales de feu d'artifice» et un tableau représentant un drapeau utilisé par le groupe État islamique, a précisé le parquet. Agence France-Presse (TVA Nouvelle); Reuters; 570 News; NY Times; Metro; NY Post; CNN; The Guardian

Islamic State 'has lost 50,000 fighters' over two years
At least 50,000 militants from so-called Islamic State have been killed since the US-led coalition started fighting in Iraq and Syria two years ago, a US military official has said. The senior official described the figure as a "conservative estimate". The figure showed air power and a small number of US figures supporting local forces were having an impact, the official said. The US has, however, repeatedly warned that IS can replace fighters rapidly. BBC News

'People just panicked': 3,000 affected by earthquake in Solomon Islands, initial reports say
Hundreds of people in remote parts of the Solomon Islands have had their homes damaged or destroyed by a powerful magnitude 7.7 earthquake that struck Friday, an aid organization said. There have been no deaths reported from the quake, which also caused some small tsunami waves in the Solomon Islands and other Pacific islands. Speaking from the capital Honiara, Suzy Sainovski, World Vision's Pacific Timor-Leste spokeswoman, said it has been hard to get a full assessment from some more remote communities, some of which don't have cellphone coverage. Associated Press (National Post)

Révélations Snowden : otages et rançons, le double jeu des alliés de la France
La France ne compte pas que sur elle-même pour libérer ses ressortissants des mains de ravisseurs à l'étranger. Elle s'appuie souvent sur les Etats-Unis et le Royaume-Uni. Mais de nouveaux documents extraits par Le Monde, en collaboration avec le site The Intercept, des archives de l'ex-contractuel de l'Agence nationale de sécurité (NSA) américaine Edward Snowden confiées à Glenn Greenwald et Laura Poitras, montrent que cette coopération n'est pas aussi loyale qu'on pourrait le croire, malgré la sensibilité du sujet. Le Monde

Syrian civilians leave crumbling rebel enclave in Aleppo
Hundreds of Syrian civilians streamed out on foot from the eastern part of the city of Aleppo on Friday in the wake of the relentless campaign by government troops and their allies to drive rebels from their rapidly crumbling enclave. The U.N. human rights office said it was deeply concerned about reports that hundreds of men have gone missing after crossing from eastern Aleppo into government-controlled areas of the city. Spokesman Rupert Colville said that family members have reported losing contact with the fighting-age men, who are between 30 and 50 years old, after they fled opposition-held areas of Aleppo around a week or 10 days ago. It was not clear whether they were fighters or civilians. (…) "Bombing is truly round the clock," said Ziad Mohammed, a lawyer and father of three, still living in eastern Aleppo's al-Mashhad neighbourhood. "There are no hospitals, the remnants of the dead fill the streets and the wounded have to fend for themselves." News 1130

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

RalphGoodale
US VP Joe Biden speaks at Ottawa Dinner - blizzard outside, warm Cda-US cross-border friendship celebrated inside!

ceasefireblog
@RalphGoodale #Nationalsecurity review should heed strong call from all of Canada's Privacy Commissioners #cdnpoli https://t.co/keTpoOBY2T

drmarcspooner
Canadian spywatcher's Snowden remark 'highly inappropriate,' Goodale says - The Globe & Mail http://www.theglobeandmail.com/news/politics/canadian-spywatchers-snowden-remark-highly-inappropriate-goodale-says/article33279449/ … @Snowden @RalphGoodale

MacleansMag
Ralph Goodale leaves the door open to CSIS crunching potentially sensitive data about innocent people: https://t.co/bTVVJtTM2C

ipoliticsca
New counter-radicalization office head could be named before Christmas. @amandacconn reports. http://ipoli.ca/2gkVfSE

amandacconn
New counter-radicalization office head could be named before Christmas https://t.co/Z22tEXMFQO

ChantalCarey
19 postes qui exigent une maîtrise essentielle du français à la @grcrcmppolice : Il y aura un plan de redressement, déclare @RalphGoodale

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

lpsmediaoffice
Some #Winter #SafetyTips from Public Safety Canada: https://www.getprepared.gc.ca/cnt/rsrcs/sfttps/tp201212-en.aspx … #ldnont #BePrepared

ottawasuncom
Ottawa paramedics warned to don masks against deadly new drug http://ow.ly/lb2l306Y2yF

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

1alexhemingway
File under: not confidence-inspiring. And another reason to repeal #C51. More on that from @OpenMediaOrg: https://saveoursecurity.ca/ #cdnpoli

OpenMediaOrg
.@1alexhemingway +1 -- this shocking statement reinforces the need for accountability + end to #C51! https://SaveOurSecurity.ca #YourNatlSec

NATIONAL SECURITY / SÉCURITÉ NATIONALE

fabricedp
!!! Procès #Habib : la GRC avait comme source un montréalais d'une 40aine d'année, un "mentor" qui "pratique l'islam salafiste" à Montréal.

katemckenna8
And this. "Lyes," the civilian agent, is a mentor in the Islamic community in Montreal, in his 40s. Is (was?) working with the RCMP.

fabricedp
Cet Agent Civil Infiltration était géré comme source humaine par deux contrôleurs depuis 1 an avant lancement op. d'infiltration #Habib

fabricedp
Avocat Défense Me Montpetit demande à témoin GRC s'il s'est deja posé la question si la taupe n'avait pas des intérêts cachés.... #Habib

fabricedp

Certains membres de la communauté musulmane fréquentaient assidûment le commerce de vêtements de l'agent civil infiltration de la #GRC

fabricedp
On imagine que dans la communauté on doit chercher à savoir ou on sait déjà qui a été la taupe de la #GRC .... #Habib

fabricedp
1/Témoin dit que GRC voulait en savoir + sur le groupe Tchétchène dont Habib aurait dit avoir avoir fait partie et quel groupe il voulait
2/ rejoindre au cas où il parviendrait à retourner en #Syrie

fabricedp
Fin de la preuve de la Couronne au procès #Habib. Rdv fin janvier pour débat sur admissibilité preuve operation infiltration #terrorisme

rolandparis
Why am tweeting about this stuff? Russian interference in Western elections is national security issue for all democracies - and for NATO.

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CBCAlerts
CBSA border services officer charged in connection with smuggling contraband tobacco into Canada from US at Peace Bridge near Niagara Falls.

CP24
Suspect in Scarborough homicide from 2010 located in Malaysia, returned to Toronto http://www.cp24.com/news/suspect-in-2010-scarborough-homicide-located-in-malaysia-returned-to-toronto-1.3196715 ...

nspector4
.@Scott_Gilmore @acoyne May have read about a CBSA report in a @PostmediaNews newspaper

CanBorderPRA
A little friendly singing competition between #CBSA singers in #YYC and #YWG raised $200 for #GCWCC #CBSAgives

Transport_gc
Visiting south of the border this season? Check with @CanBorder for border wait times: http://ow.ly/dooa306P4S

CYBER SECURITY / CYBERSÉCURITÉ

RadioCanadaInfo
États-Unis : le président Obama demande l'ouverture d'une enquête sur le piratage de l'élection présidentielle http://ici.radio-canada.ca/nouvelle/1004892/obama-demande-une-enquete-sur-le-piratage-de-lelection-presidentielle ...

motherboard
Hacker finds a way to get into any Yahoo Mail inbox, gets $10,000 for alerting Yahoo http://bit.ly/2gl8aUR

LAW ENFORCEMENT / APPLICATION DE LA LOI

GlobalCalgary
RCMP renew plea for help finding Alberta woman who vanished almost 2 months ago https://t.co/zwoq1ojEPL

globalnews
Man who intimidated witness in a trial sought by Fort McMurray RCMP. https://t.co/oS4ugmsPcc

OttawaCitizen
Owner of four convenience stores expresses shock over Thursday raids by CRA, RCMP. http://ow.ly/t1L3306Ydow

Momin680NEWS
What you are looking at here, is $2.5 Million dollars worth of counterfeit merchandise Toronto Police seized off of 16 trucks.

metromontreal
Une femme mord une policière dans un bar de Québec http://bit.ly/2htqB5T

CTVVancouver
Caught on cam: Thieves use keys to open mailbox, steal large bag of mail https://t.co/Lsk95ddV6e

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

CBCWorldNews
Clemency bid for Canadian on death row in Montana awaits action from governor http://ift.tt/2gsux9b

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

KelownaNow
Pro-white posters torn down at @UBCOnews #Kelowna https://t.co/VFKFdx9fsj

vicecanada
A Calgary mother was beaten with a hockey stick and nearly run over in a road rage attack: http://bit.ly/2giWVai

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

tlupick
"Access to clean opioids is critical." - Leslie McBain w/ passionate argument for legalization & regulation of all drugs. #vanpoli #fentanyl

HuffPostCanada
There's been no bait-and-switch on cannabis legalization, by @jennav5 http://huff.to/2heY8l6

OTHER / AUTRE

CBCNews
'Unfriendly action': Canada quietly applies more sanctions against Russians, including six MPs
http://www.cbc.ca/1.3888309

INTERNATIONAL

AlArabiya_Eng
#BREAKING: #UNGA #Syria ceasefire voting results: 122 for, 13 against, 36 abstain. http://ara.tv/bhpta

CBCWorldNews
Blasts kill 30 in northeast Nigeria; Boko Haram blamed http://ift.tt/2h5yZeN

tvanouvelles
Un «suspect terroriste» possiblement lié à l'El arrêté à Rotterdam http://bit.ly/2gkQN6x

fabricedp
50.000 ? Vraiment ? RT Islamic State 'has lost 50,000 fighters' over two years #IS https://t.co/HNq7fyKE7P

fabricedp

Révélations Snowden : otages et rançons, le double jeu des alliés US, GB de la France pour saborder le processus https://t.co/JbKw6Tzzkl

StewartBellNP
AQIM shows how it posed as UN to bomb peacekeeping office at Gao airport in Mali. @siteintelgroup

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

Today's News / Actualités
December 16, 2016 / le 16 décembre 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Food portions at heart of Sask. Penitentiary riot, inmate's mother says
A riot that left one man dead and several others injured at Saskatchewan Penitentiary was the result of unmet requests from inmates for more food, one inmate's mother says... Canada's prisoners' ombudsman Howard Sapers said Saskatchewan Penitentiary generated more complaints — 413 — last year than any other federal facility in the country and that 93 per cent of complaints in the prairie region came from the Prince Albert prison. The complaints were made about things including food, health care, family visits and access to parole hearings. Sapers, the Correctional Investigator of Canada, has sent a

team from his office to investigate Wednesday's riot alongside the RCMP, the Union of Canadian Correctional Officers, and Correctional Service Canada. His office will not only be looking into the riot, but also the issue of food, he said. There have been several recent changes to food services and the "national diet" in federal institutions with the introduction of a new menu... Sapers said facilities across the Prairies tend to be the most overcrowded. He's raised concerns about the issue for years as it relates to the scarcity of resources, inmates being forced to double-bunk, and competition for employment and program placement."... **The office of Public Safety Ministry Ralph Goodale** sent a statement Friday saying Correctional Service Canada is reviewing the incident. "**Minister Goodale** was continuously briefed about the riot at Saskatchewan Penitentiary throughout the incident," the statement read. "His thoughts are with the family and friends of the inmate who passed away after the incident, and with those who suffered injuries." Don Head, Correctional Service Canada commissioner, was at Saskatchewan Penitentiary Friday. CTV News

Forget about "one-size-fits-all" counter-radicalization policies
An opinion piece states "The term 'radicalization' is used so much these days that people have come to assume that it refers to a single, undifferentiated process that every terrorist goes through. The quest to define and detail the specific steps of this process has become the 'Holy Grail' mission of radicalization studies in the post-9/11 era. Yet after a decade of searching, most experts have come to the conclusion that there's no single 'terrorist profile' to determine who might become dangerous and how... There is no overarching process that can account for every terrorist's personal journey to violence. Different life circumstances can produce different motivations and pressures. Canada's counterterrorism policies should reflect this reality... The Toronto Police Service revealed this week that it's been operating a secret radicalization prevention program for more than two years. Police officers and 'participating agencies' have been referring youth who they deem to be in danger of radicalization to one of four deradicalization 'hubs' across the city... This latest effort in Toronto is just Canada's latest attempt at getting counterterrorism right. The Trudeau government has set aside $35 million for counter-radicalization efforts **and Public Safety Minister Ralph Goodale** is sourcing public opinion on public safety strategies via his national consultations. All this will be in vain if the Canadian establishment doesn't take the latest conclusions on radicalization seriously and try to implement policies that reflect these findings." Policy Options

Opioids, pot and economics – three ways politics touched Canadians this week
It was the final week of Parliament before Christmas, and all through the House ... the Liberals did their best to make sure no one had any time to think about ethics or fundraising before heading home for the holidays. By the time MPs agreed Wednesday to rise until the end of January, the government had announced a new opioid strategy; ramped up negotiations with the provinces on health-care funding; welcomed a complicated blueprint on how to legalize pot; set up a different system for new Canadians to bring in their parents and grandparents; and launched a review of the assisted-dying law... The government has announced a two-pronged approach to confronting the opioid crisis. Health Minister Jane Philpott has tabled legislation that would give cities more leeway to open up supervised drug injection sites. The law would essentially remove the high bar set by the previous Conservative government, which required communities to meet 26 conditions in order to qualify. For now, there are only two safe-injection sites in Canada, both in Vancouver. At the same time, **Public Safety Minister Ralph Goodale** proposed measures to crack down on illegal drugs and their ingredients coming over the border. Border guards would be allowed to examine very small suspicious packages and also restrict the import of equipment used to make drugs... Even as Ottawa moved to more strictly control opioids, it also got a step closer to legalizing pot. A government-appointed task force finally made public a blueprint that would allow those 18 and older to buy regulated marijuana from stores and through the mail. Canadian Press (Ottawa Citizen)

TOP STORIES / MANCHETTES

Ottawa appoints special rep on First Nation border-crossing rights
The federal government is moving on the recommendations of a Senate committee and appointing a special representative on Canada-U.S. border issues for First Nations. Fred Caron, who is already

Ottawa's lead negotiator with Nunavut on the devolution of more government powers to the territory, will now also play a key role in figuring out how to ease travel between the two countries for First Nations split by the border. The Mohawk of Akwesasne, for example, have communities in both countries and face many practical problems in making the border crossing, the Standing Senate Committee on Aboriginal Peoples heard earlier this year... The committee heard from security officials who discussed several programs designed to ease travel between the two countries, like the Nexus card program for frequent travellers. The Akwesasne would like to see "the creation and admissibility of a secure ID card that would facilitate crossing for their members within their territory," says the committee's final report published in June. The committee's sole recommendation — the appointment of a special representative to explore solutions on border issues — includes looking at "secure identification cards, telephone and video reporting, and a review of admissibility requirements for Native Americans entering Canada." The committee advised the appointment take place before the end of this year. In a news release issued Friday, Indigenous and Northern Affairs Minister Carolyn Bennett said Caron's work will "inform the work of an interdepartmental steering committee" that's working on finding solutions to the border issue. "These solutions will also balance the need to maintain national security and public safety," said Bennett in the release. Caron's recommendations are due in the spring, said a spokesperson for Bennett. iPolitics

Investigation, cleanup underway after riot at Saskatchewan Penitentiary

A Saskatchewan prison where a major riot took place this week had the most complaints of any penitentiaries in the country last year, according to Canada's prisoners' ombudsman. Howard Sapers, the Correctional Investigator of Canada, says there were 413 complaints about things including food, health care, family visits and access to parole hearings from inmates at the Saskatchewan Penitentiary in Prince Albert. One inmate was killed during the riot Wednesday, as prisoners set fires, smashed windows and pulled heat registers off walls. Sapers says it's extremely troubling to hear about the incident because it speaks to a real dysfunction in an institution. He has sent a team from his office to investigate, along with RCMP, the Union of Canadian Correctional Officers and Correctional Service Canada. Canadian Press (Sudbury.com; Province; Vancouver Sun; Leader-Post; CP24); AM 650 CKOM

Saskatchewan RCMP officer charged with firearms offences in Edmonton

A Saskatchewan Mountie is facing firearms charges in Alberta. Const. Dale Malbeuf of the Morse detachment in southern Saskatchewan was arrested this week at a home in Edmonton. Police allege the officer produced and pointed a firearm at a woman in the home. Malbeuf appeared in Edmonton court Wednesday on charges of pointing a firearm and careless use of a firearm. He was released on conditions and is to attend court again Jan. 6. RCMP say Malbeuf, on the force for 12 years, has been suspended with pay. Canadian Press (Global News); Postmedia Network (Edmonton Sun); AM 980 CJME; Radio Canada

RCMP seize furanylfentanyl in raid on Orléans home

A police raid on an Orléans home Thursday resulted in the seizure of enough of the designer drug furanylfetanyl to supply between 21,000 and 38,000 doses, according to the RCMP. The RCMP said they found 19 grams of the opioid during a search of a home at 731 Clearcrest Crescent. Furanylfentanyl is an extremely potent drug with a similar compound to fentanyl. Police said they executed the search warrant following a joint investigation with the Canada Border Services Agency. Said Mehdi Rostaee, 42, was arrested and charged with importing a controlled substance and other drug-related offences, according to police. The investigation is ongoing. Postmedia Network (Ottawa Citizen; Ottawa Sun); CBC News

Update: B.C. man targeted by police for terrorism peace bond denies having any involvement in terrorism

The latest target of Canada's terrorism peace bond system insisted he has no connection to extremist violence and turned up at a B.C. police station to complain about press coverage of his case. "I throw your newspaper in the garbage," Khalid Ahmad Ibrahim, 39, told a reporter at the door of a New Westminster, B.C. apartment. "There is no terrorism," he added. The RCMP told the provincial court on Dec. 8 there were "reasonable and probable grounds to believe ... that Khalid Ahmad Ibrahim may commit a terrorism offence."... Meanwhile in Ottawa, Tevis Gonyou-McLean, arrested on an ISIL-related peace bond in August and released on bail, was arrested once again on Tuesday for six alleged

violations of his bail conditions. He was to appear in court Friday at 1:30 p.m. Postmedia Network (National Post; Calgary Herald)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Is Canada ready to weather an electromagnetic pulse and widespread blackout? We don't know
In the early morning hours of March 13, 1989, Christine Gombas thought the world was ending. The then-52-year-old was at her home in rural Quebec, her son glued to the family's television, when the power blinked out. "The house made a funny noise, like a hum," Gombas told a reporter from The Montreal Gazette the next day. What she — and anyone else still awake at that hour in Quebec — saw was a solar storm hitting the Earth's upper atmosphere. Within minutes, Hydro Quebec's highly inter-linked electrical grid collapsed, plunging the province into darkness as temperatures dipped to -15 C. In 1989, the hours-long loss of electricity was inconvenient, costly and potentially dangerous. But the storm that struck Earth that night was nothing compared to the one that hit us over a century earlier, in the late summer of 1859. The so-called Carrington Event lit the sky so brightly that people could read newspapers by the aurora it generated. It blew out telegraph systems all over the globe. More than a few telegraph operators got a nasty shock. Today, a similar event would be catastrophic. Electrical distribution networks could theoretically be blown out across Canada, with some experts predicting that blackouts would last anywhere from weeks to over a year... **According to Public Safety Canada spokesperson Karine Martel, a series of "guidelines" for confronting an EMP pulse or major solar storm have been established for the owners and operators of Canada's electrical grid (these would include hundreds of utilities like Hydro Quebec and Ontario's Hydro One), local governments and other stakeholders.** These guidelines were also referenced, but not listed, in documents obtained by Global News last summer through Access to Information legislation. The guidelines themselves are only available though the department's Critical Infrastructure Gateway, which is not publicly accessible. ***"The guidelines share best practices and challenge assumptions as to Canada's level of preparedness to respond to these unique events,"*** **Martel wrote in an emailed response to questions from Global News... Public Safety Canada's guidelines for industry don't *"speak specifically to the use of surge protectors or other technology,"* according to Martel. But they do *"outline actions that can help minimize the impact of these disasters."*** Global News

Bennett pledges aboriginal housing improvements after fatal Ontario fire
The federal government is determined to improve aboriginal housing, Indigenous Affairs Minister Carolyn Bennett said Friday after an Ontario chief blasted Ottawa for a lack of action following a deadly blaze that killed a family of five... Bennett has said the federal government doesn't know how many indigenous people die in fires on reserves because it no longer collects such statistics.The collection of fire data was stopped six years ago to ease the "reporting burden" on First Nations communities, the minister said in written responses to questions recently tabled in Parliament. She said her department would work with partners, including the Aboriginal Firefighters Association of Canada, "on new options to address the fire data gaps on reserve." "All options to generate this data are on the table so we can ensure the right programs and policies are in place to keep First Nations communities safe." Canadian Press (Globe and Mail; Huffington Post)

Notley government increasing spending on flooding, drought protection
The Alberta government has announced more funding for flood and drought protection. The province is to invest an additional $31 million over four years in flood resiliency projects through the Alberta Community Resilience Program. The 10-year, $500-million program has so far helped to build flood barriers, as well as other safeguards. Another $14 million is to go to the Watershed Resilience and Restoration Program. Canadian Press (Global News; Calgary Herald); AM 630

Ice jam reaches emergency status
The city has declared a level one emergency as the ice jam on the Nechako River has reached the confluence of the Fraser River. Level one means there is a "heightened awareness" in place, city spokesman Mike Kellett said. If a level two is invoked, the city's emergency operations centre, located at Fire Hall No. 1 next to city hall, will be manned 24 hours per day. The situation is monitored around the

clock and the provincial government Emergency Management B.C. has been notified that assets, such as gabion diking, could be needed in short order to mitigate potential damage. Prince George Citizen

The Brick's 2016 Christmas video 'overwhelms' Fort McMurray family rebuilding after fire
Following in the footsteps of companies like WestJet and Shell, The Brick has created its own Christmas experience video, helping residents affected by May's wildfire in Fort McMurray. The Brick set up a temporary Christmas tree lot Dec. 3 and handed out nearly 200 free trees and 100 wreaths in the hard-hit Beacon Hill neighbourhood. AM 680

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Update: B.C. man targeted by police for terrorism peace bond denies having any involvement in terrorism
The latest target of Canada's terrorism peace bond system insisted he has no connection to extremist violence and turned up at a B.C. police station to complain about press coverage of his case. "I throw your newspaper in the garbage," Khalid Ahmad Ibrahim, 39, told a reporter at the door of a New Westminster, B.C. apartment. "There is no terrorism," he added. The RCMP told the provincial court on Dec. 8 there were "reasonable and probable grounds to believe ... that Khalid Ahmad Ibrahim may commit a terrorism offence."... Meanwhile in Ottawa, Tevis Gonyou-McLean, arrested on an ISIL-related peace bond in August and released on bail, was arrested once again on Tuesday for six alleged violations of his bail conditions. He was to appear in court Friday at 1:30 p.m. Postmedia Network (National Post; Calgary Herald)

The best defense... : Canada is finally preparing an overhaul of its cyber security systems to protect it from threats from outside, and within. That's going to require getting proactive.
The Canadian Armed Forces is finally upping its game in the realm of cyber security — bolstering its shields against nation-state actors like Russia and China, malicious hacker groups, and "insider threats" that may be looking to follow in Edward Snowden's footsteps. In a pair of documents, published Friday, the Canadian military is asking industry to submit ideas on how they can assess and respond to cyber threats in real-time. Under the Defensive Cyber Operations Decision Project, which will ultimately culminate in a plan that will be submitted to the federal government, the Department of National Defense will be looking at capabilities that will allow the military to "operate effectively in cyberspace on government-authorized military missions, to support our federal partners in national cyber security efforts, and to work with international allies," according to a departmental spokesperson... "Domestic (routine and contingency) operations might involve assisting civil authorities in responding to natural disasters, cyber-attacks, terrorist attacks, crises in urban centres, threats to critical infrastructure, risks to health and food systems, or Chemical, Biological Radiological or Nuclear (CBRN) attack," the document reads. "Owing to the potential for an increase in domestic threats, [the Department of National Defense/Canadian Armed Forces] as a whole needs to become more integrated within the domestic response community — in particular, the security and intelligence sectors. In particular, the future security environment will require a level of domestic integration among agencies that does not exist at the present time." Canadian intelligence-watchers have, for years, noted an uptick in domestic activity amongst Canadian military intelligence units — which, traditionally, do not run national intelligence-gathering. This journalist reported in 2014 that military counter-intelligence kept tabs on Indigenous protesters, perhaps countering their own mandate. More recently, the Ottawa Citizen reported that military intelligence conscripted the Communication Security Establishment to track a Canadian within the country. The Communication Security Establishment, the signals intelligence agency that works hand-in-hand with the American NSA, does not appear to be covered by this cyber defense strategy. That agency does not have authority to do

surveillance inside Canada, unless specifically mandated to by another department. Vice News; Global News

Canada looks at possible changes to how it shares data among federal agencies, foreign partners
Canada is reviewing how intelligence agencies — such as the Royal Canadian Mounted Police (RCMP) and Canadian Security Intelligence Service (CSIS) — share information for the purposes of national security. Seeds for possible amendments to federal legislation are being planted by the House of Commons' ethics and privacy committee, which is currently reviewing the 2015 Security of Canada Information Sharing Act (SCISA) — the law that governs how information is shared between domestic agencies to thwart security threats. The committee plans to hold more hearings in coming weeks and expects to make recommendations in the near future on whether SCISA should be amended to address privacy concerns. The process is part of the Liberal government's ongoing national security consultation and review of Canada's 2015 Anti-Terrorism Act, previously known as Bill C-51, of which SCISA is a component... But while the SCISA exists to regulate how Canada shares information domestically, the review hearings have also raised questions around how Canada shares data with its foreign partners — a process critics say is shrouded in secrecy. Specifically, the review is looking at how Canada participates in one of its most important foreign spying arrangements — the decades-old deal between Ottawa and its Five Eyes allies in the U.S., UK, Australia and New Zealand. Open Canada

Man who killed soldier Patrice Vincent wanted more victims: Quebec coroner
A coroner says a Quebec man who killed a Canadian Forces warrant officer in 2014 wanted more victims. Patrice Vincent, 53, was killed in the parking lot of a shopping mall in Saint-Jean-sur-Richelieu when Martin Couture-Rouleau plowed into him and a fellow soldier, who survived. Couture-Rouleau had known jihadist sympathies. Coroner Andre Dandavino's report contains excerpts from a conversation Couture-Rouleau had with a 911 operator just minutes after Vincent's death. The report says Couture-Rouleau called 911 and said he was not going to surrender because he might run into another soldier and that he would kill him. Earlier, Couture-Rouleau tried to attack a police officer, while Dandavino noted he later had two knives in his hand as he tried to charge another officer before he was killed. Canadian Press (Global News; CTV News); CBC News

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Ottawa appoints special rep on First Nation border-crossing rights
The federal government is moving on the recommendations of a Senate committee and appointing a special representative on Canada-U.S. border issues for First Nations. Fred Caron, who is already Ottawa's lead negotiator with Nunavut on the devolution of more government powers to the territory, will now also play a key role in figuring out how to ease travel between the two countries for First Nations split by the border. The Mohawk of Akwesasne, for example, have communities in both countries and face many practical problems in making the border crossing, the Standing Senate Committee on Aboriginal Peoples heard earlier this year... The committee heard from security officials who discussed several programs designed to ease travel between the two countries, like the Nexus card program for frequent travellers. The Akwesasne would like to see "the creation and admissibility of a secure ID card that would facilitate crossing for their members within their territory," says the committee's final report published in June. The committee's sole recommendation — the appointment of a special representative to explore solutions on border issues — includes looking at "secure identification cards, telephone and video reporting, and a review of admissibility requirements for Native Americans entering Canada." The committee advised the appointment take place before the end of this year. In a news release issued Friday, Indigenous and Northern Affairs Minister Carolyn Bennett said Caron's work will "inform the work of an interdepartmental steering committee" that's working on finding solutions to the border issue. "These solutions will also balance the need to maintain national security and public safety," said Bennett in the release. Caron's recommendations are due in the spring, said a spokesperson for Bennett. iPolitics

Winnipeg man faces 136 fraud charges
A Winnipeg man has has been hit with a slew of charges after he is alleged to have fraudulently collected fees as an immigration consultant. The Canada Border Services Agency announced 56-year-old Vladimir Bibilov is facing 102 counts under the Immigration and Refugee Protection Act, and another 34 counts under the Criminal Code for alleged offences between January 2009 and December 2015. Bibilov is alleged to have acted as a paid immigration consultant when he was not licensed to do so and allegedly took fees from clients. The CBSA alleged Bibilov "misrepresented himself to foreign nationals with the promise to provide immigration services to Canada," and also alleged he "provided false and misleading information to induce or deter immigration to Canada." He will appear in a Winnipeg courtroom on Monday. "The CBSA takes immigration fraud very seriously and is committed to fully investigating and prosecuting those who violate our laws and seek to profit illegitimately from our immigration system," CBSA spokeswoman Kim Scoville said in a release. Postmedia Network (Winnipeg Sun)

Quebecer pleads guilty to possession of cocaine found on cruise ship
Isabelle Lagacé today pleaded guilty in an Australian court to cocaine possession charges, months after she and two other Canadians were arrested when 95 kilograms of cocaine valued at about $30.5 million were found in suitcases on a cruise ship… Their movements were tracked by a joint operation involving the Canada Border Services Agency (CBSA), Australian Federal Police and the U.S. Department of Homeland Security from the time they boarded the cruise ship in England. Police in Australia believe the operation was organized by a powerful drug syndicate. CBC News

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

One quarter of Canadian online traffic vulnerable to NSA sweeps: researchers
A large amount of Canadian internet traffic is being routed through the United States, leaving it vulnerable to collection and probing by the National Security Agency. And most Canadians have no idea of how exposed they are to American data sweeps, say the researchers behind a new tool that aims to show Canadians what path their internet traffic takes to connect to the websites they want to visit. In a new online project launched Thursday, researchers from the University of Toronto and York University have partnered with Open Media to create a tool to show the paths Canadians' internet data take when they access websites or send online communications. iPolitics

Yahoo faces proposed Canadian class action following hacks
Yahoo is now facing a proposed class action on behalf of Canadians whose personal information may have been stolen. A Toronto-based law firm says a notice of action was filed today. The class action will take in Canadians whose user account information was stolen or whose email accounts were accessed. The representative plaintiff is a Canadian who used Yahoo for her email. The proposed $50-million suit comes on the heels of a similar action in the United States. Yahoo published a security notice in September and another earlier this week that its computer networks were hit with cyberattacks. Canadian Press (CP24; Huffington Post; CTV News); Presse Canadienne (La Presse)

Grade 10 literacy test to be done on paper
Ontario's Grade 10 literacy test — which suffered a major cyberattack during an online trial this fall — will be offered on paper only this spring as the agency that runs it tries to ensure any move to digital is secure. Toronto Star

LAW ENFORCEMENT / APPLICATION DE LA LOI

Saskatchewan RCMP officer charged with firearms offences in Edmonton
A Saskatchewan Mountie is facing firearms charges in Alberta. Const. Dale Malbeuf of the Morse detachment in southern Saskatchewan was arrested this week at a home in Edmonton. Police allege the officer produced and pointed a firearm at a woman in the home. Malbeuf appeared in Edmonton court Wednesday on charges of pointing a firearm and careless use of a firearm. He was released on conditions and is to attend court again Jan. 6. RCMP say Malbeuf, on the force for 12 years, has been

suspended with pay. Canadian Press (Global News); Postmedia Network (Edmonton Sun); AM 980 CJME; Radio Canada

RCMP seize furanylfentanyl in raid on Orléans home
A police raid on an Orléans home Thursday resulted in the seizure of enough of the designer drug furanylfetanyl to supply between 21,000 and 38,000 doses, according to the RCMP. The RCMP said they found 19 grams of the opioid during a search of a home at 731 Clearcrest Crescent. Furanylfentanyl is an extremely potent drug with a similar compound to fentanyl. Police said they executed the search warrant following a joint investigation with the Canada Border Services Agency. Said Mehdi Rostaee, 42, was arrested and charged with importing a controlled substance and other drug-related offences, according to police. The investigation is ongoing. Postmedia Network (Ottawa Citizen; Ottawa Sun); CBC News

Man arrested as cocaine, marijuana seized from home in C.B.S
The equivalent of 1,290 marijuana cigarettes and 224 "dosages" of cocaine have been seized from a residence in Conception Bay South, police say. The RCMP said on Friday afternoon that officers arrested a 22-year-old man after a search warrant was executed at his residence. Cocaine, marijuana and cannabis resin were taken from the home. CBC News

Dawson Creek man arrested counterfeit U.S. money investigation
A Dawson Creek man has been arrested in connection with what police believe is a counterfeit money ring operating in communities across the north. On Dec. 13 at around 2 a.m., police in Prince George were called to a convenience store where a woman had tried to pass counterfeit American currency. The woman fled in a "distinctive" vehicle bearing Alberta plates, according to an RCMP news release. Police tracked down the vehicle a short time later at another Prince George convenience store and arrested the woman and a 33-year-old man she was travelling with. Both were carrying counterfeit American dollars, as well as pre-paid credit cards and "other counterfeiting evidence," according to the release. The woman was later found to hail from Spruce Grove, Alta., while the man is from Dawson Creek. Police have not released the names of either suspect. RCMP are sharing information with police in other communities to determine whether there are connections to other counterfeiting incidents. Dawson Creek Mirror

Man charged with murder on Little Black Bear First Nation
A 37-year-old man has been charged with second-degree murder on the Little Black Bear First Nation. RCMP were called to a residence Thursday morning where they found an unresponsive woman outside. EMS declared 33-year-old Lauren Quewezance dead at the scene. Police arrested Sherman Luke Bellegarde, who is also from Little Black Bear. He was known to Quewezance. CBC News

Saisie de 1,2 tonne de tabac et 4 suspects arrêtés à Saint-Anicet
Quatre suspects ont récemment été arrêtés à Saint-Anicet, en Montérégie, alors qu'ils étaient en possession de plus de 1,2 tonne de tabac de contrebande. Le 7 décembre, en début de journée, les policiers ont repéré une embarcation près de la berge du fleuve Saint-Laurent, dans le secteur de Saint-Anicet... L'opération a été menée par des policiers de la Sûreté du Québec, de la Gendarmerie royale du Canada et par des membres du Groupe de travail régional de Cornwall, une force policière mixte composée de la Gendarmerie Royale du Canada, de la Police provinciale de l'Ontario et du ministère des Finances de l'Ontario. Agence QMI (TVA Nouvelles); Journal Saint-Francois

RCMP to be on patrol during the holidays
Throughout the year (from Jan.1 to Dec. 15) Gander's RCMP detachment received 76 documented impaired driving complaints, resulting in nine charges being laid. With Christmas holiday celebrations now in full swing, Staff Sargent Roger Flynn said, traditionally in Canada, impaired driving is at its peak. Impaired takes in more than just alcohol, he noted. It also encompasses drugs – both prescription and illegal. But if anyone is fool hardy enough to put their lives and others in danger, be prepared to face the consequences. Throughout the holidays the RCMP will be carrying out numerous checkpoints and patrols to try and curb illegal activity. Gander Beacon

Schools benefit from RCMP officer's presence

Positive relationships have been cultivated by having a member of the RCMP available at high schools in Spruce Grove and Stony Plain. Parkland School Division's (PSD) board of trustees received a report from its school resource officer, Const. Pat Chornoby, during its regular meeting on Dec. 13. The partnership to provide a uniformed officer to the high schools was formed five years ago between the Town of Stony Plain, City of Spruce Grove, Parkland County, RCMP and PSD. The intention of the officer's presence is to help students make positive choices through law education and law counseling. The program has fostered relationships with youth, intervened with students making poor choices that may lead to criminal or risky lifestyles, and provided assistance with situations. Spruce Grove Examiner

RCMP stuff two cruisers for Digby Foodbank
Roger Tibbetts, manager at the Digby Foodbank, says he was extremely pleased with the generous response to the RCMP's Stuff the Cruiser donation drive at the Digby Sobeys and Superstore on Dec. 10 Shelburne County Coast Guard

Surrey residents generously "Pack the Police Car"
MORE than 4,500 pounds of food and over $8,000 in cash were collected in support of local food banks and Christmas hamper programs during the Surrey RCMP's 11 "Pack the Police Car" events held across the city between December 1 and 13. Indo-Canadian Voice

Toys for the North with RCMP and North Star Air
Toys for the North headed to seven communities in Northern Ontario on December 16, 2016. While the usual path for toys at this time of the year is from the North Pole at Santa's workshop, Toys for the North sees toys head north to make a brighter Christmas holiday for children across the north. The program in Northern Ontario runs in partnership with the "O" Division of the Royal Canadian Mounted Police (RCMP), and North Star Air. For the past three years, across Northern Ontario, North Star Air has participated in the 'Toys for the North' toy drive. Toys are flown from the Thunder Bay International Airport to make sure children across the North have some extra smiles over the holiday season. Net News Ledger

Help Mounties cram their cruiser
Nanaimo RCMP and Country Grocer have joined forces again for Cram the Cruiser, an annual drive to raise food for local families in need at Christmas. This year's event happens Saturday (Dec. 17) 9:30 a.m. to 2:30 p.m. at Country Grocer's Chase River Market Place location at 82 Twelfth St., where Mounties will be filling police vehicles with food. Nanaimo News Bulletin

Autochtones et policiers: Québec donnerait le feu vert à une enquête
Tout porte à croire que Québec donnera le feu vert à une enquête publique sur la relation entre les autochtones et les forces policières, comme le réclame depuis les événements de Val-d'Or l'Assemblée des Premières Nations du Québec et du Labrador. «Tout converge vers une décision à mon sens qui est inévitable. Tous les éléments sont réunis» pour que Québec acquiesce à notre demande, a affirmé au Soleil le chef Ghislain Picard. «Jusqu'où le gouvernement est prêt à aller? [...] Je pense qu'on est plus près du 100% en ce qui concerne nos demandes que le contraire.» Selon Radio-Canada, l'exercice porterait sur plusieurs services gouvernementaux pour examiner plus largement les liens entre l'État et les communautés des Premières Nations. Le Soleil (La Presse); Radio Canada

Permanent protection for police HQ remains 2 years away
Winnipeg's new police headquarters may be stuck with temporary protection against drive-up vehicle attacks for another two years, according to a plan to replace concrete slabs with a more permanent and more esthetically pleasing alternative. A city plan to improve downtown streetscaping calls for permanent bollards to replace temporary Jersey barriers — upright concrete slabs — around the police headquarters by 2019. CBC News; CTV News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Investigation, cleanup underway after riot at Saskatchewan Penitentiary
A Saskatchewan prison where a major riot took place this week had the most complaints of any penitentiaries in the country last year, according to Canada's prisoners' ombudsman. Howard Sapers, the Correctional Investigator of Canada, says there were 413 complaints about things including food, health care, family visits and access to parole hearings from inmates at the Saskatchewan Penitentiary in Prince Albert. One inmate was killed during the riot Wednesday, as prisoners set fires, smashed windows and pulled heat registers off walls. Sapers says it's extremely troubling to hear about the incident because it speaks to a real dysfunction in an institution. He has sent a team from his office to investigate, along with RCMP, the Union of Canadian Correctional Officers and Correctional Service Canada. Canadian Press (Sudbury.com; Province; Vancouver Sun; Leader-Post; CP24); AM 650 CKOM

'They were setting fires': New details emerge about deadly Saskatchewan prison riot
A more detailed picture emerged Friday about a deadly riot that broke out at a federal prison in Prince Albert, Sask. Jason Leonard Bird, 43, who was serving a 31-month sentence for breaking and entering, died in Wednesday's rampage at Saskatchewan Penitentiary. Eight other inmates were hurt, two seriously. James Bloomfield of the Union of Canadian Correctional Officers spoke to the National Post's Douglas Quan. Postmedia Network (Montreal Gazette; Province)

Family of Jason Bird grieving following his death at Sask. prison
Holly Lynn Lafond says underneath his tough exterior, her older brother Jason Leonard Bird was a man who had a heart of gold... Prison watchdog Howard Sapers said in his experience the issue is likely bigger than food. "There's been a lot of changes around food in Canadian penitentiaries and so it's not just that there wasn't enough food or just that the food wasn't very appetizing, although both of those things may be true — there's usually a lot more behind it," Sapers told CBC Radio's Morning Edition. Sapers said while double bunking and use of segregation is down in federal prisons, other things have the institutions in flux. "We've seen trends going up in terms of assaults, use of pepper spray, use-of-force incidents, lockdowns. [Prince Albert] is not unique in that regard," Sapers said. Staff from Sapers' office are on their way to Prince Albert today to further investigate the cause of the riot. CBC News; Radio Canada

Prison violence won't stop until overcrowding addressed, says former inmate
For many familiar with this country's correctional facilities, news of prison riots is not surprising. For years across Canada, violence in prisons has been steadily rising. Lee Chapelle has 100 convictions on his record — all of them property-related and non-violent in nature. He's spent 21 years in prison and tells The Current's Friday host Piya Chattopadhyay that overcrowding plays a huge role in prison violence... He suggests "public safety should come to the forefront," to make Canada's prison system work better for the people that are incarcerated inside them. "If they are not violent, scary people and don't have a long history, let's look at alternative sentencing - restorative," Chapelle says. "I think we really need to restore our belief in the potential of rehabilitation." CBC – The Current

Alberta jails battling the scourge of drugs
With more than three-quarters of incoming inmates having addictions, stemming the flow of drugs and other contraband in prisons is a priority, officials say. It has become even more crucial as toxic narcotics such as fentanyl are being smuggled into institutions and unsuspecting staff and prisoners are exposed. "Almost 80 per cent of offenders arrive at federal institutions with some level of substance abuse problem, and many have multiple addictions," said Jeff Campbell, spokesman with the Correctional Service of Canada (CSC). "We acknowledge the prevalence of substance abuse problems among offenders and assist in addressing those problems through a drug strategy." A Bowden Institution guard collapsed this week during a search for drugs and it's believed he was exposed to fentanyl. Postmedia Network (Calgary Sun)

Care homes being warned about high-risk sex offender who abused seniors
Vancouver police say they will visit care homes to tell them about the release of a high-risk sex offender who's known for targeting seniors. James Burrows, 56, was convicted of four sexual assaults against women between the ages of 72 and 93 years old, and has just been released from prison. He is currently residing in a halfway house somewhere in the city, although the exact location is being withheld due to

privacy laws. Because he is from "back east," police say there are no indications that he will stay in B.C. – but they wanted to warn the public because of his "disturbing past." An assessment by the Correctional Service of Canada found Burrows is a high-risk for violent and sexual re-offending. CTV News; CKNW News; Global News; BC Local News

Canada's federal jails may stop sorting trans inmates by their genitalia
Canada's federal prison system could soon scrap a longstanding policy of housing trans and intersex offenders based on their genitalia while effectively barring them from gender-confirming surgeries, Xtra has learned. Since at least 1999, Correctional Service Canada (CSC) has sorted trans inmates who haven't transitioned based on their genitalia. CSC's current "gender dysphoria" policy allows for hormone therapy. However, it restricts gender-confirmation surgery to those who have spent "12 continuous months in an identity-congruent gender role," while only counting months prior to their incarceration. But that will likely change soon. In an email to Xtra, CSC spokesperson Lori Halfper says the policy "is currently being reviewed after recent consultations," including the clause that jail time doesn't count towards the 12 months. "The revised guideline should be finalized and published this winter," Halfper writes. Daily Xtra

Ontario Correctional Services Minister David Orazietti quits
Liberal cabinet minister David Orazietti is resigning from provincial politics, setting the stage for a byelection in his northern Ontario riding about a year before the next general election. The Community Safety and Correctional Services minister made the announcement in his Sault Ste. Marie riding Friday, saying he is leaving for family reasons… Orazietti took on the corrections file in June, at a time of increasing public scrutiny and anger over solitary confinement practices. He had to answer for the treatment of Adam Capay, an inmate held in segregation for four years in Thunder Bay. Orazietti recently announced he had tapped federal correctional investigator Howard Sapers to lead a provincial review into the use of segregation. Just one day before his resignation, Orazietti announced the province was hiring more corrections staff, including officers, nurses, psychologists and segregation managers in an attempt to address issues with solitary confinement and inmates with mental-health challenges. Canadian Press (Ottawa Citizen; Globe and Mail); CTV News; Canadian Press (CTV News); Toronto Star

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Le fentanyl tue 9 personnes en une nuit à Vancouver
Des surdoses de fentanyl ont provoqué la mort de neuf personnes à Vancouver dans la nuit de jeudi à vendredi, a déclaré le chef de la police municipale, Adam Palmer, en conférence de presse. Le maire de Vancouver, Gregor Robertson, se tenait debout à ses côtés… Adam Palmer affirme que les toxicomanes ont besoin d'une aide immédiate. Il n'existe pas assez de lits pour les aider à surmonter leur dépendance et il faut parfois les transférer jusqu'à Nanaimo sur l'île de Vancouver. D'après le maire Gregor Robertson, les toxicomanes attendent huit ou neuf jours avant de pouvoir être pris en charge par les autorités sanitaires, ce qui est « inacceptable » lorsqu'environ 1300 personnes prennent des opioïdes illicites chaque jour. Radio Canada; Postmedia Network (National Post); Canadian Press (Huffington Post; City News); CTV News; CBC News

Calgary police chief open to supervised-injection sites
Calgary's police chief is open to introducing supervised facilities for drug users, so long as such programs are part of a larger strategy to lower addiction rates and address problems that accompany drug dependency, such as crime and joblessness. "It always makes police chiefs look resistant when they say no to these things. My answer has been: 'Sure, as long as it is part of a better strategy,'" Calgary Police Service chief Roger Chaffin said in an interview this week. "I'd be more mindful of it if it was part of a more robust strategy to lower the issues of addiction." Globe and Mail

In The Mayor's Chair
Steinbach City Councillor Earl Funk got to be Mayor for the morning. Funk sat in the Mayor's chair Friday for the monthly open door session… Meanwhile, Funk also sat down Friday morning with a member of

the local Citizens On Patrol Program (COPP). "I just want to really thank the entire group, all the members for what they do for our city and how they tirelessly provide security for us, they work very closely with the RCMP," he says. Funk says earlier this week when he stopped by his business late at night, there were COPP volunteers patrolling the area. He notes that provided a level of comfort to know that his store was being looked after while he was at home resting. He adds COPP is always looking for new recruits. Further to that he says this time of year they are stressing the importance of locking our doors. Steinbach Online

Allan Waugh's family seeks answers, justice and peace
A week away from Christmas, a Yukon family is asking for one thing: to know what happened to their father. On Monday the Waugh family made yet another public appeal asking anybody with information about the 2014 murder of 69-year-old Allan Waugh to come forward… Now they want to take advantage of the new Crime Stoppers program that relaunched last week after a five-year hiatus. The program passes on anonymous tips to the RCMP. If the tip leads to an arrest, the tipster could collect a cash reward. Yukon News

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Man charged in 2014 death of Indigenous woman in Edmonton's west end
Edmonton police have charged a man with second-degree murder in the death of a woman in Edmonton's west end in 2014. Freda Goodrunning was 35 when her body was found in a storage shed at 174th Street and Stony Plain Road on June 4, 2014. She died of blunt force trauma, police said. A Cree woman from the Sunchild First Nation, Goodrunning had lived on the streets for the final four years of her life, according to police… She had been married with six children, and was considered one of Alberta's unsolved cases of missing and murdered Indigenous women. On Wednesday police arrested and charged a 33-year-old man with second degree murder and possession of an offensive weapon. CBC News; Turtle Island News

A 'tub of ugly:' Stories of victims turned survivors
Her diaries, trial transcripts, letters, newspaper clippings, and videos of television reports were put in storage years earlier, in a large plastic tote marked "trial stuff." Such a simple and mundane label, it didn't aptly describe the evil contained there. The contents reflected horrific acts of sexual violence committed against children, teens and women spanning three decades… A dangerous sexual predator, the senseless murder of a teenage girl, a missing indigenous woman ultimately found murdered — they were shocking crimes that dominated the news anywhere from a decade to three decades ago. But what happens next, after the trial ends, the offender goes to prison and the crime falls from the headlines? Visit a courtroom on any given day, and you'll hear about the long-term devastation wrought by such trauma, the suffering at times leading to alcoholism, addiction, or worse, victims turned perpetrators. These are the other stories, of victims who became survivors. Shaped by their experiences, they found ways to move beyond them to help themselves and others. Postmedia Network (Leader-Post)

7,420 kms With Caribou Legs to End Violence Against Women
This week I'm sharing part of a speech I gave in tribute to ultra-marathon runner, Brad Firth AKA Caribou Legs, who crossed Canada over 7 months to raise awareness about missing and murdered Indigenous women and girls (#MMIW, #MMIWG). Brad's work was an epic adventure that also happened to occur not long before the long-awaited official inquiry into the issue by the Canadian government commenced. This adventure was an eye-opener for many Canadians who, despite news coverage of varying degrees, didn't know of the depth of the subject, nor why Indigenous groups were fervently calling for that inquiry. It was also a stark reminder for those of us who do know the background, that we must always remember, regardless of how well we know our issues and think we've publicized them, we're not even close to having reached the populace in Canada or the U.S. Blog Woman!!!

Anti-Poverty Activist Looking to Replace NDP MLA Kevin Chief
Only one day after NDP MLA Kevin Chief announced he's stepping down from provincial politics, another well-known Manitoba is stepping up to the plate. Bernadette Smith, an anti-poverty activist and co-founder of the Manitoba Coalition of Families of Missing and Murdered Women in Manitoba and the Drag the Red Initiative is looking for the NDP nomination for the Point Douglas riding. AM 770 CHQR; Postmedia Network (Winnipeg Sun); CBC News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Cannabis Canada supports Task Force recommendations for legalization of marijuana
"Overall, the Task Force has succeeded in providing the federal government with a set of well-informed and comprehensive recommendations that will guide the development of legislation for the legalization and regulation of cannabis in Canada," said Colette Rivet, Executive Director of Cannabis Canada Association. Rivet says that Cannabis Canada encourages the government to allow product branding and advertisements for cannabis that in no way appeals to children, which is one thing that the Task Force recommended. Along with recommending that the packaging the product don't appeal to children, the Task Force also suggests an age restriction for purchasing cannabis, re-sealable and childproof packaging, comprehensive labelling and a well developed public education campaign. Kelowna Now

Le SPVM frappe une boutique de pot illégal
Les agents du Service de police de la Ville de Montréal ont frappé au moins une des boutiques de pot illégal qui avait ouvert ses portes il y a seulement 24 heures, celle sur Mont-Royal. Dans ces boutiques administrées par la compagnie de Vancouver Cannabis Culture, on ne trouvait pas du pot médicinal, mais bien du pot récréatif. TVA Nouvelles; La Presse; Canadian Presse (Vancouver Sun); CTV News; Le Devoir

Saskatchewan Compassion Club trio headed to trial
Three people charged in a bust of a medical marijuana dispensary have been committed to trial. A preliminary hearing for Mark Hauk, Jeff Lundstrom and Jaime Michelle Hagel wrapped up in Saskatoon Provincial court on Thursday. The three have been charged with trafficking marijuana and cannabis resin and possession of a controlled substance for the purpose of trafficking. Police raided the Saskatchewan Compassion Club in October of 2015. Marijuana was seized from the club, which eventually closed down, although it still has a presence online. CBC News

How Weed Is Helping Opioid Users Beat Addiction
... The Liberal government's Task Force on Cannabis Legalization and Regulation released dozens of recommendations this week on how the legal weed regime in Canada should look. While much of the report focused on recreational use, it also recommended more clinical research about the medical use of cannabis with the aim of bringing cannabis-based drugs onto the market. But some Canadians, including doctors and patients who deal with pain, are asking why the government hasn't already embraced cannabis as an alternative to opioids—especially with the country in the grips of a deadly overdose crisis. Vice News

Canada Is On Track To Legalize Cannabis, But Here's Why It Will Still Be A Bumpy Ride
This week, Canada's cannabis task force released a report with 80 recommendations for the federal government to consider while drafting regulations for the country's legal recreational marijuana market. But even with that intel, the road to legalization will be a bumpy ride as Canada becomes the second country in the world to legalize recreational marijuana (after Uruguay). Here are six reasons why the road ahead will be rocky but still worthwhile for Canada to take. Civilized

Details of marijuana regulation remain hazy
Legal weed may not be the "revenue cash cow" provinces and territories were hoping for, says the Yukon's assistant deputy minister of justice. While the recreational marijuana market will open up new

revenue streams, said Al Lucier, those dollars, at least in the early days, will be funneled into awareness and education campaigns, research and policy enforcement. "The regulatory and enforcement aspects that will come in with these changes will certainly offset revenues generated by the taxation of the products," Lucier said in an interview this week. He is also a senior official in a working group on the legalization, regulation and restriction of cannabis in Canada. On Tuesday, a cannabis legalization task force, chaired by former Liberal cabinet minister Anne McLellan, released a report with more than 80 recommendations for how to regulate marijuana and end nearly a century of prohibition in Canada. Whitehorse Daily Star

Legal weed will be ridiculously profitable — and a huge headache
An opinion piece states, "…So I read with some interest the way the task force on the legalization of cannabis sees the landscape facing Canada as we move towards becoming the first major developed nation to legalize recreational marijuana. "Like scraping ice from the car windows on a cold winter morning, we believe that we can now see enough to move forward," this week's report said. I wasn't reassured. Don't get me wrong. I understand the arguments in favour of legalization — that recreational use of cannabis is already widespread, that most of it is controlled by criminal elements who have no concern for the quality of the product and its impact on society. And does it really make sense for our police forces to be wasting so much time and effort on arresting pot users? The report notes that 49,577 of the 96,423 police-registered drug charges in 2015 were for possession of cannabis. Yet the report and its 80 recommendations makes for sobering reading. It shows how hugely complicated setting up a national regime to regulate the growing, sale and distribution of cannabis will be, let alone dealing with the health impacts and the surge in impaired driving cases that inevitably will result…" iPolitics

Good pot report stumbles on medical access
An opinion piece states, "The federal task on marijuana released a thorough report last week that proposes to end Canada's 93-year prohibition on legal pot production and consumption. Its 80 recommendations touched on the important considerations and concerns for a well-regulated system, and appeared to borrow from the experience of several U.S. states that are several years ahead of us. But the federal task force failed on one important point: the merger of the medical and recreational marijuana markets…" Times Colonist

Broadcast Media / Médias télédiffusés

CBC News' Power & Politics, interviewed Jenna Valleriani, a PhD candidate studying medical cannabis and strategic advisor for Canadian Students for Sensible Drug Policy regarding the Task Force on Cannabis Legalization and Regulation's Final Report. Rough Transcript

PUBLIC SERVICE / FONCTION PUBLIQUE

Bonuses for Phoenix executives still under review, department insists
Public Services and Procurement Canada insisted Friday that bonuses for executives responsible for the Phoenix pay system remain under review and have not been approved, after a department official said some involved in the project would get the incentive pay. The official, speaking on background Friday, told CBC News that performance pay had been approved for some executives involved with the troubled payroll system. But the department's media relations manager, Me'Shel Gulliver Bélanger, later contacted CBC News to apologize for any confusion and stressed that bonuses for the top decision-makers responsible for Phoenix were still under review. CBC News

Federal government departments have a 'dismal' record of hiring wounded veterans, senator says
Just over 25 per cent of veterans who were given priority hiring status in the federal public service because the military released them for medical reasons weren't able to find jobs, according to newly released statistics. Five hundred and eighty-five individuals released from the Canadian Forces for medical reasons between 2005 and early 2016 were unsuccessful in finding work with federal departments within the period for which they were allotted priority status for employment appointments, and as a result lost that status. That has prompted one Liberal senator to call on federal departments to

step up... Since 2005, when those medically released from the Forces have been eligible for priority status, the bulk of hiring of those eligible has been by the Department of National Defence. Since 2005, it has been responsible for 70 per cent of the hires of those with priority-status, some 928 veterans. Correctional Service Canada hired five per cent, or 66 veterans, according to the figures provided to Downe. Employment and Social Development Canada has been responsible for 4.2 per cent of the hires of those eligible, or 56 individuals, while Fisheries and Oceans, the RCMP, and Public Services and Procurement Canada were each hovering at around two per cent of the hires. Postmedia Network (National Post; Ottawa Citizen; Province; Vancouver Sun; Windsor Star)

Lower-cost alternative was ignored for stumbling, over-budget Canada.ca project
The federal government could have employed a simple framework for its massive Canada.ca web renewal project, making it much cheaper than the large corporate Adobe contract it signed, according to several sources familiar with the project. Ottawa Citizen

Government offices closed because of flooding, boiler failure
Readers are reporting that Department of National Defence offices at 25 Nicholas St. was evacuated due to power outage and sprinkler system outage. There has also been a flood there. It is unclear whether the whole building is affected or whether the issue was confined just to DND facilities. And the government building at 615 Booth St. has been shut down completely because of a boiler failure. The Department of National Defence has confirmed both. Repairs are under way at Booth Street and the building is expected to re-open on Saturday. At the Nicholas St., building, DND says a damage assessment is underway and it is uncertain when the building will be reopened. Ottawa Citizen

PSAC welcomes asbestos ban
The federal government has announced its commitment to banning asbestos and asbestos-containing products by 2018. This is a long-awaited decision; PSAC has been calling on the federal government to ban the import, export and manufacturing of asbestos for years. The federal government will create new regulations to ban asbestos, establish new federal workplace health and safety rules, and enhance the registry for federally owned buildings. "We welcome the government's decision to ban asbestos, which is the result of years of hard work by activists in the labour movement and our allies," said PSAC National President Robyn Benson. "Asbestos is the leading cause of workplace-related deaths in Canada; we must put an end to this epidemic." Public Service Alliance of Canada

OTHER / AUTRES

Canadian Armed Forces sergeant sentenced to six years in prison for child porn offences
A Canadian Armed Forces sergeant based at CFB Trenton in eastern Ontario has been sentenced to six years in prison for child pornography offences and arranging to commit a sexual offence against a child. Court officials in Belleville, Ont., say David Rodwell was sentenced yesterday. The 57-year-old air weapons system technician was convicted on Sept. 22 of possession of child pornography, making child pornography and making an agreement to commit a sexual offence against a child. He was arrested last year after an online sting involving a U.S. Homeland Security special agent posing as a mother of three. Canadian Press (Vancouver Sun; City News)

Coast Guard seizes 26.5 tons of cocaine
More than 26 tons of cocaine worth $2 billion have been seized by the US Coast Guard and Royal Canadian Navy, officials said Thursday. Approximately 100 suspected drug smugglers were apprehended at sea and turned over to federal authorities, said Vice Adm. Karl Schultz, commander of the U.S. Coast Guard Atlantic Area. The inter-agency operation intercepted 27 shipments and five bale recovery efforts over the course of 10 weeks, Schultz said. CNN

Tips for stress-free air travel this holiday season
Like creamy eggnog, holiday movie marathons and cookies for Santa Claus, airline travellers at Vancouver International Airport should be prepared to add one more holiday tradition to their list

this year: the long airport lineup. "Our partners at CATSA (Canadian Air Transport Security Authority) are doing a great job of adding staff, and all of our partners have been working for months having extra staff ready for the extra volumes, but you can be prepared to wait a little bit longer than normal," said Reg Krake, director of customer care at Vancouver International Airport. CBC News

INTERNATIONAL

NIL

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

RalphGoodale
Avant d'ajourner cette semaine, le Parlement a approuvé des investissements dans la sécurité nationale. #polcan

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

globalnews
An electromagnetic pulse from a solar storm or a nuclear blast would cause electrical meltdown. But are we prepared? http://glbn.ca/NF8hLt

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Global_Montreal
Man who killed soldier #PatriceVincent wanted more victims: #Quebec coroner https://t.co/xnyLEz01HK

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

ipoliticsca
Ottawa appoints special rep on First Nation border-crossing rights. @james_munson has more. | AP Photo http://ipoli.ca/2hCIlPT #cdnpoli

yvrairport
From toy guns to live ammo & large liquids - a few things surrendered to @catsa_gc recently at screening. Don't pack these in your carry on! https://pbs.twimg.com/media/Cz0MHE8VEAAMiQj.jpg

CYBER SECURITY / CYBERSÉCURITÉ

Justin_Ling
The Canadian military has a new cyber defense plan in the works. And it's...interesting. https://t.co/WtlyoI87JZ

ipoliticsca
One quarter of Canadian online traffic vulnerable to NSA sweeps: researchers. Our @amandacconn reports. http://ipoli.ca/2gTojzd #cdnpoli

PeterFinnWP
FBI backs CIA view that Russia intervened to help Trump win election https://t.co/jBEgwRyazE

CP24

Yahoo faces proposed Canadian class action following hacks http://www.cp24.com/lifestyle/technology/yahoo-faces-proposed-canadian-class-action-following-hacks-1.3206838 …

LAW ENFORCEMENT / APPLICATION DE LA LOI

OttawaCitizen
RCMP seize furanylfentanyl — an extremely potent drug with a similar compound to fentanyl — in raid on Orléans home https://t.co/b3vwuPane8

SurreyRCMP
Receive the latest policing info from #SurreyBC by e-mail: http://ow.ly/4yeQ307aGn4 or through our mobile app: http://ow.ly/NUjN307aH3i

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Sheila_Scott
VPD warning about high risk sex offender (who targets seniors) living in Vancouver. Did story on this guy in March.. http://bc.ctvnews.ca/care-homes-being-warned-about-high-risk-sex-offender-who-abused-seniors-1.2803326 …

CityCristinaH
. @MPPKevinFlynn (MOL) now acting #corrections minister, following @DavidOrazietti 's resignation. @CityNews #onpoli

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

rp_browne
Vancouver police calling for more treatment following 9 overdose deaths last night. Our story on existing options: https://t.co/y6gHsjAqkl

ChiefPalmer
People are dying - we need better treatment services - #TreatmentOnDemand @VancouverPD @CityofVancouver @VanFireRescue

AndreaWoo
Takeaway from #Vancouver mayor/police presser: Harm reduction very important. But we desperately, urgently need more treatment options

tlupick
Last night 13 people in B.C. died of a suspected drug overdose. 1 night. 13 families. Coroners Service release: #bcpoli #fentanyl

CTVVancouver
Developing: Police chief says city is failing drug users. "They are at risk of dying if we don't help them." https://t.co/NipgQmAPGe

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

AmnestyNow
Our human rights report card found that concerns raised about the #MMIW Inquiry were not addressed>>http://amn.st/60158MRzf

caribouleg1
7,420 kms With Caribou Legs to End Violence Against Women #MMIW #MMIWG #Indigenous #cdnmedia https://blog-woman.com/2016/12/16/7420-kms-with-caribou-legs/ … via @robynwins111

fdastous

Site web de l'Enquête nationale sur les femmes + filles autochtones disparues et assassinées -> http://bit.ly/2gPSCc0 via @FFADA #MMIW

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

toinz
Police raiding Cannabis Culture in Little Italy

davidakin
The Emerys couldn't wait for these shops to be legal. And now they'll never get a license even when it is legal.

amil
Can weed help people curb their opioid addictions? These Canadians are proving it can. @joerogan http://www.vice.com/en_ca/read/how-weed-is-curbing-opioid-addiction-for-some-canadians … @vicecanada

tvanouvelles
À VOIR | Le «prince du pot» prêt à être arrêté http://bit.ly/2hD1tNC cc @poirieryvesTVA

ipoliticsca
OPINION: Legal weed will be ridiculously profitable — and a huge headache, says Alan Freeman http://bit.ly/2hGUC30 #cdnpoli

PnPCBC
.@jennav5 welcomes 18 as pot age, challenges research about impact on developing brain. #cdnpoli #pnpcbc

PUBLIC SERVICE / FONCTION PUBLIQUE

CBCKatie
UPDATE: this single mom had her expense claim approved after her story aired on CBC News: https://t.co/fzYXoZwBdj

CBCKatie
As explained to me today by the department, some mangers who had involvement with Phoenix will get performance pay: https://t.co/GdTl2ai4Bq

CBCKatie
Some background on how the Phoenix bonus story evolved. CBC News received a tip about bonuses on Monday. Put in Qs to PSPC to ask if...

CBCKatie
...bonuses (or performance pay) for executives involved with Phoenix was going to be handed out. Tuesday we got a statement....

CBCKatie
Story update to come. Again - PSPC official provided me with inaccurate information. Correct update coming.

OttawaCitizen
Government offices closed because of flooding, boiler failure http://ow.ly/h1fA507DCFJ #ottnews

INTERNATIONAL

MagnusRanstorp
Saudi Arabia and Gulf states 'support Islamic extremism in Germany,' intelligence report finds | The Independent https://t.co/emFYBtVGZl

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

BLANK PAGE / PAGE BLANCHE

Today's News / Actualités
December 20, 2016 / le 20 décembre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

TOP STORIES / MANCHETTES

Missing and murdered Indigenous women inquiry launches new website
Families of missing and murdered Indigenous women should sign up for MMIW inquiry emails while they wait to register to participate, inquiry commission officials say. The emails will provide updates ahead of the inquiry, which is expected to begin in spring. "We want to create a families first process," said Michael Hutchinson, the commission's director of communications. "Nobody has a list of the people that

want to take part in the national inquiry.... We're trying to collect that information from families." The MMIW inquiry has a new website, where families should be able to register soon. The inquiry has five commissioners who in the new year will hear testimony from families of missing and murdered Indigenous women and others in order to examine the systemic causes of violence against Indigenous women and girls in Canada, and make recommendations about how to prevent violence against Indigenous women. CBC News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Ferocious Fort McMurray wildfire voted news story of the year for 2016
The ferocious wildfire that forced nearly 90,000 to flee Canada's oilsands region and reduced thousands of homes to rubble has been picked as the top news story of 2016 in an annual survey of newsrooms across Canada. Dubbed "the beast" for its merciless unpredictability, the Fort McMurray wildfire garnered 39 of the 67 votes cast by senior editors. It was followed by Canada's ongoing resettlement of Syrian refugees with 11 votes, the fentanyl crisis with six and the Tragically Hip's farewell tour with five. "Not even a Hollywood script could match the terror, uncertainty, and heroism to come out of what seemed to be a surreal event," wrote Dave Barry, news director of CKPG TV in Prince George, B.C. Canadian Press (Brandon Sun, Winnipeg Free Press, Metro News, Global News, 570 News, Globe and Mail)

Sask. government rejects privacy commissioner's recommendation to release Husky pipeline records
The Saskatchewan government has rejected a recommendation from the provincial privacy commissioner to release records and information about Husky Energy pipeline inspections. In a report focused on the Ministry of the Economy, the Office of the Saskatchewan Information and Privacy Commissioner says the government should not have withheld records in response to an access to information request. On July 21, about 200,000 litres of heavy oil mixed with another petroleum product spilled into the North Saskatchewan River from a Husky pipeline near Lloydminster, Sask. The cities of Prince Albert, Melfort and North Battleford had to temporarily shut down their drinking water intake from the river and find other means to supply their residents with drinking water. CBC News (2016-12-19)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Fête du Nouvel An : la sécurité à l'ordre du jour
L'attentat survenu lundi au Marché de Noël de Berlin fait réfléchir sur les mesures de sécurité à l'approche des célébrations du Nouvel An sur la Grande Allée à Québec. La sécurité sera d'ailleurs au coeur des discussions lors d'une rencontre qui était déjà prévue mercredi entre les organisateurs de la fête, les services de sécurité et la Ville de Québec. La Ville ne veut pas confirmer si elle envisage des mesures supplémentaires et de quelle nature elles pourraient être. Marie-Ève Painchaud, porte-parole du Service de police de la Ville de Québec, souligne que le risque n'est pas le même à Québec, mais que la Ville est bien outillée. Radio-Canada

Eight reasons why Canada must repeal its anti-terror laws
An opinion piece states, ""Sunny ways my friends," Canadian prime Minister Justin Trudeau told his supporters on election night last year. "Sunny ways. This is what positive politics can do." One of Trudeau's main campaign promises was to hold public consultations to review and amend draconian national security laws (known as Bill C-51 at the time) that the outgoing Conservative government enacted prior to being thrown out in 2015. After public consultations wrapped up last week, many are now awaiting to see if sunlight will disinfect the national security shadow. Like most countries, Canada's legal landscape underwent a seismic shift in the immediate aftermath of 9/11. The Liberal government, led at the time by prime minister Jean Chretien, enacted a slew of national security laws and policies. They included the 2001 Anti-Terrorism Act, which echoed the infamous American Patriot Act. (...) Canada's spy agency, the Canadian Security Intelligence Service (CSIS), was created in 1984 as a civilian agency to address abuses of power that occurred when the Royal Canadian Mounted Police (RCMP) handled both intelligence and law enforcement. The Anti-Terrorism Act of 2015 radically expands

the powers of the CSIS, and disregards constitutional protections. (…) Thousands of Canadian Muslims and Arabs have had to submit themselves to "voluntary" interviews with the CSIS. The number and frequency will undoubtedly increase under the new laws. Many of these people are ensnared in the national security web merely through guilt by association and the inevitable false positives." Middle East Eye

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

The Lie-Detecting Security: Kiosk of the Future
SDSU professor is developing a robotic kiosk that could help detect travelers with sinister intentions. When you engage in international travel, you may one day find yourself face-to-face with border security that is polite, bilingual and responsive—and robotic. The Automated Virtual Agent for Truth Assessments in Real Time (AVATAR) is currently being tested in conjunction with the Canadian Border Services Agency (CBSA) to help border security agents determine whether travelers coming into Canada may have undisclosed motives for entering the country. (…) In the meantime, Elkins is looking for a government agency willing to utilize the technology in a real-world application. "AVATAR has been tested in labs, in airports and at border crossing stations," Elkins noted. "The system is fully ready for implementation to help stem the flow of contraband, thwart fleeing criminals, and detect potential terrorists and many other applications in the effort to secure international border. San Diego Metro

Why are public schools recruiting adult students overseas?
The Quebec government encourages school boards to conduct vocational training Quebec English School Boards Association president Jennifer Maccarone told The Suburban. "Emploi Québec dictates if, say, we need 40 skilled workers in a particular region in welding and fitting, 100 new jobs in secretarial and another number in plumbing and fitting," she explained in an interview last month. "We hold regular meetings with universities CEGEPs and school boards to work with Emploi Québec to determine what programs we need to be backing away from because there is a surplus and which ones will see growth in demand." The results are then coordinated with provincial education and immigration officials, to ensure that Quebec has sufficient qualified workers to keep its economy thriving. The vocational studies thus indirectly help international students to apply for permanent residence, so they can remain here and make a useful contribution by reducing Canada's skilled worker shortage, once they complete their program. "People come here to get a profession," English Montreal School Board (EMSB), communication and marketing specialist Michael Cohen told The Suburban. "Many apply to immigrate and Quebec gets workers skilled and able to pay taxes." Suburban

Americans dream of Canada after Trump
As electoral college votes in Donald Trump, many US citizens plan move to Canada, but may face cold reception. Lola Al-Uqdah won't soon forget the morning of November 9. A mother of three and psychology professor who lives in Camden, New Jersey, Al-Uqdah was in the midst of her usual pre-work routine when she learned that Donald Trump had defeated Hillary Clinton to become the next president of the United States. It was the morning after the US election and her husband had delivered the message through the bathroom door. (…) Her American Dream was dead. There was only one thing left to do: plan her move to Canada. Al-Uqdah is one of hundreds, if not thousands of Americans who, during the election, contemplated moving to Canada if Trump won. But unlike the vast majority of liberal anti-Trumpers who flip-flopped on Canada once the billionaire real estate mogul pulled off a stunning victory, Al-Uqdah was serious. For Al-Uqdah, a Muslim woman, a Trump presidency wasn't just an inconvenience - it was a terrifying reality. AlJazeera

Gypsum tariffs will save Canadian manufacturing jobs
An opinion piece states, "The International Brotherhood of Boilermakers represent 120 workers employed at CertainTeed Gypsum (CTG) wallboard manufacturing operations in Western Canada and we are concerned their jobs are at stake. We appeared before the Canadian International Trade Tribunal (CITT) to explain what happens to laid-off workers and why Canada should not change its 112-year-old policy of fighting the evils of dumping. Our members have already lost over 100 well-paid, middle-class union jobs at idled gypsum plants in Western Canada and we cannot afford to lose 120 more. David Campbell, of

Empire Drywall Ltd., presented an argument on Dec. 13 in the Edmonton Journal, for why U.S. drywall producers should be given a licence to engage in what the Canada Border Services Agency (CBSA) has already determined to be illegal dumping. We disagree with this notion. Ottawa must not give U.S. producers a licence to dump gypsum board and steal our jobs; to do so would be a miscarriage of justice. Western Canada needs jobs and potential investors must be convinced that they will have protection against unfair trade practices." Edmonton Journal

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

ShadowBrokers Dump Came from Internal Code Repository, Insider
An analysis of the latest ShadowBrokers dump of alleged NSA spy tools points to an insider with access to a code repository belonging to the intelligence agency, experts said. Researchers at security company Flashpoint said today that its investigation of the leaked data points away from an attack against NSA infrastructure, or other theories that operators mistakenly left classified data on staging servers, for example. Instead, clues in code made available last week point toward an NSA employee or contractor. Threatpost

Privacy groups complain to FTC over Google's 'deceptive' policy change
Privacy groups have complained to the Federal Trade Commission that Google is encroaching on user privacy through a policy change in June that allows it to combine personally identifiable information with browsing data collected by its DoubleClick digital advertising service. The complaint, by Consumer Watchdog and Privacy Rights Clearing House, alleged that Google has created "super-profiles" as it can track user activity on Android mobile phones, with an 88 percent market share of smartphones worldwide. The information can also be gleaned "from any website that uses Google Analytics, hosts YouTube videos, or displays ads served by DoubleClick or AdSense," according to the complaint. Computerworld

Malware Exchange Busted by the Feds Relaunches, At Least in Name
The digital underground is a fragile place, with hacking forums sometimes being shuttered by police. That's what happened to malware-marketplace Darkode last year: in coordinated raids, the FBI, UK's National Crime Agency, and a slew of other law enforcement bodies arrested over 70 hackers and closed the popular site. Now, Darkode, is back, at least in name. Motherboard

Hackers Might Have Turned Off the Lights in Ukraine for the Second Time
Ukraine experienced a new power outage during the weekend, and it's believed that hackers are once again responsible, after they previously breached energy companies in 2015. Softpedia; Bleeping Computer

This is your captain speaking... or is it?
Vulnerabilities in Panasonic in-flight entertainment systems create a possible mechanism for attackers to control in-flight displays, PA systems and lighting, say researchers. Ruben Santamarta, principal security consultant at IOActive, said it had found vulnerabilities in Panasonic Avionic In-Flight Entertainment (IFE) systems that it claims could allow hackers to "hijack" passengers' in-flight displays and, in some instances, potentially access their credit card information. The research revealed it would also theoretically be possible that such a vulnerability could present an entry point to the wider network, including the aircraft controls domain. Register; Infosecurity Magazine

Hailstorm methods used to spread malware in phishing attacks
Cisco Talos researchers have spotted Hailstorm spam tactics used to evade cyber defenses and spread malware via phishing attacks. Rather than send large volumes of mail for large periods of time, hailstorm campaigns send larges bursts of spam over very short periods of time, according to a Dec. 19 blog post. The spam is sent via IP addresses located around the world with the intent of flying under the radar with respect to any reputation or volume-based metrics that could be applied by anti-spam systems. SC Magazine

Evolved DNSChanger malware slings evil ads at PCs, hijacks routers

Malware that spreads via evil web ads and menaces broadband routers has been discovered – and it's going to be particularly horrible for small business and home internet users, which it targets. This latest variant of the years-old DNSChanger nasty, just spotted by Californian infosec biz Proofpoint, works like this: some JavaScript code is hidden in advertisements placed on mainstream websites via ad networks. The code – which prefers Chrome on Windows and Android – checks for the local IP address of the browser visiting the site using a WebRTC request to a Mozilla STUN server. Register

Mobile banking trojans adopt ransomware features
Cybercriminals are adding file-encrypting features to traditional mobile banking trojans, creating hybrid threats that can steal sensitive information and lock user files at the same time. One such trojan is called Faketoken and its primary functionality is to generate fake login screens for more than 2,000 financial applications in order to steal login credentials. Computerworld

Inside LeakedSource and Its Database of 3 Billion Hacked Accounts
By now it's hard to keep track of which companies have been hacked and which haven't. Remember the FourSquare hack? What about Adobe? Even breaches that were high-profile at the time are fading into obscurity as bigger and scarier ones crop up. (Ahem, Yahoo.) And if you can't remember what's been hacked, you're probably struggling to keep track of which leaks have included your personal data. That's where "the Google of data breaches" comes in. LeakedSource is a service that sends email notifications about new breaches and offers a database of information stolen in hacks. Its basic services—the ability to sign up for email notifications and search the database—are free, but users can pay to access more advanced search functionality. Wired Magazine

LAW ENFORCEMENT / APPLICATION DE LA LOI

Scars on his body remind boy of abuse he suffered in Mountie's basement
The boy who was restrained, tortured, sexually abused and neglected in the basement of his family's home told court in a recorded victim impact statement that while he's doing better, the scars on his body remind him of the abuse he suffered. He was 11 when his parents were arrested in February 2013 and is now 14 years old. He appeared in Ontario Superior Court in Ottawa Tuesday via a video recorded last week. The boy looked healthy, though his voice sometimes cracked. He said he avoids answering questions about the scars on his body and that he's reminded in the shower about what he endured when he sees the red marks around his ankles from his restraints. He said he knows he needs psychological help, and that he one day hopes to be able to put the memories aside. Her Mountie husband — the boy's father — was found guilty of aggravated assault, sexual assault causing bodily harm, forcible confinement and failing to provide the necessaries of life. He has been suspended from the RCMP without pay. The Mountie is expected to be sentenced in March. CBC News

RCMP sing at six care homes in Parksville Qualicum Beach
Residents at a half-dozen Parksville and Qualicum Beach care homes were serenaded with Christmas carols Thursday by an unusual choral group — the Oceanside RCMP. Outfitted in red serge and supported by several family members, civilian office staff and women from the victims services department, a group of 18 detachment members regaled seniors with classic carols in a one-day tour of brief stops. Parksville Qualicum Beach News

Police constable debunks Vader's claim strip search was 'humiliating'
A constable involved in the strip search of Travis Vader in 2010 at the Edson RCMP detachment told an Edmonton courtroom he was just following instructions from a superior officer. Const. Steven McQueen, with the Edmonton serious crimes unit, testified at Vader's sentencing hearing Monday that he and another officer brought Vader to an empty cell where they proceeded to "secure his clothes as potential evidence." They searched for weapons and drugs, McQueen said, then gave Vader a fresh T-shirt, sweatpants and socks to wear as they put his clothes in an evidence bag. Vader was naked for less than a minute in a quiet cell with nobody else around, McQueen said, suggesting the search was routine and requested by a superior. Last week, Vader testified the strip search went on for five minutes, with the

door to the holding cell left open where "everybody could see." He called the experience "absolutely humiliating." CBC News

Calgary police chief announces independent review of officer-involved shootings
Calgary's police chief announced on Monday there will be an independent review into officer-involved shootings in Calgary. Speaking before Calgary city council, Chief Roger Chaffin said he wants the review to be conducted by someone outside of the City of Calgary and Calgary Police Service. They have been 10 officer-involved shootings in Calgary so far in 2016, five of which were fatal. There were three in 2015. Chaffin has attributed the increase to a changing nature of crime in the city, citing the presence of meth and opioids on the Calgary streets as driving factors. Calgary Mayor Naheed Nenshi said an independent review is the right approach. A provincial watchdog does review officer-involved shootings in Alberta. The Alberta Serious Incident Response Team (ASIRT) determines if officers acted appropriately and whether or not any wrongdoing took place. Global News

Body found on Big Island Lake Cree Nation during RCMP theft investigation
RCMP believe the death of a person found on the Big Island Lake Cree Nation as officers investigated a theft is suspicious. Mounties say officers were investigating a theft Tuesday at about 5 a.m. when police found the deceased male — officers do not yet know his age — outdoors on the First Nation. Investigators do not yet know the circumstances of the death or the body's identity, but police do believe the death is suspicious. The RCMP's major crimes north unit and forensic identification section are investigating alongside the officers from Pierceland, the Meadow Lake detachment's police dog unit and the coroner's office. CTV News Saskatoon; StarPhoenix; CBC News

Vigil grows at apparent murder-suicide scene in Spruce Grove
With just days to go before Christmas, an Alberta family will spend the holidays planning funerals, instead of celebrating. Two hockey sticks, two teddy bears and a collection of flowers formed a memorial on the front lawn of a home west of Edmonton, where two brothers and their father were found dead Monday morning in what appears to be a murder-suicide. The bodies discovered inside the home were those of Corry MacDougall and his sons, 13-year-old Ryder MacDougall and 11-year-old Radek MacDougall. Brent Stark, the boys' stepfather, spoke to Global News Monday evening. He said it was he and the boys' mother Tracy who discovered the bodies and called police. He also said he believes Corry killed his sons in an apparent murder-suicide. RCMP confirmed that the bodies of three people were found in the home at 2 Haney Ct. Monday morning and that they are not looking for any suspects. Global News

RCMP looking for Big River teen
A 13-year-old girl from the Big River area has been reported missing. Maria McAdam, who also goes by 'Littlechief,' was reported missing on Dec. 18. She was last seen at a school on Dec. 16 and was supposed to be at a friend's home over the weekend, but this wasn't the case. PA Now

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

L'ex-juge Delisle saura s'il peut reprendre sa liberté mardi
L'ex-juge Jacques Delisle saura mardi s'il peut recouvrir sa liberté en attendant que la ministre fédérale de la justice détermine s'il a été victime, ou non, d'une erreur judiciaire en étant condamné pour le meurtre de sa femme. Ces dernières semaines, les avocats de M. Delisle ont tenté de démontrer que l'homme est innocent du crime pour lequel il a été condamné en 2012 à la prison à perpétuité en présentant une nouvelle analyse balistique. M. Delisle, aujourd'hui âgé de 81 ans, a passé les quatre dernières années derrière les barreaux suite au meurtre de sa femme survenue en 2009. Agence QMI (Journal de Québec, Journal de Montréal); TVA Nouvelles

Saskatchewan Penitentiary remains under lockdown following riot
A lockdown at the Saskatchewan Penitentiary remains in place after 185 inmates in medium security destroyed parts of the prison during a deadly riot last Wednesday. There are still plenty of questions as to what sparked the riot but it appears food portions being served to inmates may have played a role.

During the rampage, six inmates suffered non-life threatening injuries after being hit by shotgun pellets. Another three were sent to hospital in serious condition after being assaulted by other prisoners, including Jason Leonard Bird, who died Wednesday evening. A wake for Bird will take place on Tuesday. An investigation into his death and the entire riot is still on-going. "The investigation that is going to be done by both Corrections Canada and the police will be extremely difficult," James Bloomfield, with the Union of Canadian Correctional Officers, said in a phone interview with Global News. Global News

Broadcast Media / Médias télédiffusés:

A lockdown is still in effect at Saskatchewan Penitentiary following last week's deadly riot. The riot prompted the lockdown in maximum and medium security areas. Three inmates were injured. Officers were forced to discharge shotguns to control the riot, as a result, six other inmates were injured. (CTV NEWS, 8:00)

What Teaching In Jail Is Teaching Me About Privilege
A blog states, "Four months ago, I began teaching inmates in two of Ontario's maximum security jails. The experience has taught me a lot in a very short amount of time. I'm learning about an alternative universe that exists in parallel to mine. I'm accessing a dimension which is completely divergent from the one I was born into, and I'm still trying to digest it all. I come from an upper-middle class, white family, and I grew up in an affluent Toronto suburb. It was the modern-day "leave it to beaver." I started walking to school in grade three, and I wandered through life feeling safe and protected. I ventured into the downtown core once every six months to see the dentist, and that's about as much of Toronto as I registered. To me, this city consisted of my tiny suburbia and the urban dentist chair. (…) *Literal Change is dedicated to teaching the incarcerated population the skills and strategies that will help these individuals reach literacy proficiency. According to the Correctional Services of Canada:* "[A] survey of Canadian institutional libraries warned that limited access to information, exacerbated by low literacy levels, renders inmates ill-equipped to cope with the complexities of Canada's information driven society upon release."" Huffington Post

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Supervised drug site aims to cut overdose deaths
An orange shipping container converted into a supervised consumption site for injection drug users opens today in the courtyard at Our Place on Pandora Avenue. The hope is that the new temporary and limited service helps to curb the catastrophic number of overdose deaths in Victoria. It is the first supervised consumption service to open at the end of a year of unprecedented deaths, the day after the B.C. Coroners Service announced November overdose deaths were the highest on record for the province. Victoria is in the top three communities of overdose deaths, and Vancouver Island has the highest rate of overdose deaths in the province, with 139 so far this year and November the worst month yet with 18 deaths. "It's completely devastating. The numbers are devastating but sadly I'm not surprised," said Heather Hobbs, who has worked in harm reduction with Aids Vancouver Island for 13 years. "I remember very clearly this time last year when there were a number of deaths in the community and it started to get really bad. We've never seen anything like this. It just keeps getting worse." Hobbs said that despite harm-reduction measures such as supervised consumption services and training to administer naloxone - the antidote to the powerful opioid fentanyl - part of the problem stems from years of "bad" drug policy. "We've done a lot of work to treat drug use as a health issue, not a criminal justice issue, but the justice system is far behind," said Hobbs. "Systems that criminalize and punish people for having a health problem do not work. The whole attempt to keep on top of drugs and dealers is not working. We thought fentanyl was bad, now there's carfentanil." Times Colonist

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Missing and murdered Indigenous women inquiry launches new website
Families of missing and murdered Indigenous women should sign up for MMIW inquiry emails while they wait to register to participate, inquiry commission officials say. The emails will provide updates ahead of the inquiry, which is expected to begin in spring. "We want to create a families first process," said Michael Hutchinson, the commission's director of communications. "Nobody has a list of the people that want to take part in the national inquiry.... We're trying to collect that information from families." The MMIW inquiry has a new website, where families should be able to register soon. The inquiry has five commissioners who in the new year will hear testimony from families of missing and murdered Indigenous women and others in order to examine the systemic causes of violence against Indigenous women and girls in Canada, and make recommendations about how to prevent violence against Indigenous women. CBC News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Who is Canada's self-styled 'Prince of Pot' — and what does he want?
Marc Emery and his stores, Cannabis Culture, came out of nowhere last week with the announcement that they were breaking Federal marijuana laws at eight secret locations in the city. A few days later, the stores were raided, closed and Emery was thrown in jail. He was charged with drug trafficking, possession for the purpose of trafficking and conspiracy. He has been released on bail and is due back in court Feb. 15. Here's a look at Emery's background and what he might hope to accomplish in Montreal. CBC News

How young is too young for legal pot?
Experts are debating the age limit for buying marijuana, with one Edmonton group saying a legal age on par with alcohol could ease the crowding of prisons and remand centres. “There’s a lot of people that are in remand, that are in provincial institutions, for minor drug offences,” said Chris Hay, executive director of the John Howard Society, a non-profit advocating for prison reform. “I think this will definitely help to stave that off, or prevent that a little bit.” Legalization is expected in spring 2017. A recent landmark report from the federal Task Force on Cannabis Legalization and Regulation recommended age 18, but the Canadian Medical Association is pushing for 21. “This is a balance between protecting the developing brain versus trying to address some of the social realities and harm reduction,” said Dr. Jeff Blackmer, who is based in Ottawa. “Obviously there’s no perfect solution here.” Blackmer said evidence shows marijuana has a detrimental effect on short-term memory and retention of information, and chronic use is linked to depression, anxiety and psychosis in some users. Ideally, he said, youth would not use the drug until their brains stop developing around age 25. Metro News

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Officials investigate U.S. air traffic incident with Air Canada plane
U.S. officials are investigating after an air traffic controller error sent a jet from Los Angeles International Airport into the flight path of an Air Canada plane while flying low over Southern California mountains. KABC-TV reports an EVA Air Boeing 777 that left LAX around 1:20 a.m. Friday heading to Taiwan was given an incorrect instruction by a controller based in San Diego to turn left instead of right. That sent the airliner toward mountains above Altadena, as well as toward the path of an Air Canada plane that had just

taken off. Audio traffic indicates the same controller realized the error and told the airliner to "stop your climb" and head southbound. CBC News

Jordanie: l'EI revendique l'attaque de Karak
Le groupe État islamique (EI) a revendiqué l'attaque meurtrière ayant «visé forces de sécurité et touristes» dimanche près du site touristique de Karak en Jordanie, selon un communiqué diffusé mardi sur internet. «Quatre soldats du Caliphat --décédés-- munis d'armes automatiques et de grenades ont attaqué des rassemblements de la sécurité jordanienne et des ressortissants des États de la coalition croisée dans la ville de Karak en Jordanie», affirme le texte faisant référence à la coalition internationale antijihadistes qui lutte contre l'EI en Syrie et en Irak. L'attaque près du site de Karak, à 120 km au sud d'Amman a fait dix morts, sept policiers, deux civils jordaniens et une touriste canadienne, et une trentaine de blessés, selon les autorités jordaniennes. Elle a visé un commissariat et une patrouille de police. Agence France-Presse (Journal de Montréal, Journal de Québec); Associated Press (Sault Star, Fort McMurray Today, Cornwall Standard Freeholder, Owen Sound Sun Times, Brantford Expositor, Chatham Daily News, North Bay Nugget, Thunder Bay Chronicle-Journal, Kelowna Daily Courier, Calgary Sun, Edmonton Sun, Ottawa Sun, Toronto Sun, Winnipeg Sun, Guelph Mercury, MetroNews Canada, Brandon Sun)

Canadian and American hostages appeal to Trump and Obama in new scripted video
An American woman and her Canadian husband who were captured four years ago by the Taliban are appealing to President Barack Obama and President-elect Donald Trump to exchange Afghan prisoners for their release, in a video that also shows their two young children for the first time. "My children have seen their mother defiled," says Caitlan Coleman in the new video released on Monday by the Haqqani Network, an Afghan and Pakistani insurgent group, and posted to YouTube. Next to her, a baby and toddler squirm on her husband Joshua Boyle's lap. The toddler laughs at something off camera, and then picks his nose. "We ask quickly, in our collective fourteenth year of prison, urge the governments on both sides to reach some agreement to allow us freedom." Coleman was 27 and pregnant in the fall of 2012 when she and Boyle were captured by the Taliban as they were backpacking in Afghanistan. They are now being held by the Haqqanis, a group affiliated with the Taliban who have been known for their hostage operations — including holding American soldier Bowe Berghdal. "Obama, your legacy in leaving office is probably important to you, and our lives and those of our children are to us," Coleman says in the video. "So please don't become the next Jimmy Carter. Just give the offenders something so they and you can save face, and we can leave the region permanently." VICE News; Radio-Canada (Huffington Post Québec)

INTERNATIONAL

Berlin Christmas market: Police release man from custody
The man detained after a truck crashed into a Berlin Christmas market has been set free, Germany's general prosecutor said in a statement Tuesday. "The investigations thus far have not produced urgent suspicion against the suspect," the statement said. Police say the man they detained after a truck plowed into a Berlin Christmas market may not have been the driver, leading to fears that the attacker could still be on the loose. "They're really back to square one in terms of this investigation. ... It may well be a scenario of a manhunt, a race against time to arrest this individual before they can strike again," CNN terrorism analyst Paul Cruickshank said. CNN; Radio-Canada ; Associated Press (Calgary Sun, Edmonton Sun, Ottawa Sun, Toronto Sun, Winnipeg Sun)

First Berlin victim a Pole who fought for his life
He was the first victim in the attack on a Berlin Christmas market -- a 37-year-old Polish truck driver who was seemingly stabbed and shot to death in the cabin of his truck. One of his colleagues said he was so dedicated to his work and his truck that he could be expected to defend the vehicle "to the end." Lukasz Urban, a 37-year-old from the western village of Roznowo, near the border with Germany, was found dead in the cabin of the truck that was hijacked and driven into the crowd Monday evening, killing at least another 11 people. German authorities are calling it an "act of terrorism." Chronicle Herald

UK police forces reviewing security plans after Berlin attack
Police forces across Britain are reviewing their security plans following the Berlin Christmas market attack and remain on high alert. The threat level in London remains at "severe", meaning the police consider an attack highly likely, the Metropolitan police said in a statement on Tuesday. A Downing Street spokeman said: "The safety and security of British citizens in the government's number one priority. Clearly in the light of what has happened in Berlin police will be reviewing what is in place." Guardian UK; BBC News

NSA watchdog on leave in whistleblower case
Allegations of retaliation against a whistleblower at the National Security Agency have left its top watchdog fighting for his job, according to an intelligence official and another individual familiar with the case. The case could offer some credence to Edward Snowden's claim that he could not have reported the government's domestic surveillance program without facing reprisals. George Ellard, the NSA's inspector general, was placed on administrative leave after he refused to give the whistleblower a certain job assignment. The Project on Government Oversight, an advocacy group, first reported last week that Adm. Mike Rogers, director of NSA, had placed Ellard on leave and recommended that he be terminated. Ellard is appealing that decision. Associated Press (CTV News)

US cities step up security at Christmas gatherings after terrorist truck attack on Berlin market which killed 12 shoppers
Cities across America are stepping up security at Christmas events following a terrorist truck attack on a Berlin market that has left 12 people dead. Police are boosting their presence at holiday villages and major sites around cities such as New York, Chicago and Boston as the US remains on high alert. It comes after a Christmas market in the German capital was deliberately targeted by a man, who is believed to have used a hijacked 25-tonne lorry to murder 12 people and injure 48 more. And in New York, police confirmed highly trained specialist units and its anti-terror squad would be deployed to high profile locations around the city. Sites expected to have a high armed police presence include the Winter Village market in Bryant Park, the Christmas market near Columbus Circle and the festive stalls in Union Square. Also under close surveillance by the security services are the world-famous Christmas tree at Rockefeller Center, Times Square and Herald Square, home to department store Macy's. Daily Mail

After Berlin atttack, the cracks in Germany's security are showing
An opinion piece by professor Christian Leuprecht states, "The attack in Berlin may have taken the world by surprise; the only surprise to the German security and intelligence establishment is that something of the sort did not happen sooner. Hannover, Würzburg, Ansbach: An air of terrorism has been hanging over Germany all year. Since the attacks in Paris and Brussels, German authorities have been on high alert, and nowhere more so than in Berlin: Note the pattern of sensational attacks in capital cities. The July shooting in Munich that caused authorities to shut down the city was the canary in the coal mine. As in Munich – but unlike Paris – the response in Berlin was swift and co-ordinated; with one notable difference: Information operations in Berlin were far superior because authorities there finally understood social media. Yet, authorities seem to have few leads (if any) and there are now doubts about the suspect who was initially apprehended. How is that possible? Much of German's security architecture was designed to prevent what happened during the Third Reich: The logic was to take domestic security out of the hands of the central government. Germany has some of the strictest privacy laws in the world. As a result, agencies are loath to talk to one another: Foreign intelligence (the *Bundesnachrichtendienst*, or BND) faces severe hurdles communicating with domestic intelligence (the *Verfassungsschutz*, which loosely translates to protection of the constitution) – and is subject to an extensive parliamentary inquiry into unauthorized "selector" data sharing with the U.S. National Security Agency." Globe and Mail

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

Meaghan Willis

Min. @RalphGoodale announces nearly $4.4M in funding for recreational & cultural projects across Saskatchewan. #yqr #sask #Canada150

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Canadian Forces
"Search and rescue is going to become a lot less about search and a lot more about rescue." - Comd of @RCAF_ARC, LGen Hood #SAR

Coquitlam SAR
Outside of regular training, #SAR members get a lot of their experience the same way you do. Getting out & recreating with friends. #SARelf

The Canadian Press
UPDATE: Ferocious Fort McMurray wildfire voted @CdnPress news story of the year for 2016 http://bit.ly/2hDPaQJ

globalnews
Fort McMurray wildfire named Canada's news story of 2016 https://t.co/F7e8dxtaUf

Canadian Red Cross
It's been a challenging year for many people impacted by #ABfires. Send them your warmest #HolidayWishes

Transports_gc
Pour les collectivités: fonds visant à réduire blessures et décès sur #VoiesFerrées. tc.gc.ca/foalx @ReseauFCM @Gareautrain pic.twitter.com/B9mCgb5FKE

Transport_gc
Calling on communities to apply for funding to reduce injuries & fatalities at #TrainTracks tc.gc.ca/33j8g @FCM_online @oplifesaver pic.twitter.com/UpY8PTYR3V

NATIONAL SECURITY / SÉCURITÉ NATIONALE

CJFE
We join @OpenMediaOrg to call on government to release all results from the National Security consultation http://bit.ly/2hM4FEs

CBC News
Canadian telecoms push back on proposed police powers http://www.cbc.ca/1.3903930 #C31

The Muslim Lawyer
Eight reasons why Canada must repeal its anti-terror laws https://shar.es/1DWadk via @MiddleEastEye @nccm @ICLMG

Resiliency_CBoC
The Evolving Threat of #Terrorism: A Shifting Security Landscape in Europe by @The_Fuzz74 conferenceboard.ca/topics/securit… #lesm #natsec

NSPS (CBoC)
Fighting #Extremism: Counter-#radicalization and the "Danish Model" with @rolhol1 http://www.conferenceboard.ca/e-library/abstract.aspx?did=8492&utm_source=twitter&utm_medium=social&utm_campaign=kbtweet … #natsec #security #lesm #cdnpoli

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

SC Media
Domino's Pizza advises customers to change their passwords

Kaspersky Lab
We've built a new decryptor to help victims of CryptXXX! Don't pay the ransom! https://kas.pr/At8T #nomoreransom #infosec

SC Media
What did Yahoo know? And when did they know it?

LAW ENFORCEMENT / APPLICATION DE LA LOI

Joanne Schnurr
Stepmother and father now in courtroom. Suspended Mountie to find out his sentencing date in torture starvation trial of his son @ctvottawa

CTV Ottawa
Follow @JoanneCTV for updates from sentencing hearing for step-mother of child who was tortured by his father, a former RCMP officer.

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

John Howard Society
Keeping the mentally ill out of solitary, and out of prison: Editorial http://on.thestar.com/2hQ93VL via @torontostar

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NCCM
Mental health services needed in Somali community, says settlement director

John Howard Society
#Employment is a stabilizing factor in preventing crime but a #criminalrecord is a major obstacle to finding a job

CKNW
BC Coroner opens up about the fentanyl crisis @lizaCKNW980

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Connie Walker
RCMP say Alberta Williams case is now "very active" beacuse of new details revealed in a CBC News podcast.

CBCIndigenous
Missing and murdered Indigenous women inquiry launches new website ift.tt/2hWujFV pic.twitter.com/blzRutnZKn

OTHER / AUTRES

Amarnath Amarasingam
ISIS claims attack in Jordan, which killed 10 people, including a Canadian tourist Linda Vatcher. #Jordan #ISIS

CBCTheNational
ISIS has claimed responsibility for shootings in Jordan that left 10 dead, including a woman from Newfoundland http://www.cbc.ca/1.3904730

VassyKapelos
Canada calls for release of Joshua Boyle, Canadian held in Afghanistan after new video appears http://globalnews.ca/news/3137600/canada-calls-for-release-joshua-boyle-canadian-held-in-afghanistan-with-family/ … #cdnpoli

HuffPost Canada
Canada calls for release of couple held captive in Afghanistan since 2012 http://huff.to/2h6649Y

INTERNATIONAL

Independent
Germany told to expect 'further significant attacks' after Berlin lorry tragedy http://ind.pn/2hE8tcl

Associated Press
BREAKING: German prosecutor: Treating Berlin attack as act of terrorism but no claim of responsibility yet.

SkyNews
Gunman who shot three worshippers at mosque in Zurich was interested in "the occult", police have said trib.al/UHrWqn1

lemondefr
Un groupe radical kurde revendique l'attentat contre des soldats à Kayseri, en Turquie lemonde.fr/international/…

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

Today's News / Actualités
December 20, 2016 / le 20 décembre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

TOP STORIES / MANCHETTES

Missing and murdered Indigenous women inquiry launches new website
Families of missing and murdered Indigenous women should sign up for MMIW inquiry emails while they wait to register to participate, inquiry commission officials say. The emails will provide updates ahead of the inquiry, which is expected to begin in spring. "We want to create a families first process," said Michael Hutchinson, the commission's director of communications. "Nobody has a list of the people that

want to take part in the national inquiry.... We're trying to collect that information from families." The MMIW inquiry has a new website, where families should be able to register soon. The inquiry has five commissioners who in the new year will hear testimony from families of missing and murdered Indigenous women and others in order to examine the systemic causes of violence against Indigenous women and girls in Canada, and make recommendations about how to prevent violence against Indigenous women. CBC News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Ferocious Fort McMurray wildfire voted news story of the year for 2016
The ferocious wildfire that forced nearly 90,000 to flee Canada's oilsands region and reduced thousands of homes to rubble has been picked as the top news story of 2016 in an annual survey of newsrooms across Canada. Dubbed "the beast" for its merciless unpredictability, the Fort McMurray wildfire garnered 39 of the 67 votes cast by senior editors. It was followed by Canada's ongoing resettlement of Syrian refugees with 11 votes, the fentanyl crisis with six and the Tragically Hip's farewell tour with five. "Not even a Hollywood script could match the terror, uncertainty, and heroism to come out of what seemed to be a surreal event," wrote Dave Barry, news director of CKPG TV in Prince George, B.C. Canadian Press (Brandon Sun, Winnipeg Free Press, Metro News, Global News, 570 News, Globe and Mail)

Sask. government rejects privacy commissioner's recommendation to release Husky pipeline records
The Saskatchewan government has rejected a recommendation from the provincial privacy commissioner to release records and information about Husky Energy pipeline inspections. In a report focused on the Ministry of the Economy, the Office of the Saskatchewan Information and Privacy Commissioner says the government should not have withheld records in response to an access to information request. On July 21, about 200,000 litres of heavy oil mixed with another petroleum product spilled into the North Saskatchewan River from a Husky pipeline near Lloydminster, Sask. The cities of Prince Albert, Melfort and North Battleford had to temporarily shut down their drinking water intake from the river and find other means to supply their residents with drinking water. CBC News (2016-12-19)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Fête du Nouvel An : la sécurité à l'ordre du jour
L'attentat survenu lundi au Marché de Noël de Berlin fait réfléchir sur les mesures de sécurité à l'approche des célébrations du Nouvel An sur la Grande Allée à Québec. La sécurité sera d'ailleurs au coeur des discussions lors d'une rencontre qui était déjà prévue mercredi entre les organisateurs de la fête, les services de sécurité et la Ville de Québec. La Ville ne veut pas confirmer si elle envisage des mesures supplémentaires et de quelle nature elles pourraient être. Marie-Ève Painchaud, porte-parole du Service de police de la Ville de Québec, souligne que le risque n'est pas le même à Québec, mais que la Ville est bien outillée. Radio-Canada

Eight reasons why Canada must repeal its anti-terror laws
An opinion piece states, ""Sunny ways my friends," Canadian prime Minister Justin Trudeau told his supporters on election night last year. "Sunny ways. This is what positive politics can do." One of Trudeau's main campaign promises was to hold public consultations to review and amend draconian national security laws (known as Bill C-51 at the time) that the outgoing Conservative government enacted prior to being thrown out in 2015. After public consultations wrapped up last week, many are now awaiting to see if sunlight will disinfect the national security shadow. Like most countries, Canada's legal landscape underwent a seismic shift in the immediate aftermath of 9/11. The Liberal government, led at the time by prime minister Jean Chretien, enacted a slew of national security laws and policies. They included the 2001 Anti-Terrorism Act, which echoed the infamous American Patriot Act. (...) Canada's spy agency, the Canadian Security Intelligence Service (CSIS), was created in 1984 as a civilian agency to address abuses of power that occurred when the Royal Canadian Mounted Police (RCMP) handled both intelligence and law enforcement. The Anti-Terrorism Act of 2015 radically expands

the powers of the CSIS, and disregards constitutional protections. (…) Thousands of Canadian Muslims and Arabs have had to submit themselves to "voluntary" interviews with the CSIS. The number and frequency will undoubtedly increase under the new laws. Many of these people are ensnared in the national security web merely through guilt by association and the inevitable false positives." Middle East Eye

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

The Lie-Detecting Security: Kiosk of the Future
SDSU professor is developing a robotic kiosk that could help detect travelers with sinister intentions. When you engage in international travel, you may one day find yourself face-to-face with border security that is polite, bilingual and responsive—and robotic. The Automated Virtual Agent for Truth Assessments in Real Time (AVATAR) is currently being tested in conjunction with the Canadian Border Services Agency (CBSA) to help border security agents determine whether travelers coming into Canada may have undisclosed motives for entering the country. (…) In the meantime, Elkins is looking for a government agency willing to utilize the technology in a real-world application. "AVATAR has been tested in labs, in airports and at border crossing stations," Elkins noted. "The system is fully ready for implementation to help stem the flow of contraband, thwart fleeing criminals, and detect potential terrorists and many other applications in the effort to secure international border. San Diego Metro

Why are public schools recruiting adult students overseas?
The Quebec government encourages school boards to conduct vocational training Quebec English School Boards Association president Jennifer Maccarone told The Suburban. "Emploi Québec dictates if, say, we need 40 skilled workers in a particular region in welding and fitting, 100 new jobs in secretarial and another number in plumbing and fitting," she explained in an interview last month. "We hold regular meetings with universities CEGEPs and school boards to work with Emploi Québec to determine what programs we need to be backing away from because there is a surplus and which ones will see growth in demand." The results are then coordinated with provincial education and immigration officials, to ensure that Quebec has sufficient qualified workers to keep its economy thriving. The vocational studies thus indirectly help international students to apply for permanent residence, so they can remain here and make a useful contribution by reducing Canada's skilled worker shortage, once they complete their program. "People come here to get a profession," English Montreal School Board (EMSB), communication and marketing specialist Michael Cohen told The Suburban. "Many apply to immigrate and Quebec gets workers skilled and able to pay taxes." Suburban

Americans dream of Canada after Trump
As electoral college votes in Donald Trump, many US citizens plan move to Canada, but may face cold reception. Lola Al-Uqdah won't soon forget the morning of November 9. A mother of three and psychology professor who lives in Camden, New Jersey, Al-Uqdah was in the midst of her usual pre-work routine when she learned that Donald Trump had defeated Hillary Clinton to become the next president of the United States. It was the morning after the US election and her husband had delivered the message through the bathroom door. (…) Her American Dream was dead. There was only one thing left to do: plan her move to Canada. Al-Uqdah is one of hundreds, if not thousands of Americans who, during the election, contemplated moving to Canada if Trump won. But unlike the vast majority of liberal anti-Trumpers who flip-flopped on Canada once the billionaire real estate mogul pulled off a stunning victory, Al-Uqdah was serious. For Al-Uqdah, a Muslim woman, a Trump presidency wasn't just an inconvenience - it was a terrifying reality. AlJazeera

Gypsum tariffs will save Canadian manufacturing jobs
An opinion piece states, "The International Brotherhood of Boilermakers represent 120 workers employed at CertainTeed Gypsum (CTG) wallboard manufacturing operations in Western Canada and we are concerned their jobs are at stake. We appeared before the Canadian International Trade Tribunal (CITT) to explain what happens to laid-off workers and why Canada should not change its 112-year-old policy of fighting the evils of dumping. Our members have already lost over 100 well-paid, middle-class union jobs at idled gypsum plants in Western Canada and we cannot afford to lose 120 more. David Campbell, of

Empire Drywall Ltd., presented an argument on Dec. 13 in the Edmonton Journal, for why U.S. drywall producers should be given a licence to engage in what the Canada Border Services Agency (CBSA) has already determined to be illegal dumping. We disagree with this notion. Ottawa must not give U.S. producers a licence to dump gypsum board and steal our jobs; to do so would be a miscarriage of justice. Western Canada needs jobs and potential investors must be convinced that they will have protection against unfair trade practices." Edmonton Journal

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

ShadowBrokers Dump Came from Internal Code Repository, Insider
An analysis of the latest ShadowBrokers dump of alleged NSA spy tools points to an insider with access to a code repository belonging to the intelligence agency, experts said. Researchers at security company Flashpoint said today that its investigation of the leaked data points away from an attack against NSA infrastructure, or other theories that operators mistakenly left classified data on staging servers, for example. Instead, clues in code made available last week point toward an NSA employee or contractor. Threatpost

Privacy groups complain to FTC over Google's 'deceptive' policy change
Privacy groups have complained to the Federal Trade Commission that Google is encroaching on user privacy through a policy change in June that allows it to combine personally identifiable information with browsing data collected by its DoubleClick digital advertising service. The complaint, by Consumer Watchdog and Privacy Rights Clearing House, alleged that Google has created "super-profiles" as it can track user activity on Android mobile phones, with an 88 percent market share of smartphones worldwide. The information can also be gleaned "from any website that uses Google Analytics, hosts YouTube videos, or displays ads served by DoubleClick or AdSense," according to the complaint. Computerworld

Malware Exchange Busted by the Feds Relaunches, At Least in Name
The digital underground is a fragile place, with hacking forums sometimes being shuttered by police. That's what happened to malware-marketplace Darkode last year: in coordinated raids, the FBI, UK's National Crime Agency, and a slew of other law enforcement bodies arrested over 70 hackers and closed the popular site. Now, Darkode, is back, at least in name. Motherboard

Hackers Might Have Turned Off the Lights in Ukraine for the Second Time
Ukraine experienced a new power outage during the weekend, and it's believed that hackers are once again responsible, after they previously breached energy companies in 2015. Softpedia; Bleeping Computer

This is your captain speaking... or is it?
Vulnerabilities in Panasonic in-flight entertainment systems create a possible mechanism for attackers to control in-flight displays, PA systems and lighting, say researchers. Ruben Santamarta, principal security consultant at IOActive, said it had found vulnerabilities in Panasonic Avionic In-Flight Entertainment (IFE) systems that it claims could allow hackers to "hijack" passengers' in-flight displays and, in some instances, potentially access their credit card information. The research revealed it would also theoretically be possible that such a vulnerability could present an entry point to the wider network, including the aircraft controls domain. Register; Infosecurity Magazine

Hailstorm methods used to spread malware in phishing attacks
Cisco Talos researchers have spotted Hailstorm spam tactics used to evade cyber defenses and spread malware via phishing attacks. Rather than send large volumes of mail for large periods of time, hailstorm campaigns send larges bursts of spam over very short periods of time, according to a Dec. 19 blog post. The spam is sent via IP addresses located around the world with the intent of flying under the radar with respect to any reputation or volume-based metrics that could be applied by anti-spam systems. SC Magazine

Evolved DNSChanger malware slings evil ads at PCs, hijacks routers

Malware that spreads via evil web ads and menaces broadband routers has been discovered – and it's going to be particularly horrible for small business and home internet users, which it targets. This latest variant of the years-old DNSChanger nasty, just spotted by Californian infosec biz Proofpoint, works like this: some JavaScript code is hidden in advertisements placed on mainstream websites via ad networks. The code – which prefers Chrome on Windows and Android – checks for the local IP address of the browser visiting the site using a WebRTC request to a Mozilla STUN server. Register

Mobile banking trojans adopt ransomware features
Cybercriminals are adding file-encrypting features to traditional mobile banking trojans, creating hybrid threats that can steal sensitive information and lock user files at the same time. One such trojan is called Faketoken and its primary functionality is to generate fake login screens for more than 2,000 financial applications in order to steal login credentials. Computerworld

Inside LeakedSource and Its Database of 3 Billion Hacked Accounts
By now it's hard to keep track of which companies have been hacked and which haven't. Remember the FourSquare hack? What about Adobe? Even breaches that were high-profile at the time are fading into obscurity as bigger and scarier ones crop up. (Ahem, Yahoo.) And if you can't remember what's been hacked, you're probably struggling to keep track of which leaks have included your personal data. That's where "the Google of data breaches" comes in. LeakedSource is a service that sends email notifications about new breaches and offers a database of information stolen in hacks. Its basic services—the ability to sign up for email notifications and search the database—are free, but users can pay to access more advanced search functionality. Wired Magazine

LAW ENFORCEMENT / APPLICATION DE LA LOI

Scars on his body remind boy of abuse he suffered in Mountie's basement
The boy who was restrained, tortured, sexually abused and neglected in the basement of his family's home told court in a recorded victim impact statement that while he's doing better, the scars on his body remind him of the abuse he suffered. He was 11 when his parents were arrested in February 2013 and is now 14 years old. He appeared in Ontario Superior Court in Ottawa Tuesday via a video recorded last week. The boy looked healthy, though his voice sometimes cracked. He said he avoids answering questions about the scars on his body and that he's reminded in the shower about what he endured when he sees the red marks around his ankles from his restraints. He said he knows he needs psychological help, and that he one day hopes to be able to put the memories aside. Her Mountie husband — the boy's father — was found guilty of aggravated assault, sexual assault causing bodily harm, forcible confinement and failing to provide the necessaries of life. He has been suspended from the RCMP without pay. The Mountie is expected to be sentenced in March. CBC News

RCMP sing at six care homes in Parksville Qualicum Beach
Residents at a half-dozen Parksville and Qualicum Beach care homes were serenaded with Christmas carols Thursday by an unusual choral group — the Oceanside RCMP. Outfitted in red serge and supported by several family members, civilian office staff and women from the victims services department, a group of 18 detachment members regaled seniors with classic carols in a one-day tour of brief stops. Parksville Qualicum Beach News

Police constable debunks Vader's claim strip search was 'humiliating'
A constable involved in the strip search of Travis Vader in 2010 at the Edson RCMP detachment told an Edmonton courtroom he was just following instructions from a superior officer. Const. Steven McQueen, with the Edmonton serious crimes unit, testified at Vader's sentencing hearing Monday that he and another officer brought Vader to an empty cell where they proceeded to "secure his clothes as potential evidence." They searched for weapons and drugs, McQueen said, then gave Vader a fresh T-shirt, sweatpants and socks to wear as they put his clothes in an evidence bag. Vader was naked for less than a minute in a quiet cell with nobody else around, McQueen said, suggesting the search was routine and requested by a superior. Last week, Vader testified the strip search went on for five minutes, with the

door to the holding cell left open where "everybody could see." He called the experience "absolutely humiliating." CBC News

Calgary police chief announces independent review of officer-involved shootings
Calgary's police chief announced on Monday there will be an independent review into officer-involved shootings in Calgary. Speaking before Calgary city council, Chief Roger Chaffin said he wants the review to be conducted by someone outside of the City of Calgary and Calgary Police Service. They have been 10 officer-involved shootings in Calgary so far in 2016, five of which were fatal. There were three in 2015. Chaffin has attributed the increase to a changing nature of crime in the city, citing the presence of meth and opioids on the Calgary streets as driving factors. Calgary Mayor Naheed Nenshi said an independent review is the right approach. A provincial watchdog does review officer-involved shootings in Alberta. The Alberta Serious Incident Response Team (ASIRT) determines if officers acted appropriately and whether or not any wrongdoing took place. Global News

Body found on Big Island Lake Cree Nation during RCMP theft investigation
RCMP believe the death of a person found on the Big Island Lake Cree Nation as officers investigated a theft is suspicious. Mounties say officers were investigating a theft Tuesday at about 5 a.m. when police found the deceased male — officers do not yet know his age — outdoors on the First Nation. Investigators do not yet know the circumstances of the death or the body's identity, but police do believe the death is suspicious. The RCMP's major crimes north unit and forensic identification section are investigating alongside the officers from Pierceland, the Meadow Lake detachment's police dog unit and the coroner's office. CTV News Saskatoon; StarPhoenix; CBC News

Vigil grows at apparent murder-suicide scene in Spruce Grove
With just days to go before Christmas, an Alberta family will spend the holidays planning funerals, instead of celebrating. Two hockey sticks, two teddy bears and a collection of flowers formed a memorial on the front lawn of a home west of Edmonton, where two brothers and their father were found dead Monday morning in what appears to be a murder-suicide. The bodies discovered inside the home were those of Corry MacDougall and his sons, 13-year-old Ryder MacDougall and 11-year-old Radek MacDougall. Brent Stark, the boys' stepfather, spoke to Global News Monday evening. He said it was he and the boys' mother Tracy who discovered the bodies and called police. He also said he believes Corry killed his sons in an apparent murder-suicide. RCMP confirmed that the bodies of three people were found in the home at 2 Haney Ct. Monday morning and that they are not looking for any suspects. Global News

RCMP looking for Big River teen
A 13-year-old girl from the Big River area has been reported missing. Maria McAdam, who also goes by 'Littlechief,' was reported missing on Dec. 18. She was last seen at a school on Dec. 16 and was supposed to be at a friend's home over the weekend, but this wasn't the case. PA Now

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

L'ex-juge Delisle saura s'il peut reprendre sa liberté mardi
L'ex-juge Jacques Delisle saura mardi s'il peut recouvrir sa liberté en attendant que la ministre fédérale de la justice détermine s'il a été victime, ou non, d'une erreur judiciaire en étant condamné pour le meurtre de sa femme. Ces dernières semaines, les avocats de M. Delisle ont tenté de démontrer que l'homme est innocent du crime pour lequel il a été condamné en 2012 à la prison à perpétuité en présentant une nouvelle analyse balistique. M. Delisle, aujourd'hui âgé de 81 ans, a passé les quatre dernières années derrière les barreaux suite au meurtre de sa femme survenue en 2009. Agence QMI (Journal de Québec, Journal de Montréal); TVA Nouvelles

Saskatchewan Penitentiary remains under lockdown following riot
A lockdown at the Saskatchewan Penitentiary remains in place after 185 inmates in medium security destroyed parts of the prison during a deadly riot last Wednesday. There are still plenty of questions as to what sparked the riot but it appears food portions being served to inmates may have played a role.

During the rampage, six inmates suffered non-life threatening injuries after being hit by shotgun pellets. Another three were sent to hospital in serious condition after being assaulted by other prisoners, including Jason Leonard Bird, who died Wednesday evening. A wake for Bird will take place on Tuesday. An investigation into his death and the entire riot is still on-going. "The investigation that is going to be done by both Corrections Canada and the police will be extremely difficult," James Bloomfield, with the Union of Canadian Correctional Officers, said in a phone interview with Global News. Global News

Broadcast Media / Médias télédiffusés:

A lockdown is still in effect at Saskatchewan Penitentiary following last week's deadly riot. The riot prompted the lockdown in maximum and medium security areas. Three inmates were injured. Officers were forced to discharge shotguns to control the riot, as a result, six other inmates were injured. (CTV NEWS, 8:00)

What Teaching In Jail Is Teaching Me About Privilege
A blog states, "Four months ago, I began teaching inmates in two of Ontario's maximum security jails. The experience has taught me a lot in a very short amount of time. I'm learning about an alternative universe that exists in parallel to mine. I'm accessing a dimension which is completely divergent from the one I was born into, and I'm still trying to digest it all. I come from an upper-middle class, white family, and I grew up in an affluent Toronto suburb. It was the modern-day "leave it to beaver." I started walking to school in grade three, and I wandered through life feeling safe and protected. I ventured into the downtown core once every six months to see the dentist, and that's about as much of Toronto as I registered. To me, this city consisted of my tiny suburbia and the urban dentist chair. (…) *Literal Change is dedicated to teaching the incarcerated population the skills and strategies that will help these individuals reach literacy proficiency. According to the Correctional Services of Canada:* "[A] survey of Canadian institutional libraries warned that limited access to information, exacerbated by low literacy levels, renders inmates ill-equipped to cope with the complexities of Canada's information driven society upon release.'" Huffington Post

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Supervised drug site aims to cut overdose deaths
An orange shipping container converted into a supervised consumption site for injection drug users opens today in the courtyard at Our Place on Pandora Avenue. The hope is that the new temporary and limited service helps to curb the catastrophic number of overdose deaths in Victoria. It is the first supervised consumption service to open at the end of a year of unprecedented deaths, the day after the B.C. Coroners Service announced November overdose deaths were the highest on record for the province. Victoria is in the top three communities of overdose deaths, and Vancouver Island has the highest rate of overdose deaths in the province, with 139 so far this year and November the worst month yet with 18 deaths. "It's completely devastating. The numbers are devastating but sadly I'm not surprised," said Heather Hobbs, who has worked in harm reduction with Aids Vancouver Island for 13 years. "I remember very clearly this time last year when there were a number of deaths in the community and it started to get really bad. We've never seen anything like this. It just keeps getting worse." Hobbs said that despite harm-reduction measures such as supervised consumption services and training to administer naloxone - the antidote to the powerful opioid fentanyl - part of the problem stems from years of "bad" drug policy. "We've done a lot of work to treat drug use as a health issue, not a criminal justice issue, but the justice system is far behind," said Hobbs. "Systems that criminalize and punish people for having a health problem do not work. The whole attempt to keep on top of drugs and dealers is not working. We thought fentanyl was bad, now there's carfentanil." Times Colonist

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Missing and murdered Indigenous women inquiry launches new website
Families of missing and murdered Indigenous women should sign up for MMIW inquiry emails while they wait to register to participate, inquiry commission officials say. The emails will provide updates ahead of the inquiry, which is expected to begin in spring. "We want to create a families first process," said Michael Hutchinson, the commission's director of communications. "Nobody has a list of the people that want to take part in the national inquiry.... We're trying to collect that information from families." The MMIW inquiry has a new website, where families should be able to register soon. The inquiry has five commissioners who in the new year will hear testimony from families of missing and murdered Indigenous women and others in order to examine the systemic causes of violence against Indigenous women and girls in Canada, and make recommendations about how to prevent violence against Indigenous women. CBC News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Who is Canada's self-styled 'Prince of Pot' — and what does he want?
Marc Emery and his stores, Cannabis Culture, came out of nowhere last week with the announcement that they were breaking Federal marijuana laws at eight secret locations in the city. A few days later, the stores were raided, closed and Emery was thrown in jail. He was charged with drug trafficking, possession for the purpose of trafficking and conspiracy. He has been released on bail and is due back in court Feb. 15. Here's a look at Emery's background and what he might hope to accomplish in Montreal. CBC News

How young is too young for legal pot?
Experts are debating the age limit for buying marijuana, with one Edmonton group saying a legal age on par with alcohol could ease the crowding of prisons and remand centres. “There’s a lot of people that are in remand, that are in provincial institutions, for minor drug offences,” said Chris Hay, executive director of the John Howard Society, a non-profit advocating for prison reform. “I think this will definitely help to stave that off, or prevent that a little bit.” Legalization is expected in spring 2017. A recent landmark report from the federal Task Force on Cannabis Legalization and Regulation recommended age 18, but the Canadian Medical Association is pushing for 21. “This is a balance between protecting the developing brain versus trying to address some of the social realities and harm reduction,” said Dr. Jeff Blackmer, who is based in Ottawa. “Obviously there’s no perfect solution here.” Blackmer said evidence shows marijuana has a detrimental effect on short-term memory and retention of information, and chronic use is linked to depression, anxiety and psychosis in some users. Ideally, he said, youth would not use the drug until their brains stop developing around age 25. Metro News

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Officials investigate U.S. air traffic incident with Air Canada plane
U.S. officials are investigating after an air traffic controller error sent a jet from Los Angeles International Airport into the flight path of an Air Canada plane while flying low over Southern California mountains. KABC-TV reports an EVA Air Boeing 777 that left LAX around 1:20 a.m. Friday heading to Taiwan was given an incorrect instruction by a controller based in San Diego to turn left instead of right. That sent the airliner toward mountains above Altadena, as well as toward the path of an Air Canada plane that had just

taken off. Audio traffic indicates the same controller realized the error and told the airliner to "stop your climb" and head southbound. CBC News

Jordanie: l'EI revendique l'attaque de Karak
Le groupe État islamique (EI) a revendiqué l'attaque meurtrière ayant «visé forces de sécurité et touristes» dimanche près du site touristique de Karak en Jordanie, selon un communiqué diffusé mardi sur internet. «Quatre soldats du Caliphat --décédés-- munis d'armes automatiques et de grenades ont attaqué des rassemblements de la sécurité jordanienne et des ressortissants des États de la coalition croisée dans la ville de Karak en Jordanie», affirme le texte faisant référence à la coalition internationale antijihadistes qui lutte contre l'EI en Syrie et en Irak. L'attaque près du site de Karak, à 120 km au sud d'Amman a fait dix morts, sept policiers, deux civils jordaniens et une touriste canadienne, et une trentaine de blessés, selon les autorités jordaniennes. Elle a visé un commissariat et une patrouille de police. Agence France-Presse (Journal de Montréal, Journal de Québec); Associated Press (Sault Star, Fort McMurray Today, Cornwall Standard Freeholder, Owen Sound Sun Times, Brantford Expositor, Chatham Daily News, North Bay Nugget, Thunder Bay Chronicle-Journal, Kelowna Daily Courier, Calgary Sun, Edmonton Sun, Ottawa Sun, Toronto Sun, Winnipeg Sun, Guelph Mercury, MetroNews Canada, Brandon Sun)

Canadian and American hostages appeal to Trump and Obama in new scripted video
An American woman and her Canadian husband who were captured four years ago by the Taliban are appealing to President Barack Obama and President-elect Donald Trump to exchange Afghan prisoners for their release, in a video that also shows their two young children for the first time. "My children have seen their mother defiled," says Caitlan Coleman in the new video released on Monday by the Haqqani Network, an Afghan and Pakistani insurgent group, and posted to YouTube. Next to her, a baby and toddler squirm on her husband Joshua Boyle's lap. The toddler laughs at something off camera, and then picks his nose. "We ask quickly, in our collective fourteenth year of prison, urge the governments on both sides to reach some agreement to allow us freedom." Coleman was 27 and pregnant in the fall of 2012 when she and Boyle were captured by the Taliban as they were backpacking in Afghanistan. They are now being held by the Haqqanis, a group affiliated with the Taliban who have been known for their hostage operations — including holding American soldier Bowe Berghdal. "Obama, your legacy in leaving office is probably important to you, and our lives and those of our children are to us," Coleman says in the video. "So please don't become the next Jimmy Carter. Just give the offenders something so they and you can save face, and we can leave the region permanently." VICE News; Radio-Canada (Huffington Post Québec)

INTERNATIONAL

Berlin Christmas market: Police release man from custody
The man detained after a truck crashed into a Berlin Christmas market has been set free, Germany's general prosecutor said in a statement Tuesday. "The investigations thus far have not produced urgent suspicion against the suspect," the statement said. Police say the man they detained after a truck plowed into a Berlin Christmas market may not have been the driver, leading to fears that the attacker could still be on the loose. "They're really back to square one in terms of this investigation. ... It may well be a scenario of a manhunt, a race against time to arrest this individual before they can strike again," CNN terrorism analyst Paul Cruickshank said. CNN; Radio-Canada ; Associated Press (Calgary Sun, Edmonton Sun, Ottawa Sun, Toronto Sun, Winnipeg Sun)

First Berlin victim a Pole who fought for his life
He was the first victim in the attack on a Berlin Christmas market -- a 37-year-old Polish truck driver who was seemingly stabbed and shot to death in the cabin of his truck. One of his colleagues said he was so dedicated to his work and his truck that he could be expected to defend the vehicle "to the end." Lukasz Urban, a 37-year-old from the western village of Roznowo, near the border with Germany, was found dead in the cabin of the truck that was hijacked and driven into the crowd Monday evening, killing at least another 11 people. German authorities are calling it an "act of terrorism." Chronicle Herald

UK police forces reviewing security plans after Berlin attack
Police forces across Britain are reviewing their security plans following the Berlin Christmas market attack and remain on high alert. The threat level in London remains at "severe", meaning the police consider an attack highly likely, the Metropolitan police said in a statement on Tuesday. A Downing Street spokeman said: "The safety and security of British citizens in the government's number one priority. Clearly in the light of what has happened in Berlin police will be reviewing what is in place." Guardian UK; BBC News

NSA watchdog on leave in whistleblower case
Allegations of retaliation against a whistleblower at the National Security Agency have left its top watchdog fighting for his job, according to an intelligence official and another individual familiar with the case. The case could offer some credence to Edward Snowden's claim that he could not have reported the government's domestic surveillance program without facing reprisals. George Ellard, the NSA's inspector general, was placed on administrative leave after he refused to give the whistleblower a certain job assignment. The Project on Government Oversight, an advocacy group, first reported last week that Adm. Mike Rogers, director of NSA, had placed Ellard on leave and recommended that he be terminated. Ellard is appealing that decision. Associated Press (CTV News)

US cities step up security at Christmas gatherings after terrorist truck attack on Berlin market which killed 12 shoppers
Cities across America are stepping up security at Christmas events following a terrorist truck attack on a Berlin market that has left 12 people dead. Police are boosting their presence at holiday villages and major sites around cities such as New York, Chicago and Boston as the US remains on high alert. It comes after a Christmas market in the German capital was deliberately targeted by a man, who is believed to have used a hijacked 25-tonne lorry to murder 12 people and injure 48 more. And in New York, police confirmed highly trained specialist units and its anti-terror squad would be deployed to high profile locations around the city. Sites expected to have a high armed police presence include the Winter Village market in Bryant Park, the Christmas market near Columbus Circle and the festive stalls in Union Square. Also under close surveillance by the security services are the world-famous Christmas tree at Rockefeller Center, Times Square and Herald Square, home to department store Macy's. Daily Mail

After Berlin atttack, the cracks in Germany's security are showing
An opinion piece by professor Christian Leuprecht states, "The attack in Berlin may have taken the world by surprise; the only surprise to the German security and intelligence establishment is that something of the sort did not happen sooner. Hannover, Würzburg, Ansbach: An air of terrorism has been hanging over Germany all year. Since the attacks in Paris and Brussels, German authorities have been on high alert, and nowhere more so than in Berlin: Note the pattern of sensational attacks in capital cities. The July shooting in Munich that caused authorities to shut down the city was the canary in the coal mine. As in Munich – but unlike Paris – the response in Berlin was swift and co-ordinated; with one notable difference: Information operations in Berlin were far superior because authorities there finally understood social media. Yet, authorities seem to have few leads (if any) and there are now doubts about the suspect who was initially apprehended. How is that possible? Much of German's security architecture was designed to prevent what happened during the Third Reich: The logic was to take domestic security out of the hands of the central government. Germany has some of the strictest privacy laws in the world. As a result, agencies are loath to talk to one another: Foreign intelligence (the *Bundesnachrichtendienst*, or BND) faces severe hurdles communicating with domestic intelligence (the *Verfassungsschutz*, which loosely translates to protection of the constitution) – and is subject to an extensive parliamentary inquiry into unauthorized "selector" data sharing with the U.S. National Security Agency." Globe and Mail

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

Meaghan_Willis

Min. @RalphGoodale announces nearly $4.4M in funding for recreational & cultural projects across Saskatchewan. #yqr #sask #Canada150

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Canadian Forces
"Search and rescue is going to become a lot less about search and a lot more about rescue." - Comd of @RCAF_ARC, LGen Hood #SAR

Coquitlam SAR
Outside of regular training, #SAR members get a lot of their experience the same way you do. Getting out & recreating with friends. #SARelf

The Canadian Press
UPDATE: Ferocious Fort McMurray wildfire voted @CdnPress news story of the year for 2016 http://bit.ly/2hDPaQJ

globalnews
Fort McMurray wildfire named Canada's news story of 2016 https://t.co/F7e8dxtaUf

Canadian Red Cross
It's been a challenging year for many people impacted by #ABfires. Send them your warmest #HolidayWishes

Transports_gc
Pour les collectivités: fonds visant à réduire blessures et décès sur #VoiesFerrées. tc.gc.ca/foalx @ReseauFCM @Gareautrain pic.twitter.com/B9mCgb5FKE

Transport_gc
Calling on communities to apply for funding to reduce injuries & fatalities at #TrainTracks tc.gc.ca/33j8g @FCM_online @oplifesaver pic.twitter.com/UpY8PTYR3V

NATIONAL SECURITY / SÉCURITÉ NATIONALE

CJFE
We join @OpenMediaOrg to call on government to release all results from the National Security consultation http://bit.ly/2hM4FEs

CBC News
Canadian telecoms push back on proposed police powers http://www.cbc.ca/1.3903930 #C31

The Muslim Lawyer
Eight reasons why Canada must repeal its anti-terror laws https://shar.es/1DWadk via @MiddleEastEye @nccm @ICLMG

Resiliency_CBoC
The Evolving Threat of #Terrorism: A Shifting Security Landscape in Europe by @The_Fuzz74 conferenceboard.ca/topics/securit… #lesm #natsec

NSPS (CBoC)
Fighting #Extremism: Counter-#radicalization and the "Danish Model" with @rolhol1 http://www.conferenceboard.ca/e-library/abstract.aspx?did=8492&utm_source=twitter&utm_medium=social&utm_campaign=kbtweet … #natsec #security #lesm #cdnpoli

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

SC Media
Domino's Pizza advises customers to change their passwords

Kaspersky Lab
We've built a new decryptor to help victims of CryptXXX! Don't pay the ransom! https://kas.pr/At8T #nomoreransom #infosec

SC Media
What did Yahoo know? And when did they know it?

LAW ENFORCEMENT / APPLICATION DE LA LOI

Joanne Schnurr
Stepmother and father now in courtroom. Suspended Mountie to find out his sentencing date in torture starvation trial of his son @ctvottawa

CTV Ottawa
Follow @JoanneCTV for updates from sentencing hearing for step-mother of child who was tortured by his father, a former RCMP officer.

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

John Howard Society
Keeping the mentally ill out of solitary, and out of prison: Editorial http://on.thestar.com/2hQ93VL via @torontostar

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NCCM
Mental health services needed in Somali community, says settlement director

John Howard Society
#Employment is a stabilizing factor in preventing crime but a #criminalrecord is a major obstacle to finding a job

CKNW
BC Coroner opens up about the fentanyl crisis @lizaCKNW980

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Connie Walker
RCMP say Alberta Williams case is now "very active" beacuse of new details revealed in a CBC News podcast.

CBCIndigenous
Missing and murdered Indigenous women inquiry launches new website ift.tt/2hWujFV pic.twitter.com/blzRutnZKn

OTHER / AUTRES

Amarnath Amarasingam
ISIS claims attack in Jordan, which killed 10 people, including a Canadian tourist Linda Vatcher. #Jordan #ISIS

CBCTheNational
ISIS has claimed responsibility for shootings in Jordan that left 10 dead, including a woman from Newfoundland http://www.cbc.ca/1.3904730

VassyKapelos
Canada calls for release of Joshua Boyle, Canadian held in Afghanistan after new video appears http://globalnews.ca/news/3137600/canada-calls-for-release-joshua-boyle-canadian-held-in-afghanistan-with-family/ … #cdnpoli

HuffPost Canada
Canada calls for release of couple held captive in Afghanistan since 2012 http://huff.to/2h6649Y

INTERNATIONAL

Independent
Germany told to expect 'further significant attacks' after Berlin lorry tragedy http://ind.pn/2hE8tcl

Associated Press
BREAKING: German prosecutor: Treating Berlin attack as act of terrorism but no claim of responsibility yet.

SkyNews
Gunman who shot three worshippers at mosque in Zurich was interested in "the occult", police have said trib.al/UHrWqn1

lemondefr
Un groupe radical kurde revendique l'attentat contre des soldats à Kayseri, en Turquie lemonde.fr/international/…

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

Today's News / Actualités
December 22, 2016 / le 22 décembre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

TOP STORIES / MANCHETTES

Extract, decode, analyze
As the RCMP tries to convince the public that phone encryption is hobbling its investigations, new documents obtained by VICE News show that the federal police agency already has the ability crack encrypted and locked cellphones without help from the owner or the manufacturer. The records, obtained via access to information request, show that the RCMP's British Columbia branch just renewed its license

for the Cellebrite Touch Ultimate. That device, according to the documents, "enables the most technically advanced extraction, decoding, analysis, and reporting of mobile data. It performs physical, logical, file system, and password extraction of all data (even if deleted) from the widest range of devices including legacy and feature phones, smartphones, portable GPS devices, tablets, and phones manufactured with Chinese chipsets." The cost of the renewal, dated February, 2016, was redacted from the documents. The records show that they were sent out to both the B.C. division of the RCMP, and the local RCMP detachment in Nanaimo. Other contract documents suggest that, for the Cellebrite device and an enclosure in which police can hack the phone — one that blocks all outside cell, Wi-Fi, and other signals — the total cost was just above $90,000. (…) "We generally do not comment on specific investigative methods, tools and techniques outside of court," an RCMP spokesperson told VICE News over email. Staying mum on their current techniques hasn't stopped the force from launching a public relations campaign on the problem of encryption — dubbed "going dark" — aimed at getting new powers, however. (…) Next month, Constable Frank Dudas of the RCMP's Technological Crime Section, is slated to speak on a panel regarding the "cutting-edge solutions" for search warrants, especially for encrypted and locked smartphones, "to maximize technology investments and respect privacy rights within Canada." Dadas will be joined on that panel by Daniel Embury, a technical director at Cellebrite. Ultimately, mention of this sort of technology appears nowhere in the federal government's national security consultations, which were designed to give the public a voice in drafting new legislation that could authorize — or forbid — certain intrusive investigative techniques. VICE News

Four charged in alleged human smuggling ring near Cornwall
Four people have been charged after a joint Canada-U.S. investigation broke up an alleged human trafficking ring operating across the St. Lawrence River near Cornwall. The charges come after a seven-month investigation and authorities say more charges may follow. The investigation, called Project Oinertia (the 'O' comes from the RCMP's 'O' division, plus 'inertia'), involved the Canada Border Services Agency, the Royal Canadian Mounted Police, the Akwesasne Mohawk Police Service and Massena Border Enforcement Security Task Force (BEST). Police allege the ring smuggled people across the border in both directions between Cornwall, St. Regis, Que., and Massena in New York state. The arrests were made in raids in Ontario and Quebec back on Oct. 20, but weren't announced until Thursday. A fifth person was arrested, but has not been charged. Ottawa Citizen; WWNYTV; Radio-Canada; CBC News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

'An over-stressed workforce with little or no support,' B.C.'s paramedics are hitting mental health tipping point
Incessant overdose calls and multiple drug deaths during shifts are taking a serious toll on the mental health of B.C. paramedics, according to their union. Bob Parkinson, director of health and wellness for the Ambulance Paramedics and Emergency Dispatchers of B.C., said even before the current fentanyl-related overdose crisis, paramedics were feeling strained while responding daily to life-and-death situations (…) Paramedics aren't able to respond as quickly to non-life-threatening calls and are arriving to find upset patients and family members. Parkinson said depression and anxiety are the most common mental-health issues among paramedics, but some are dealing with post-traumatic stress disorder or struggling with family problems and their own addiction issues. He's worried the workforce will lose quality women and men. Postmedia (Vancouver Province)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

2017 may be the year of the battle over encryption, again
As cyber security pros look to 2017 there's no shortage – as in previous years – of predictions that we're going to see more of the same: More spear phishing attacks, more DDoS attacks, more ransomware, more suspected state-sponsored intrusions … But the year may also be notable for another reason: The return of the fight to give police easier access to encrypted devices and documents through backdoors. "In the Western world I'm sure we'll see increasing pressure to do that," says Jacob Ginsberg, senior director of products at Toronto-based Echoworx, which makes enterprise email encryption solutions.

"Canadian police came out this past summer saying they want access to people's phones as part of an investigation … We're seeing a pretty serious erosion of our privacy by way of technology." With the installation of Donald Trump as president a number of observers believe the fight over giving law enforcement and intelligence agencies in the U.S. better access to encrypted communications and devices will be re-opened after having been smothered in 2016. It's a debate that was included in the just-closed federal public consultation on a new Canadian national security framework, which saw the IT and telecom industry line up against any law forcing makers or distributors of encryption solutions to add backdoors to their software or make decryption keys available. A discussion paper included the police arguments that encryption of mobile devices and data has stalled some investigations, although it also included arguments about expectations of privacy. IT World Canada

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Four charged in alleged human smuggling ring near Cornwall
Four people have been charged after a joint Canada-U.S. investigation broke up an alleged human trafficking ring operating across the St. Lawrence River near Cornwall. The charges come after a seven-month investigation and authorities say more charges may follow. The investigation, called Project Oinertia (the 'O' comes from the RCMP's 'O' division, plus 'inertia'), involved the Canada Border Services Agency, the Royal Canadian Mounted Police, the Akwesasne Mohawk Police Service and Massena Border Enforcement Security Task Force (BEST). Police allege the ring smuggled people across the border in both directions between Cornwall, St. Regis, Que., and Massena in New York state. The arrests were made in raids in Ontario and Quebec back on Oct. 20, but weren't announced until Thursday. A fifth person was arrested, but has not been charged. Ottawa Citizen; WWNYTV; Radio-Canada; CBC News

Belarusian steel mill BMZ ready to assist Canada with antidumping investigation
The Belarusian steel mill BMZ is ready to assist the Canada Border Services Agency with carrying out an antidumping investigation. Anatoly Savenok, Director General of Belarusian Steel Works (BMZ trademark), made the relevant statement in a recent interview with the SB. Belarus Segodnya newspaper, BelTA has learned. The BMZ Director General said: "It is difficult to predict the outcome of the investigation for now. I can only note that BMZ has declared its readiness to assist with the investigation. The Canada Border Services Agency will get answers to all the questions in addition to explanations needed to make the relevant decisions. In turn, the company will invite experienced lawyers, who will work together with specialists and entities of the company's proprietary distribution chain to take all measures to properly protect BMZ." Belarus News

Couple sent back to Canada for trying to sneak cat into New Zealand
A Canadian woman who authorities say managed to hide her 4-year-old pet cat Bella in her handbag during a trans-Pacific flight had her vacation cut short when border agents discovered the ruse at a New Zealand airport. The woman was refused entry into the country and she, her husband and the cat were forced to catch the next flight home, Ministry for Primary Industries spokesman Craig Hughes said Thursday. He called the woman's actions "reckless and dangerous." New Zealand has strict regulations for importing pets. Cats and dogs from most approved countries must have an implanted microchip and be quarantined for a minimum of 10 days after arrival. Hughes said the couple, both in their mid- to late-20s, managed to conceal the cat from the flight crew and other passengers during the 11,300-kilometre flight from Vancouver to Auckland. CTV News

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

OurMine Hacks Netflix's Twitter Account
Hackers who are part of the group called OurMine have managed to get control of the official Netflix Twitter account and post public messages to the nearly 2.5 million followers. One of the tweets taunts Netflix's security on Twitter, probably a weak password, with a message reading "World security is s**t. We are here to prove this." At the time of writing this article, Netflix seems to be back in control of its

Twitter account, but the company has also sent out messages using the official support account, which shows that it's still working on recovering after the hack. Softpedia; Register

Russian hacks into Ukraine power grids a sign of things to come for U.S.?
Russian hacking to influence the election has dominated the news. But CBS News has also noticed a hacking attack that could be a future means to the U.S. Last weekend, parts of the Ukrainian capitol Kiev went dark. It appears Russia has figured out how to crash a power grid with a click (…) The hackers sent emails with infected attachments to power company employees, stealing their login credentials and then taking control of the grid's systems to cut the circuit breakers at nearly 60 substations. The suspected motive for the attack is the war in eastern Ukraine, where Russian-backed separatists are fighting against Ukrainian government forces. But hackers could launch a similar attack in the U.S. "We can't just look at the Ukraine attack and go 'oh we're safe against that attack,'" said Rob Lee, a former cyberwarfare operations officer in the U.S. military, investigated the Ukraine attack. CBS News

US-Israel cybersecurity collaboration act signed into law
US President Barack Obama on Friday enacted legislation to strengthen collaborative cybersecurity research and development efforts between the United States and Israel, one of the congressman involved in drafting the bill said Monday. The US-Israel Advanced Research Partnership Act of 2016, which had bipartisan support, will expand existing joint research and create a grant for new development. Times of Israel

Chubb expands suite of cyber loss mitigation services for Canadian and U.S. policyholders
Chubb announced on Thursday an expanded suite of cyber loss mitigation services is now available to help the company's policyholders in Canada and the United States reduce the impact and likelihood of a cyber incident. Canadian Underwriter

LAW ENFORCEMENT / APPLICATION DE LA LOI

Extract, decode, analyze
As the RCMP tries to convince the public that phone encryption is hobbling its investigations, new documents obtained by VICE News show that the federal police agency already has the ability crack encrypted and locked cellphones without help from the owner or the manufacturer. The records, obtained via access to information request, show that the RCMP's British Columbia branch just renewed its license for the Cellebrite Touch Ultimate. That device, according to the documents, "enables the most technically advanced extraction, decoding, analysis, and reporting of mobile data. It performs physical, logical, file system, and password extraction of all data (even if deleted) from the widest range of devices including legacy and feature phones, smartphones, portable GPS devices, tablets, and phones manufactured with Chinese chipsets." The cost of the renewal, dated February, 2016, was redacted from the documents. The records show that they were sent out to both the B.C. division of the RCMP, and the local RCMP detachment in Nanaimo. Other contract documents suggest that, for the Cellebrite device and an enclosure in which police can hack the phone — one that blocks all outside cell, Wi-Fi, and other signals — the total cost was just above $90,000. (…) "We generally do not comment on specific investigative methods, tools and techniques outside of court," an RCMP spokesperson told VICE News over email. Staying mum on their current techniques hasn't stopped the force from launching a public relations campaign on the problem of encryption — dubbed "going dark" — aimed at getting new powers, however. (…) Next month, Constable Frank Dudas of the RCMP's Technological Crime Section, is slated to speak on a panel regarding the "cutting-edge solutions" for search warrants, especially for encrypted and locked smartphones, "to maximize technology investments and respect privacy rights within Canada." Dadas will be joined on that panel by Daniel Embury, a technical director at Cellebrite. Ultimately, mention of this sort of technology appears nowhere in the federal government's national security consultations, which were designed to give the public a voice in drafting new legislation that could authorize — or forbid — certain intrusive investigative techniques. VICE News

Yellowknife police test technology to identify high drivers

Yellowknife RCMP officers are testing out new technology to identify high drivers. Officers will be equipped with hi-tech mouth swabs and will administer roadside tests to see how well the swabs work in real life situations. The detachment is one of seven forces across the country testing the swabs, as the federal government prepares to legalize marijuana. "We have the dark, we have the cold, the environment itself. What we're doing is seeing how practical we can implement these devices and use them in real world situations," says Cpl. Todd Scaplin. If a driver decides to participate, they'll be asked to provide a saliva sample, which will be analyzed to see whether drugs are in their system. "Everything is confidential, there's no names taken, nothing like that. It's completely voluntary. If they don't want to do it, [it's] 'have a nice day. Thank you very much,"' says Scaplin. People who fail the test won't be charged. However, if they appear impaired anyway, officers will still investigate. "Nothing's changed. It's just that we're gonna hopefully eventually have really good tools for us to use," says Scaplin. CBC News

Every child in Tuk gets a gift, thanks to RCMP toy giveaway

Christmas came a little early for children in Tuktoyaktuk, thanks to a toy giveaway organized by the RCMP. The annual Christmas toy give away with Santa Clause was held this week in the Hamlet. Members of the RCMP and their spouses bought, wrapped, and sorted all of the presents to make sure everyone got an age appropriate gift. "I think it was a great event for the whole community," said Sgt. Marco Papillon with the Tuktoyaktuk RCMP. "It allowed RCMP officers and their families to meet with most of the community." Nestled on the shores of the Arctic Oceans, Tuktoyaktuk is an Inuvialuit hamlet of about 850 people, according to the 2011 census. The community is currently in total darkness until January 6. The event, which featured Christmas carols and refreshments, was supported by Stanton Group Limited. Several hundred parents and children reportedly turned out. My Yellowknife Now

Phil Sheegl's lawyer calls claim his client was 'in on it' false, stupid and ill-informed

The lawyer for former Winnipeg chief administrative officer Phil Sheegl says allegations about attempts to influence the award of a major Winnipeg construction contract are false, stupid, ill-informed and defamatory. The RCMP investigation into Winnipeg's police headquarters has unearthed emails that officers suggest show Caspian Construction owner Armik Babakhanians said he tried to curry favour with Sheegl and others to obtain the $156-million construction contract. The information was provided to a judge in February 2016 in order to obtain bank records and represents a snapshot of a two-year-old RCMP investigation, dubbed Project Dalton. Before police are allowed to search financial records, they are required to present evidence to support their request for institutions to produce documents. According to prior information presented to a judge in order to obtain a search warrant, the police-HQ investigation originally involved fraud and forgery allegations. Last year, the investigation expanded into allegations the principal engineer and architect on the project, as well as Caspian's owner, conspired to offer project director Ossama AbouZeid a $600,000 secret commission. AbouZeid said he never asked for one, was never offered one and he never received one. CBC News

Pictou Landing youth charged with attempted murder

Pictou County District RCMP, with the assistance of Northeast Nova Major Crimes Unit, has charged a 17-year-old male as a result of a stabbing in Pictou Landing. Shortly after 11:30 p.m. on Tuesday evening, RCMP received a call of a stabbing that occurred on Beach Rd. in Pictou Landing First Nation. Preliminary investigation determined that a 29-year-old male from Belle Marche, Nova Scotia, had suffered apparent stab wounds to his body. He was transported to the Aberdeen Regional Hospital in New Glasgow with serious but non-life threatening injuries. He remains in hospital. The News

Fatalities involving impaired drivers rise to 20 from 5 since 2013

Motor vehicle fatalities involving impaired drivers have steadily increased over the past four years across the province, according to New Brunswick RCMP. So far this year, there have been 20 fatalities. In 2015 there were 15, while 2014 had 11 and there were five in 2013. Staff Sgt. Gilles Blinn, the RCMP's provincial traffic co-ordinator, said he's not sure why the numbers keep climbing, even after vigorous anti-drinking and driving campaigns. He also admits he doesn't know how to fix the problem. CBC News; Radio-Canada

Man charged with 1st-degree murder in Big Island Lake Cree Nation death

RCMP have charged Anthony Mitsuing with first-degree murder in the death of a 28-year-old on Big Island Lake Cree Nation. Jordan Sandfly's body was found earlier this week outdoors on the Saskatchewan First Nation. Mitsuing, 32, is from the Makwa Sahgaiehcan First Nation. Both men were known to each other and police are not seeking anyone else in relation to Sandfly's death. CBC News

17-year-old missing Yellowknifer located, say RCMP
Yellowknife RCMP are advising the public that a teenager reported missing earlier this week has been located. Ethan Moses, 17, had been last seen on Monday at the Capitol Theatre in downtown Yellowknife, according to an RCMP press release sent out on Wednesday afternoon. Police said in a news release Thursday morning that Moses has been located. The RCMP thanked the citizens of Yellowknife for their assistance in locating Moses. CBC News

More RCMP please
Re: Story in the Dec. 8 edition of The NEWS ('Worked up about speeding')
A letter to the editor states, "In response to the query as to why the RCMP do not do more to enforce the speed limits in Parksville, I was given an answer in the summer of 2015 when I called the RCMP to complain about the speeding cars on Morison Avenue between McMillan and Finholm streets. "There is only one officer assigned to traffic daily and his/her hours are 8 a.m. to 4 p.m." You cannot set up a radar trap with only one officer. Do not think reducing the speed on Chestnut Street would help. The speed limit on Morison is already 40 km, but some drivers ignore it. The officer then told me if I had actual licence plate numbers, makes, models and colours of cars they would be able to respond to my complaint. I sat for hours in my car that summer to record this information. I dropped the list off at the RCMP station. The dispatcher asked if I wanted a callback. I said I did. I am still waiting for that call." Parksville Qualicum Beach News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Elderly pedophile convicted of sex tourism seeks parole for second time
An 86-year-old Montreal man who was convicted of having sex with young girls during his frequent trips to Dominican Republic is scheduled to make his second request for parole on Thursday. Joseph-Charles Côté, a former pilot with the Canadian military, is currently serving a seven-year sentence he received in 2014 after he was found guilty at the Montreal courthouse of four counts related to how he sexually abused a girl for years and three child pornography charges. Materials seized from Côté revealed he recorded his abuse of the girl and served as evidence that had intercourse with at least one other girl. Côté travelled to Dominican Republic several times following his retirement in 1987 but that all came to an end in February 2013 when he was arrested in that country following an investigation by the Sûreté du Québec and Canada Border Services Agency. Police who searched his hotel room in Sosua found the walls covered in photos of nude girls. (…) Côté is currently incarcerated at a federal penitentiary in Laval. He was denied parole in July after making his first request. The parole board was not impressed with how he denied he is a pedophile and is therefore unwilling to address his sexual deviance. Montreal Gazette

'Watershed moment' for bail
The John Howard Society says it expects to soon have the capacity to take on more than 200 new people in their bail supervision program after receiving increased funding from the province to hire more case workers. The program is also expected to expand to courthouses in Perth, Pembroke and L'Original. That is in addition to two new workers in Ottawa, including one who will be exclusively available to those suffering from mental illness. The expansion is expected to ease pressure at the often overcrowded Ottawa-Carleton Detention Centre, as more low-risk accused people who otherwise wouldn't be released can now access the bail supervision program. Currently, the bail supervision program in Ottawa has space for 250 people and is operating at capacity. The new hires are expected to nearly double the number of accused that can participate in the program, which provides supervision to offenders who are in poverty and might lack a surety, or someone who will monitor to make sure they obey their release conditions. "Honestly, it's a watershed moment for bail. We've been advocating for this expansion for many years," said Tyler Fainstat, executive director of the John Howard Society of Ottawa. "Hundreds

more people will have access to community supervision rather than waiting at OCDC for their trial." Ottawa Citizen

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Fentanyl in Yukon: Kwanlin Dün Chief vows community patrols
The Chief of Kwanlin Dün First Nation is raising warnings about fentanyl. Doris Bill says the community is trying every possible step to prevent people from dying due to opioid overdose over the holidays. Four people have died in Yukon in the last seven weeks, in cases the Chief Medical Officer of Health says are likely related to opioid overdose. Bill says preventative measures will include community patrols during the holidays. "Four people are suspected to have died from this and it's urgent in my view. We need to reach people especially people at the street level," she says. Bill recorded a warning distributed through social media this week. "All Yukoners are important to us. Please be safe and be informed. To reduce your risk, never use street drugs alone," Bill says in the video. The message also tells viewers that Naloxone kits are available at the Kwanlin Dün's health clinic as well as Blood Ties Four Directions in Whitehorse. The video has been seen about 1,500 times through Facebook. CBC News

Seized fentanyl could have led to multiple overdoses: N.L. advocate
On the street, they have a few nicknames: green monsters, greenies, green beans, green apples. "Even cocaine is laced with fentanyl now. It's in essentially everything." Tree Walsh. They're 100 times stronger than morphine, and have caused an increasing number of deaths in Newfoundland and Labrador in recent years. It's fentanyl, an extremely potent synthetic pain medication, and it doesn't just come from pharmaceutical companies. Drug dealers are cooking them up in home labs and selling them disguised as less-potent Oxycontin pills and other drugs. On Wednesday, police said "Oxycontin" pills seized by the RNC/RCMP's Combine Forces Special Enforcement Unit (CFSEU) last month as part of Operation Titanium have been confirmed by Health Canada to be fentanyl. Police believe the pills were made in a clandestine lab and not by a pharmaceutical company, since they look identical to Oxycontin 80s -- green with the number 80 stamped on one side and "CDN" on the other. Telegram

1 in 4 Canadians admit to driving while legally drunk, half think limit is too low
A full quarter of Canadians admit they've had a few too many drinks before driving in the past, a new poll reveals. A full half of the population thinks the legal blood-alcohol limit for drivers should be raised. The survey was conducted between by Ipsos on behalf of Global News between Dec. 16 and Dec. 19, and it highlights some surprising trends when it comes to attitudes toward impaired driving across Canada. Sean Simpson, vice president of Ipsos Public Affairs, said the polling firm didn't place a time limit on when an incident occurred, so it's perhaps not surprising that 24 per cent of respondents said they'd been legally drunk behind the wheel. One of the most surprising figures in the survey, said Simpson, was that about half of respondents said they believe the legal limit for what constitutes impaired driving (0.8 per cent blood alcohol content or higher) is too low. Global News

Cyberstalking more prevalent among single, never-married women, study shows
Cybersecurity expert urges caution in sharing personal information online. Cyberstalking is more prevalent among single, never-married young women, a new study from Statistics Canada shows. The study of internet users aged 15 to 29 also showed those with a history of being victimized are much more likely to experience cyberstalking, or cyberbullying. The results come as no surprise to Ron MacLeod, a cybersecurity specialist who has worked in the industry for about 30 years and is currently the president of the High Technology Crime Investigation Association for Atlantic Canada. Young women tend to live their social life online, through online dating sites and the use of social media, said MacLeod, the father of two teens. CBC News (2016-12-20)

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Police still 'dedicated' to busting pot dispensaries, even as laws set for change
Hamilton police say they'll remain 'dedicated" to enforcing current pot laws and crack down on sales and trafficking from marijuana dispensaries, even as the federal government commits to changing regulations. The latest messaging regarding pot legalization in the city comes after police seized $20,000 in marijuana and marijuana derivatives from Royal Farmacy at 1395 Main Street East, near Kenilworth Avenue. A 45-year old Hamilton, believed to be the owner of the business, was charged with possession for the purpose of trafficking both marijuana and THC, and for proceeds under $5,000. CBC News

From Dime Bags To Money Bags, Businesses Look Forward To Legal Marijuana
It's Sunday afternoon and Toronto's Centre for Social Innovation is packed full of marijuana enthusiasts perusing tables of goods. Everything from marijuana-infused barbecue sauce to medicated body rubs is available at Green Market, where artisans peddle their various craft cannabis products. Such events, which sell to patients and casual users alike, operate within a foggy regulatory environment. Selling marijuana is illegal unless you are a large-scale producer licensed under Health Canada's medical marijuana regime. However, licensed producers are only permitted to sell dried cannabis flower and oils, in spite of a Supreme Court ruling last year that said Canadians have a right to access medical marijuana in all of its forms. The year ahead is expected to be a pivotal one for Canada's burgeoning marijuana industry, as the federal government is planning to table legislation in the spring that will lay out the ground rules for a legal, recreational market. There's also a lot of money to be made in marijuana. A report published by consultancy firm Deloitte in October estimates that legalizing recreational use of the drug could ignite a $22.6-billion industry in Canada. That figure includes sales of marijuana products as well as ancillaries such as security, transportation and testing labs. Civilized

Canora resident asks, 'Is Canada growing to pot?'
A letter to the editor states, "Our federal government will soon legalize marijuana. I'm not saying it's a good thing or bad thing. It is so prevalent in society something had to be done. My thoughts on the matter is that if the federal Liberals think that they are going to put these illegal pot-growing operations out of business, they must stay monetarily competitive or better with the underground prices for cannabis. Otherwise, people will not buy in the legal outlets." Canora Courier

PUBLIC SERVICE / FONCTION PUBLIQUE

Reevely: Toxins leaked into Dow's Lake from new hospital site, feds say
Poisonous chemicals from the demolition of the Sir John Carling Building have seeped into Dow's Lake and pose challenges for building a new hospital at the northeast corner of the Central Experimental Farm. (…) In the case of the Sir John Carling site, near Carling Avenue and Preston Street, the contamination is just a couple of years old. The 11-storey former headquarters of Agriculture Canada was demolished in 2014 and as part of the takedown, two basement levels were filled with pulverized concrete from the rubble. Before the demolition, the building had been carefully stripped of everything from its wiring to asbestos: the contractors knew a lot of dust would go flying even from the many small controlled explosions used to knock the building's supports out. But the concrete filling the basement, it turns out, was tainted with phenol from the 400 kilograms of dynamite used in the demolition. Phenols are a diverse class of chemical compounds, many of them found in nature. The kind used in explosives is highly acidic: in humans, phenols can cause chemical burns to the skin, eyes and lungs. Ottawa Citizen (2016-12-21)

OTHER / AUTRES

Jordan arrest man suspected of funding Daesh attack
Jordanian security forces have arrested a man suspected of funding an attack by Daesh which killed 10 people including a Canadian tourist, a security source said Wednesday. The suspect was detained in a raid on a house in Karak province on Tuesday by police looking for the perpetrators behind Sunday's shooting spree, official news agency Petra quoted the source as saying. The suspect "admitted to ties with the terrorist cell that targeted security forces and civilians" on Sunday "and to buying weapons and funding the cell," the source said. Agence France Presse (Gulf News Jordan)

INTERNATIONAL

Attentat de Berlin : les empreintes digitales du suspect retrouvées sur le camion
L'Allemagne a annoncé, mercredi, qu'elle recherchait activement un demandeur d'asile tunisien de 24 ans, soupçonné d'être l'auteur de l'attaque au camion qui a fait 12 morts à Berlin, le plus grave jamais revendiqué par le groupe Etat islamique dans le pays. Ses empreintes digitales ont été retrouvées sur le camion, a précisé le ministre de l'Intérieur, Thomas de Maizière, lors d'une conférence de presse, jeudi 22 décembre. La chasse à l'homme se poursuit. Anis Amri a été officiellement identifié par la justice antiterroriste qui, dans un avis de recherche européen, propose jusqu'à 100 000 euros de récompense. L'homme *"mesure 1m78, pèse environ 75 kg. Il a des cheveux noirs et des yeux bruns. Il peut être violent et armé !"* met en garde le parquet fédéral à l'attention de la population. France TV Info ; Chronicle Herald

Attentat de Berlin: la famille du suspect sous le choc
En état de choc, la famille d'Anis Amri, principal suspect dans l'attaque de Berlin, affirme qu'il avait quitté sa ville pauvre de Tunisie avec l'espoir de trouver une vie meilleure en Europe. Devant le domicile familial, dans un quartier populaire de Oueslatia (centre), Abdelkader, les yeux rougis, raconte à l'AFP la trajectoire de son frère, le benjamin de la famille, visé par un mandat d'arrêt à l'échelle européenne. En mars 2011, Anis Amri a quitté illégalement la Tunisie par la mer vers l'île italienne de Lampedusa, fuyant une condamnation par contumace de quatre ans de prison pour vol et cambriolage, affirme à l'AFP Abdelkader. Un responsable sécuritaire local a confirmé à l'AFP ces informations. Outre la condamnation, « Anis est aussi parti pour fuir la misère. Il n'avait aucun avenir en Tunisie et il voulait à tout prix améliorer la situation financière de notre famille qui vit en dessous du seuil de pauvreté comme la majorité des habitants de Oueslatia », poursuit Abdelkader. Agence France-Presse (La Presse)

Obama dumps post-9/11 registry for some immigrant men, mostly Muslims
The Obama administration said Thursday it is officially scrapping a post-9-11 requirement for immigrant men from predominantly Muslim countries to register with the federal government. The U.S. hasn't used the program since 2011, but a top immigration adviser to President-elect Donald Trump has spoken of renewing it. The decision to end the National Security Entry-Exit Registration System, or NSEERs, comes amid growing international terror fears and Trump's suggestions that he could ban Muslim immigrants from the United States. After a truck attack killed 12 in a Christmas market in Berlin this week, Trump told reporters, "You know my plans." The program's elimination could make it more complicated for Trump's administration to launch its own registration system for Muslims. Associated Press (Globe and Mail, Global News)

Snowden still has contacts with Russian intelligence: U.S. House report
Former National Security Agency contractor Edward Snowden "has had and continues to have contact" with Russian intelligence services, according to a newly declassified U.S. House of Representatives Intelligence Committee report released on Thursday. The Pentagon found 13 undisclosed "high risk" security issues caused by Snowden's release to media outlets of tens of thousands of the U.S. eavesdropping agency's most sensitive documents, the report said. If China or Russia obtained access to information on eight of the 13 issues, "American troops will be at greater risk in any future conflict," said the report, which contained a table outlining the "issues", but like large portions of the document, was blacked out. Reuters

Yahoo email scan shows U.S. spy push to recast constitutional privacy
Yahoo Inc's secret scanning of customer emails at the behest of a U.S. spy agency is part of a growing push by officials to loosen constitutional protections Americans have against arbitrary governmental searches, according to legal documents and people briefed on closed court hearings. The order on Yahoo from the secret Foreign Intelligence Surveillance Court (FISC) last year resulted from the government's drive to change decades of interpretation of the U.S. Constitution's Fourth Amendment right of people to be secure against "unreasonable searches and seizures," intelligence officials and others familiar with the strategy told Reuters. The unifying idea, they said, is to move the focus of U.S. courts away from what makes something a distinct search and toward what is "reasonable" overall. The basis of the argument for change is that people are making much more digital data available about themselves to businesses, and that data can contain clues that would lead to authorities disrupting attacks in the United States or on U.S. interests abroad. While it might technically count as a search if an automated program trawls through all the data, the thinking goes, there is no unreasonable harm unless a human being looks at the result of that search and orders more intrusive measures or an arrest, which even then could be reasonable. Civil liberties groups and some other legal experts said the attempt to expand the ability of law enforcement agencies and intelligence services to sift through vast amounts of online data, in some cases without a court order, was in conflict with the Fourth Amendment because many innocent messages are included in the initial sweep. Reuters

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Glenn McGillivray
Mental health response to #FortMcMurray #wildfire evacuees to be assessed by province

Conrad Sauvé
My #2016YearInReview: 25,000 @redcrosscanada volunteers respond to #ABfires, #HurricaneMatthew & more https://www.linkedin.com/pulse/canadian-red-cross-looking-back-eventful-year-wish-2017-conrad-sauve?trk=prof-post ...

The Province
'An over-stressed workforce with little or no support,' B.C.'s paramedics are hitting mental health tipping point http://bit.ly/2idbDFx

Canadian Forces
Combat Engineers build bridges and skills during winter Ex #PALADINRESPONSE http://ow.ly/58NM307nc4C

Forces canadiennes
Des sapeurs de combat exercent leurs aptitudes en construisant des ponts dans le cadre de l'ex #PALADINRESPONSE http://ow.ly/yb2q307ncny

CBC Indigenous
17-year-old Yellowknifer missing since Monday, say RCMP

NATIONAL SECURITY / SÉCURITÉ NATIONALE

ICLMG
Surveillance des journalistes: l'opposition dénonce le rapport montréalais http://www.lapresse.ca/actualites/montreal/201612/19/01-5052854-surveillance-des-journalistes-lopposition-denonce-le-rapport-montrealais.php ... @lp_lapresse #polcan #qcpoli #Montreal

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CBC Ottawa
Human smuggling conspiracy nets charges against 5 people http://ift.tt/2ijNhpx #ottnews #ottawa

Postmedia News
Four charged in alleged human smuggling ring near Cornwall - Four people have been charged after a joint Canada...

Jewel 88.5
CBSA travel tips over the holiday season - http://885thejewel.com/cbsa-travel-tips-over-the-holiday-season/ … #Holiday #Travel #Tips #Canada

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

WIRED
The most dangerous people on the internet today are often the most powerful people:

Dark Reading
Malware Used In DNC Breach Found Tracking Ukraine Military http://ubm.io/2h6jGyH #Russia #DNC #FancyBear

LAW ENFORCEMENT / APPLICATION DE LA LOI

Justin Ling
The RCMP say phone encryption is thwarting their investigations. Funny, as they've been hacking phones for years.

Alison Crawford
"This hearing would be an embarrassment for the RCMP were it to proceed" more from Osoyoos Times on Cst. Goyal http://www.osoyoostimes.com/rcmp-clear-goyal-of-all-allegations/ …

Jim Bronskill
Accused in Amanda Lindhout hostage-taking to face trial next October http://ctv.news/cqkD7LU #cdnpoli #hw

The Province
Surrey's most wanted: These 10 men are on RCMP's naughty list http://bit.ly/2icG7XU

CBC News
Police use new tactic to catch texting drivers: riding the bus http://www.cbc.ca/1.3907419

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Margot Van Sluytman
Excellent content.Howard Saper's final comment is Sawbonna. http://ipolitics.ca/ …/12/20/the-price-we-pay-for-punishment/

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

CBC Indigenous
Fentanyl in Yukon: Kwanlin Dün Chief vows community patrols http://ift.tt/2ifg6kk

PUBLIC SERVICE / FONCTION PUBLIQUE

Ottawa Citizen
Poisonous chemicals from the demolition of the Sir John Carling Building have seeped into Dow's Lake

INTERNATIONAL

Stewart Bell
In his 1st speech 2 weeks ago, new ISIS spokesman specifically called for attacks on markets. #Berlin @siteintelgroup

La Presse
Attentat de Berlin: les autorités allemandes critiquées

CBC News Alerts
Majority of Aleppo evacuees now in neighbouring province of Idlip, but UN envoy fears region could be next target of Syrian gov't forces.

The Globe and Mail
Fingerprints of Berlin attack suspect found on truck door

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

Today's News / Actualités
December 26, 2016 / le 26 décembre 2016
9:00 - 18:00 ET

This collection contains news items that appeared online between 9:00 a.m. and 6:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 09h00 et 18h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

TOP STORIES / MANCHETTES

Anti-drone conference hears from correctional service
Don Head, the commissioner of Correctional Service of Canada (CSC), told an anti-drone conference earlier this month in the United Kingdom that drones pose health, safety and security risks for correctional environments. He also said the unmanned aerial vehicles present opportunities for enhancing the overall correctional response to the needs of offenders, staff, victims and communities. Head's presentation was

shared with the Whig-Standard on Friday, a sign of more transparency at the CSC this year... "CSC is currently partnered with the National Research Council and has embarked on a collaborative investigation of the commercial technologies for the detection of drones," Head, who has been commissioner since 2008, said. Whig-Standard

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Major St. Norbert power outage caused by snowplow
An incident involving a snowplow has cut power to 1,661 customers, says Manitoba Hydro. At 6:15 a.m. this morning a piece of snow clearing equipment hit a transformer pole behind a grocery store on Pembina Highway in St. Norbert. Hydro crews are on site. Manitoba Hydro says they should know very shortly how long it will take to restore power. CBC News

Deux femmes portées disparues à Surrey
La Gendarmerie royale du Canada de Surrey est à la recherche de deux jeunes femmes qui ont disparu pendant les vacances. Catoraine Joseph, 15 ans, a été vue pour la dernière fois par sa famille près d'un pâté de maisons le long du boulevard King George. Radio-Canada ; CBC News

N.-É. : un homme de Tantallon porté disparu
Un homme de 46 ans de Tantallon manque à l'appel depuis le 23 décembre dernier. La Gendarmerie royale du Canada (GRC) demande l'aide du public afin de le repérer. Anthony Glen Sinclair mesure environ 1,80 mètres (5 pi 11 po) et pèse 165 livres. Il a les cheveux bruns et aurait été vu pour la dernière fois portant un chandail de flanelle, ainsi qu'un jeans bleu. L'homme pourrait être au volant d'une fourgonnette blanche 2009, de marque Ford. Le dernier contact avec sa famille aurait eu lieu le 23 décembre dernier et il a été porté disparu le 25 décembre. Ceux croient détenir de l'information importante sont priés de la communiquer à la GRC. Radio-Canada; Chronicle-Herald

2 men missing after Christmas Day hike
West Vancouver Police are asking the public for help finding two men who may be lost on a North Shore mountain after setting out for a hike on Christmas Day... An investigation was launched to find the registered owner of the vehicle, 43-year-old Roy Tin Hou Lee of Vancouver. Police say Lee is "an avid hiker" who set out for a hike on Christmas Day with 64-year-old Chun Sek Lam, also of Vancouver... Twenty search and rescue members are currently on the trails searching for the missing men. CTV News

'Hazardous winter conditions are expected': Environment and Climate Change Canada
On Monday morning, Environment and Climate Change Canada's website showed much of southern Manitoba still under wind and snowfall warnings... **Public Safety Canada** said people should keep an emergency kit that can be sufficient for a family for 72 hours. The kit should include drinking water, food, medicine, a first-aid kit and a battery-operated or wind-up flashlight. CTV News

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Jessica's favourite things from 2016 - Canada shifts its stance on personal data security
An opinion piece states "This past November, it came to light that the Canadian Security Intelligence Service (CSIS) had been illegally collecting Canadian data for over a decade. The federal government chastised the agency for its actions, and handed down a ruling stating that the intelligence service had breached its duty to inform the court of its mechanisms. The information had been collected for reasons other than national security threats, and therefore, should not have been retained by CSIS in the first place. This report accompanied several others in 2016 detailing the relationship between federal regulators and Canadian data. News that a Quebec police station tracked the smartphones of six journalists made headlines around the world and attracted commentary from history's most famous whistleblower, Edward Snowden. The reaction to these stories by federal courts and regulators demonstrates a more modern perspective on data than we've seen from Canadian governments in the

past. It's encouraging for many Canadians to see that the legacy left by Bill C-51 needn't be a permanent one..." Mobile Syrup

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

NIL

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

Un policier récompensé pour son rôle dans la Grande traversée
La Gendarmerie royale du Canada (GRC) a récemment récompensé le bénévole responsable de la sécurité pour la Grande traversée (LGT), ce relais pan-canadien de jeunes cyclistes organisé par une équipe de bénévoles et le Conseil scolaire francophone de la Colombie-Britannique. Le gendarme Ivan Provost, le coordonateur national de la sécurité de la Grande traversée, a reçu une citation du commandant de la Division C de la GRC pour son dévouement. Encore une fois cette année, une équipe de bénévoles dévoués s'affairent à préparer un nouveau tracé de la Grande traversée (LGT) pour permettre à 280 jeunes de parcourir environ 300 kilomètres à vélo en trois jours. Pour la cinquième Grande traversée, le relais commencera à Victoria pour finir au Nouveau-Brunswick. Cela veut dire des dizaines et des dizaines de municipalités et de villes parcourues. Le gendarme Ivan Provost, des Laurentides au Québec, est responsable de faire approuver le trajet de la Grande traversée chaque année. Pour ce faire, il accomplit des mois de travail bénévole. « Ivan c'est notre liaison entre les villes, les municipalités, les provinces, les services de police et l'équipe qui fait l'itinéraire de LGT », explique le fondateur de la Grande traversée, Laurent Brisebois. Radio-Canada

Colten Boushie shooting in review
The top crime story in the province in 2016 erupted in August on a farm in the rural municipality of Glenside. The shooting death of Colten Boushie, a 22-year old from Red Pheasant First Nation, sparked outrage among First Nation people and caused a social media firestorm... The case fueled racial tensions from the beginning, starting with a news release from the RCMP that described an initial confrontation on the property. Battlefords News-Optimist

Victim shows forgiveness
A Vernon woman who was the victim of a crime gave a Christmas gift to the thief. Pauline Vankoll lost her handbag at the Village Green Mall food court on Nov. 24. While a search failed to turn it up, mall staff were able to give her descriptions of some possible suspects at the food court during the time her bag went missing. Then RCMP suggested Vankoll use a locating app in an effort to locate her purse and phone... On Dec. 22, the victim contacted the RCMP detachment to say she wanted to give the suspect a Christmas hamper full of food items and requested officers deliver it. Castanet.net

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Anti-drone conference hears from correctional service
Don Head, the commissioner of Correctional Service of Canada (CSC), told an anti-drone conference earlier this month in the United Kingdom that drones pose health, safety and security risks for correctional environments. He also said the unmanned aerial vehicles present opportunities for enhancing the overall correctional response to the needs of offenders, staff, victims and communities. Head's presentation was shared with the Whig-Standard on Friday, a sign of more transparency at the CSC this year... "CSC is

currently partnered with the National Research Council and has embarked on a collaborative investigation of the commercial technologies for the detection of drones," Head, who has been commissioner since 2008, said. Whig-Standard

The 8 biggest Kitchener-Waterloo news stories of 2016
5. Grand Valley Institution inmate, 30, dies after being found unresponsive in cell. When 30-year-old inmate Terry Baker died in a segregation cell at the same prison where Ashley Smith was found asphyxiated almost a decade ago, it sparked a national debate on the use of solitary confinement. CBC News

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Clark calls opioid crisis biggest story of 2016 in year-end interview
Premier Christy Clark says the ongoing opioid crisis was both the biggest story and most significant challenge for BC in 2016. In a year-end interview with NEWS 1130, Clark says no one predicted the devastation the drugs would wreak upon the province. "Nobody really saw it coming the way it did and it's just been a terrible crisis and everyone one of those deaths is preventable," says Clark. "There are lots of challenges in the course of the year but this is one where people are dying every day and resources have just been completely overwhelmed." Illicit drug overdose deaths in BC for 2016 reached an all-time high of 755 by the end of November with December numbers expected next month for a grand total. November also had the monthly record number of deaths with 128, an average of more than four a day. News 1130

The 8 biggest Kitchener-Waterloo news stories of 2016
2. The fentanyl crisis. Fentanyl, a powerful painkiller that's responsible for an epidemic of overdoses that have swept Ontario, has become a growing threat to public health. So much so, law enforcement and government have been forced to change their tactics in dealing with the rash of deaths caused by the deadly street drug, which has now surpassed car accidents to become the third-leading cause of accidental death in the province. CBC News

The 8 biggest Kitchener-Waterloo news stories of 2016
1. Does Waterloo region have a racism problem? The question came up repeatedly this year. Wilfrid Laurier University held a summit this spring to address the issue after an uptick of reported racism and racist graffiti. CBC News

Manitoban's Waiting Months To Access Drug Treatment In The Province
People in Manitoba suffering from addiction are waiting months to acccess treatment programs accross the Province. Despite warnings of the opioid crisis from area police and RCMP the province has not increased funding for treatment programs in Manitoba. Pembina Valley Online

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Lacing dog treats with cannabis is a growing business
Even for a puppy, Kat Donatello's black Labrador, Austin, was hyperactive. After experimenting with natural supplements on her older dog, Donatello slipped a special biscuit to Austin. "It just kind of took the edge off of him," she recalled. Hamilton Spectator

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

NIL

INTERNATIONAL

Chile's government works to restore power in quake-affected zone
Chile's government set to work on Monday repairing roads and restoring electricity to southern regions affected by a major earthquake that struck on Christmas Day, frightening thousands but resulting in no fatalities or major damage. The quake, a magnitude 7.6 centered off Chiloe Island northwest of Patagonia, caused thousands in the tourism and salmon farming region to evacuate to higher ground amid fears of a tsunami. A tsunami never materialized however and, thanks to strict building codes in the earthquake-prone nation, structural damage was light. By Sunday night, almost all Chileans had returned to their homes. The quake did, however, cause at least one bridge collapse, cut power to 21,000 Chileans, and severed sections of the island's major highway. Reuters (Globe and Mail)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

NoFlyListKids
We're leaving behind the Canadian No Fly List in 2016. We hope @RalphGoodale @JustinTrudeau fix it soon to start 2017 right ☺#NoFlyListKids

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

CBCAlerts
RT @CBCManitoba: Major St. Norbert power outage caused by snowplow ift.tt/2hgBbwk
pic.twitter.com/BKXMH284AZ

ici_cb
Deux femmes portées disparues à Surrey rc.ca/MyxC2G

cbcnewsbc
2 missing females sought by Surrey RCMP buff.ly/2hgVM3Q

iciacadie
N.-É. : un homme de Tantallon porté disparu rc.ca/Myyng3

CTVVancouver
2 men missing after Christmas Day hike on Cypress Mountain bc.ctvnews.ca/2-men-missing-…

NATIONAL SECURITY / SÉCURITÉ NATIONALE

canadaCJFE
VICE reporter @BMakuch heads to court in February to fight a production order for his source.
#ProtectPressFreedom http://protectpressfreedom.ca https://pbs.twimg.com/media/C0m_T4ZW8AACqhN.jpg

CBCManitoba
Press freedom in Canada eroded by post-9/11 obsession with security ift.tt/2iv74Gz pic.twitter.com/XESuOnS747

MobileSyrup
Jessica's favourite things from 2016 mobilesyrup.com/2016/12/26/jes… @JessicaVomiero pic.twitter.com/jEG0nEkrgB

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CanBorder
See if you qualify for a personal exemption when bringing goods home to #Canada: http://www.cbsa-asfc.gc.ca/travel-voyage/pdt-pdt-eng.html#z1 … #BoxingDay #shopping

CYBER SECURITY / CYBERSÉCURITÉ

Safety_Canada
This year, you loved to learn ways to be more cyber safe #Bestof2016 http://ow.ly/Nu1f307nzrn https://pbs.twimg.com/media/C0nUCtuXEAA3SSt.jpg

Securite_Canada
Cette année, vous avez aimés apprendre à être cyber sécuritaire #Meilleurde2016 http://ow.ly/ubjd307nzvC https://pbs.twimg.com/media/C0nUCu5XUAEtXt8.jpg

LAW ENFORCEMENT / APPLICATION DE LA LOI

ici_cb
Un policier récompensé pour son rôle dans la Grande traversée rc.ca/Myv1vr

CastanetNews
Victim shows forgiveness #VernonBC bit.ly/2i8gW60

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

WhigStandard
Anti-drone conference hears from correctional service thewhig.com/2016/12/26/ant… pic.twitter.com/TeY6CRiVdD

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NEWS1130
AUDIO/ARTICLE: @christyclarkbc calls opioid crisis biggest story of 2016 in year-end interview with NEWS 1130 bit.ly/2i08OXq pic.twitter.com/W3X3r89BqY

pembinavnews
Manitoban's Waiting Months To Access Drug Treatment In The Province zpr.io/PGWBi

INTERNATIONAL

raffpantucci
Police uncover ISIS plot to set off phone bomb on UK streets in the run up to Christmas https://t.co/S7nPFHMO9Y

nytimes
Russia says terrorism is unlikely to be the cause of the Black Sea plane crash https://t.co/TxvlKFdHfL

globeandmail
Chile's government works to restore power in quake-affected zone https://t.co/W4v55cK2be

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

Today's News / Actualités
September 19, 2016 / le 19 septembre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Tackling the complexity of counter-radicalization
As the domestic terrorist threat has evolved since the advent of the Islamic State into the danger of citizens being weaponized by jihadist propaganda into lone-wolf attackers, governments in Canada and elsewhere have begun focusing on counter-radicalization as an effective means of counter-terrorism. When **Public Safety Minister Ralph Goodale** was sworn-in last November 4, his mandate letter included an order to "Create an Office of the Community Outreach and Counter-radicalization." While it sounds

straightforward, the office, whose director and full scope and mandate will be revealed this fall according to **Goodale**, the effort will unfold at the confluence of politically loaded debates about culture, religion, privacy, the role of the internet in radicalization and the difference between piety and nihilistic fanaticism. Michael Zekulin, a terrorism researcher at the University of Calgary, said the terms of reference and mission of the office will be crucial. "It's pretty much going to be make-or-break from the get-go, about whether you're going to get people to buy in," said Zekulin. "If you come up with a document or mission statement and certain communities or certain people look at this and say, we don't agree with this, you're in trouble." Reached by iPolitics, **Goodale spokesman Scott Bardsley** said it was still too early to comment on who might be appointed to direct the office or go into the details of its scope and mandate. **Bardsley** did say, ***"Public Safety has consulted with stakeholders, experts in the security field and community leaders about the creation of the new national centre of excellence for community outreach and engagement."*** On August 17, following a speech to the Canadian Association of Chiefs of Police in Ottawa, **Goodale** himself told reporters that he was in the final stages of choosing a director from a shortlist of candidates. ***"That person will be directing a very important effort to up our game in Canada in terms of recognizing and understanding the process of radicalization, who's vulnerable to it, why they would be vulnerable and what are the most effective tools and instruments and people and techniques and practices to prevent the problem in the first place and - in other cases where the problem has begun to develop - how do you intervene strategically?"*** Coordinating an approach to counter-radicalization is tricky business; there's no-one in the field who would suggest that what the government is trying to do will be easy and there seems to be little consensus about the right way to go about it - or even what the office's specific role should be. iPolitics

ISIL, ISIS or Daesh? Ottawa's past efforts to change its term for terrorist group plagued by confusion

The recent government decision to refer to the Islamic State of Iraq and the Levant by the name "Daesh" isn't the first time Ottawa has tried to change the way they refer to the terrorist group. A Conservative government edict last year to dump ISIL in favour of ISIS, for the Islamic State of Iraq and al-Sham, foundered in part over the inability to translate ISIS into an acceptable French acronym. (…) DND spokesman Daniel Le Bouthillier said last week the department and Canadian Forces will now use "Daesh" or "Daech" in French in its news releases and in dealing with the public and media. The changes have already been made on the Operation Impact website. "We are following the lead of senior governmental officials in this regard, while aligning our language with that used by other allies working in the area," added Le Bouthillier. **Public Safety Minister Ralph Goodale** noted the change in the introduction to a recent government report on terrorism. ***"This group is neither Islamic nor a state, and so will be referred to as Daesh in this report,"*** he wrote. National Post (Ottawa Citizen)

Neve: Mr. Trudeau, it's time to deliver justice for torture victims Almalki, Elmaati and Nureddin

An opinion piece by Alex Neve, Secretary General of Amnesty International Canada, states, "On Oct. 21, 2008, when I sat with Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin after the release of the report from the inquiry into their cases that had been conducted for two years by former Supreme Court of Canada Justice Frank Iacobucci, I was sure that they would soon see justice for what they had been through. But the staggering and disgraceful truth is that nearly eight years later, these three men – all survivors of torture that Canadian officials made possible – seem further away from justice than ever. They have, in fact, perversely only been put through deepening injustice, this time through obstructive Canadian government tactics in our own legal system. (…) There was much hope that the change of government would bring a change in approach to this case, a change that would at long last deliver justice. After all, Justin Trudeau himself – and other key members of his new government, including Foreign Minister Stéphane Dion and **Public Safety Minister Ralph Goodale** – had supported the 2009 House of Commons Motion calling for an apology and compensation. They now had the power to make that happen." Ottawa Citizen

Hack Attack Could Manipulate Biometric Border Screening: Report

Canadian border officials are concerned about potential hack attacks against their biometric databases, according to a new report from The Toronto Star's Alex Boutilier. The concerns were outlined in a report prepared by Canada Border Services Agency officials for the country's **Public Safety Minister** last November. The document outlines multiple digital threats to border security, with one of the more

sophisticated threats coming in the form of breaches into biometric identification systems that could "produce false acceptances and/or rejections," leading border agents to deny entry to innocent individuals while allowing in those known to pose security threats. It's an example of the new kinds of security concerns associated with sophisticated border screening technology. While biometric identification is effective in automating aspects of border screening and increasing their reliability, there is a new danger in potential "physical and technical" attacks against the attendant data centers and networks. With biometric identification becoming an increasingly important means of screening temporary residents and soon perhaps permanent residents and citizens, this is an important matter of concern. And it will only become more important as more governments around the world embrace the same technological approach at their borders. Find Biometrics

Canada Already Meets the Requirements of the UN Marking Scheme
The Firearm Marking Regulations, introduced on December 23, 2004, have been postponed for 11 consecutive years by 3 separate governments for one simple reason. No government wanted to be responsible for killing Canada's legitimate civilian firearm industry. Until now. On June 1, 2017 – ten short months from now – the shoe drops. The Trudeau government seems to have great faith in all things United Nations, but unfortunately they seem to be unwilling to examine all of the facts when it comes to the UN's Firearm Marking Scheme. (…) Should the Trudeau government implement these regulations, it is debatable how long we will have a retail firearm industry in Canada. Sure, we may be able to purchase ammunition still, but that is small comfort if we cannot purchase the firearms to use it? If you disagree with Canada's looming implementation of the Firearm Marking Regulations, please write to the following people and express politely why you believe implementing these regulations is a very bad idea for Canada: The Rt. Hon. Justin Trudeau, Prime Minister of Canada; The **Hon. Ralph Goodale, Minister of Public Safety; Michel Picard MP, Parliamentary Secretary to the Minister of Public Safety**; Bob Zimmer MP, Co-Chair of the Parliamentary Outdoor Caucus; Yvonne Jones MP, Co-Chair of the Parliamentary Outdoor Caucus; Your own federal Member of Parliament. Ammoland

Towards inclusive nation states: burkinis, hijabs and self-determination
An opinion piece states, "In France, the US and in many otherwise enlightened corners of Europe people and politicians are asking an awkward question: do Muslims belong in the modern nation-state? (…)In recent weeks, two contrasting approaches to this question have played out through the lens, of all things, of women's clothing. In France, photos shared on social media of armed police approaching a Cote d'Azur beachgoer in a full-body swimsuit and enforcing a ban on burkinis kicked off a firestorm around freedom, faith and what it means to be French. Despite the ban being overturned by a Nice court a week later, the debate over whether burkinis are acceptable beach wear, and whose decision that should be, rages on. Meanwhile, local police in Canada and Scotland have been offered an official hijab. New policies in the Scottish Metropolitan police and the Royal Canadian Mounted Police have introduced hijabs as part of police uniforms. They join the London Metropolitan police service, where hijab has been part of uniforms for more than a decade. A **spokesman for Canada's Public Safety ministry** told Canada's CBC that women could wear the headscarf ***"if they so choose".*** The decision, he said, was a reflection of the institution's values: ***"The Royal Canadian Mounted Police is a progressive and inclusive police service that values and respects persons of all cultural and religious backgrounds."*** Middle East Eye

American border authorities unfairly weed out weed users
An opinion piece states, "Marijuana has become widely accepted as both a recreational and medicinal drug. While weed is becoming more socially accepted here in Vancouver, our American neighbours have been less lenient. In a recent interview with the CBC, Canada's **Public Safety Minister Ralph Goodale** discussed how Canadians who admitted to border guards that they had smoked pot without a medical licence were barred from entering the States. Those banned *can* enter the States, but only if they apply for permission to enter beforehand, which costs about C$752, and will be raised to C$1,195 later this year. The expiration dates on provided permits vary, and those dates are all up to the officer who reviews the application. Once it's expired, you have to apply again, and pay the fee *again*. I understand that countries deserve the right to set rules on who can or cannot cross their borders. This particular restriction only affects people who admit to having smoked marijuana without a medical marijuana licence. But what infuriates me about this rule is that it's not a real ban at all. The barrier is one that anyone can circumvent

provided they have the money. It's not about following the rules, or being morally sound, or even hiding the so-called "reefer madness" from young children. No, it's about squeezing more dollars from citizens." The Peak

Broadcast media / Médias télédiffusés :

CBC News reports on allegations of torture of three Canadians following the 9/11 attacks. (Minister mentioned) Rough Transcript

Thousands of pages of secret files obtained by CBC reveal how Canada's police and intelligence service not only knew three Canadians were being tortured in Syrian jails in a post-Sept. 11 crackdown, but co-operated with Syrian officials in their interrogations. **Public Safety Minister Ralph Goodale** has admitted to CBC that a torture directive remains in effect. (CBC R1, 6:02, 8:04, 10:04, 11:03, CBC TV Regina, 6:06; CBC News Network, 8:49, 11:14)

Following the explosions in New York City, Canadian **Public Safety Minister Ralph Goodale** has released a statement calling the incidents concerning, and pointing out that Canadian officials always cooperate closely with our American counterparts. So far his office will not discuss whether or not there Is any Canadian connection to the explosion. (CFFR-AM, 9:34, 10:04; CKWX-AM, 10:10; CFTR-AM, 11:05, 11:35; CIWW-AM, 11:34; Rogers-22, 11:33)

TOP STORIES / MANCHETTES

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Nova Scotia drought unusual, catches people unprepared
The severe drought affecting parts of Nova Scotia may be causing more trouble than it would elsewhere in Canada because Nova Scotians aren't used to drought conditions. For more than a month now, people in the southwest have reported dry wells and throughout the province, rivers and lakes are low (…) Hadwen encourages farmers and homeowners to contact Drought Watch to report the impacts of drought. The program collects reports from people all across Canada, but historically, have collected few reports from Nova Scotia. CBC News

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

NIL

Broadcast media / Médias télédiffusés :

CBC News has obtained a cache of 18,000 government documents revealing the RCMP and CSIS sanctioned the mistreatment of Abdullah Almalki, Ahmad El Maati, and Muayyed Nureddin — three Canadians who were arrested and tortured in Syria in the years after the 9/11 attacks. CBC News reporter Terence McKenna. has prepared a three-part TV documentary, *The Torture*

Files — a joint investigation by *The National* that starts tonight and *the fifth estate* this week. (CBC R1, 9:12)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Ottawa considers expanding Remote Traveller Processing program
A unique new way of patrolling the border between Canada and the U-S is playing out in the small Quebec community of Morses Line, on the border with Vermont. The border crossing is being manned remotely with border agents stationed 700 kilometers away in Hamilton, Ontario. The Remote Traveller Processing program kicked off in February and there are now plans to expand it to 19 other border crossings across the country. Travellers who stop at the crossing in rural Quebec, enter into an enclosed garage and park next to a kiosk that allows border agents in Hamilton to communicate with them, show their passport and pay duties using a credit card. If the border guard has any doubts about the traveller they are then directed to a manned border point about 13 kilometers away. But critics say the program will see border guards working the equivalent of call centres, as they police a border crossing hundreds of kilometres away. 610 CKTB

Rotten Ambassador Bridge homes worth more to city standing
Looking across the street from her home in Windsor's west end, Carla Wiedemann cringes at the rotting boarded-up homes, desperately wanting them to be replaced and her neighbourhood restored. She bought her home on Edison Street, for $80,000 back in 2004. But around the same time, owners of the Ambassador Bridge started buying up properties to make way for the twinning of the busiest border crossing between Canada and the U.S. It didn't take long for a handful of homes across the street from Wiedemann to fall into disrepair, left to decay while bridge owners battle it out in court for permission to expand their crossing. Wiedemann's home is now worth $65,000. She and her neighbours know their property values would skyrocket, if the boarded up houses were replaced with new ones, but that won't happen any time soon. "These houses, if they have to be torn down, build new ones right in their place," she told CBC News. Leaving the structures as they are translates into more tax revenue for the city than empty lots. By not allowing the bridge company to tear down the houses, the city is forcing the owner — Manuel (Matty) Moroun — to pay more tax. CBC News

Canada Already Meets the Requirements of the UN Marking Scheme
An opinion piece states, "The Firearm Marking Regulations, introduced on December 23, 2004, have been postponed for 11 consecutive years by 3 separate governments for one simple reason. No government wanted to be responsible for killing Canada's legitimate civilian firearm industry. Until now. On June 1, 2017 – ten short months from now – the shoe drops. The Trudeau government seems to have great faith in all things United Nations, but unfortunately they seem to be unwilling to examine all of the facts when it comes to the UN's Firearm Marking Scheme. Canada's already strict firearm import process accomplishes every goal specified in United Nations Protocol 55/255, formally called the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime. (…) Each firearm contains a serial number that is "unique" to that make and model of firearm. That serial number also identifies the year of manufacture. Commercial firearm manufacturer's records are so meticulously detailed that the make, model and serial number of a specific firearm will reveal when and where the firearm was manufactured, when it was shipped and to which country, when the firearm was released from Canada Border Services Agency (CBSA) and the name and address of the company who imported the firearm." Ammo Land

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Who Are the Russian-Backed Hackers Attacking the U.S. Political System?
Two teams of highly skilled hackers directed and protected by the Russian state are on the offensive. Cybersecurity experts and intelligence officials tell NBC News the same hackers who broke into the Democratic Party's computers, the World Anti-Doping Agency's Administration System and who are

implicated in the leaks of the personal emails of former Secretary of State Colin Powell and the health documents of Olympians are executing a Kremlin-backed campaign of cyber-espionage and sabotage. Their target: Western democratic institutions and Russia's political opponents. "They are starting to figure out the way to apply the power they have in terms of technical capabilities into the geopolitical aspect," Italian cyber security investigator Stefano Maccaglia told NBC News. NBC News

The Encryption Key That Secures the Web Is Being Changed for the First Time
Soon, one of the most important encryption key pairs on the internet will be changed for the first time. The Internet Corporation for Assigned Names and Numbers (ICANN), the US-based non-profit responsible for various internet infrastructure tasks, will change the key pair that creates the first link in a long chain of cryptographic trust that lies underneath the Domain Name System, or DNS, the "phone book" of the internet. This key ensures that when web users try to visit a website, they get sent to the correct address. Without it, many internet users could be directed to imposter sites crafted by hackers, such as phishing websites designed to steal information. Motherboard

How Cybercriminals Target Victims: Report Cites Top Information Resources
Cybercriminals, whose attacks cost organizations millions of dollars a year, do extensive research on their targets. They gather organizational and personal information before deciding which vulnerabilities to exploit(…) One takeaway from the report is that websites that appear to be intended to help protect people from cyber attack are actually resources for cyber attackers (…) The top three public web sources criminals use for gathering information are Shodan.io, virustotal.com and companies' own individual websites. Hacked

Security Shortcomings Could Slow IoT Adoption
There are various elements that throttle the speed of Internet of Things adoptions and advancements but one of the most significant revolves around security. Most companies involved in creating IoT devices, platforms and strategies at least acknowledge security is paramount for consumer adoption over the long haul. Each time there's a security breach of any magnitude, whether learning that a child's Internet-connected toy has been breached or a smart home appliance was tapped by outsiders, consumer confidence can be rocked just enough for them to hold off for now. Despite the obvious need for IoT security, there are several market indicators that there's still some work to be done. For example, most (90%) organizations don't have a cybersecurity strategy for the Internet of Things, according to the new Cybersecurity Preparedness Benchmarking Study by the Berkeley Research Group (BRG). Most (86%) also don't have a strategy to deal with big data. MediaPost

LAW ENFORCEMENT / APPLICATION DE LA LOI

Procès d'Alain Perreault : les scénarios de l'opération « Mr. Big » détaillés
L'architecte de l'opération « Mr. Big » qui a permis de piéger Alain Perreault témoigne au procès de l'homme de 54 ans, accusé du meurtre de Lyne Massicotte. L'agent d'infiltration, dont l'identité est protégée, détaille les 41 scénarios auxquels l'accusé a participé avant de passer aux aveux. Cet agent a agi un peu comme le metteur en scène de l'enquête visant à créer une organisation criminelle fictive autour du suspect. Il a participé à une dizaine d'enquêtes semblables qui regroupent également des policiers de la Gendarmerie royale du Canada et de la Sûreté du Québec. Selon le témoin de la Couronne, Alain Perreault a d'abord été approché le 30 septembre 2009 par un agent qui a feint d'être perdu dans son quartier. À ce moment, l'enquête sur la disparition de Lyne Massicotte piétinait. La femme de Chambly n'a pas été revue après être venue visiter Perreault à Québec. Les agents d'infiltration ont d'abord demandé à Perreault de faire des petits travaux comme des transports de marchandises qui avaient l'air tout à fait légaux. Après quelques semaines, l'organisation lui a offert de participer à des opérations illégales, « des artifices », mentionne l'agent en spécifiant qu'aucun crime n'est commis en réalité. Le policier répète que le but des scénarios préliminaires vise à montrer au suspect les valeurs de l'organisation, soit l'honnêteté, la confiance et la loyauté. Radio-Canada

Pas de demande pour le port du hijab chez les policières du Roussillon

Alors que la Gendarmerie royale du Canada (GRC) a autorisé le port du hijab chez ses agentes, aucune demande en ce sens n'a été formulée à la Régie intermunicipale de police Roussillon. La Régie refuse de prendre position concernant cet accommodement vestimentaire que la GRC a autorisé à la fin d'août. François Michaud, des relations avec les médias à la Régie, a indiqué que si une telle requête devait être formulée, elle serait étudiée en temps et lieu. Il en est de même pour toute autre formulation d'accommodements raisonnables. Le hijab, symbole religieux musulman, est un voile qui recouvre les cheveux, les oreilles et le cou, laissant à découvert le visage. Le Reflet

New Nanaimo RCMP commander outlines police priorities
Supt. Cameron Miller makes a quick introduction and apologizes for breaking an interview appointment. Miller, the Nanaimo RCMP detachment's new commanding officer, is also head of the RCMP's Vancouver Island tactical team and has an evolving situation – a man with a firearm and possible shots fired – on his hands, but still pauses to apologize for postponing a meeting. (…) Miller strongly supports police engagement with youth through RCMP school liaison work and programs such as Kids for Kids and the youth empowerment program that run in Georgia Avenue Community and Fairview Elementary schools. "We want to expand those programs," Miller said. He's also a strong backer of 529 Garage, a mobile app-based bike anti-theft program launched in Nanaimo in June, that allows police to return more recovered stolen bikes to their owners. Miller agrees there are more serious crime issues such as the drug trade, but said police can't safely involve the public in catching people dealing fentanyl. A major side benefit of Garage 529 is its potential for safe, positive community engagement in crime prevention. Nanaimo Bulletin

RCMP Warning Youth The Dangers Behind Social Media
Facebook, Twitter, Instagram or even Snapchat are the ways many youth communicate with each, and while it may be convenient at times it can also be dangerous as well. Okotoks RCMP is putting out a gentle reminder as kids are back in school to be aware of what they share or post on social media. Sgt Sukh Randhawa says the worldwide web is big place anyone if they want to can get information on you. "You got to be conscious of the fact how much information you're putting out in social media," he says. "You never know who is looking at your account, never know who you're inviting into your friend's circles or giving access to your accounts. There is a lot of personal information about you on social media and you have to guard that." Social media sharing can lead to online bullying or even identity theft and Randhawa says it's important to not give out too much information about yourself or someone you know online. Okotoks Online

Large quantity of marijuana seized by Saskatchewan RCMP investigating grow-up
RCMP seized a large quantity of marijuana while investigating a suspected grow operation in Saskatchewan last week. At 11:20 a.m. CT on Sept. 16, police executed a search warrant in the RM of Medstead. Turtleford RCMP said marijuana plants, packaged marijuana, cash and firearms were seized. Police arrested Cory Graham, 44, and Melanie Boulette, 34, and 43-year-old Oscar Gutierrez-Reyes. Gutierrez-Reyes is from Ontario and the other two are from Medstead. All have been charged for production of cannabis marijuana, possession for the purpose of trafficking, possession of property obtained by crime. Global News; 620 CKRM

Journée d'éradication dans les régions des Laurentides et de Lanaudière
Les policiers de la Sûreté du Québec ont participé à l'éradication de plants de cannabis dans plusieurs champs dans les régions des Laurentides et de Lanaudière dans le cadre du programme Cisaille. Au total, plus de 1 800 plants de cannabis ont été saisis. Les policiers ont également procédé à l'arrestation de trois personnes. Ils pourraient faire face à des accusations de production de cannabis. Les enquêtes se poursuivent et d'autres arrestations sont à prévoir. La Sûreté du Québec tient à souligner la collaboration du détachement de Saint-Jérôme de la Gendarmerie royale du Canada et des Forces armées canadiennes. Les policiers rappellent que la période actuelle est particulièrement propice à la récolte des plantations de cannabis. Ils invitent donc le public à signaler toutes les allées et venues inhabituelles de véhicules ou d'individus suspects dans leur voisinage aux policiers. Nord Info

Cops For Kids complete annual cycling trek

After 10 days on the road, they have cycled into the hearts of 18 communities around southeastern British Columbia. Riders from the 15th annual Cops For Kids ride arrived in Kelowna Sunday (after cycling into Vernon Saturday afternoon). The team of 28, which included Const. Nicolas Reimann and detachment transcriptionist Denise McMahon from Vernon-North Okanagan RCMP detachment, cycled across the southern Interior in order to raise money for children in medical, physical, or traumatic crisis. Funds raised from this event go to support local children who are provided with transportation to medical treatment, medical supplies, medical equipment, learning tools and mobility aids, to name a few. With recent cutbacks on government programs and other charities, families are leaning on Cops for Kids more than ever. Vernon Morning Star

Photo radar is a "cash cow"
An opinion piece states "Today's truth bomb comes from Mayor Lisa Holmes of Morinville, just outside of Edmonton, a place like many other Canadian communities that has struggled to find the right balance with photo radar enforcement. Morinville's photo radar program started in 2009. It's been run by a private contractor that reports to the town office. The program was soon raising $300,000 a year, but some felt there was too much focus on handing out tickets and generating revenue. Things got so heated that in 2014 Morinville held a plebiscite. Fifty-five per cent voted to keep the program. Nonetheless, the new council vowed to make sure the program was all about safety, as opposed to being a cash cow for the local government. Town council recently approved numerous new measures to better police its own photo radar authorities. Photo radar operators will now need to keep track of where and why they're setting up and make that information available to the public. Streets with a high rate of accidents or high numbers of pedestrians will be more of a focus, along with residential areas and school zones. Enforcement on collector and arterial commuter roads will be no more than 60 per cent of enforcement hours per month. Why were such changes necessary? If a photo radar contractor is getting paid per ticket, Holmes said, they will sit at a certain site if they know it has a huge amount of traffic, even if there's no real safety issues there. And then came Holmes' truth bomb: "They were spending 90 per cent of their time in three different spots that were on the edge of a town and it's just like it was a bit of a cash cow, honey pot situation." (…) Under the new rules, Morinville RCMP will approve all spots for photo radar and decide how long photo radar can operate at each site. "It gives people more comfort in knowing it's not the contractor themselves that's choosing, because then you can look at it that it's about money," Homes said." Drayton Valley Western Review

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Province plans to reduce the number of former inmates released to Edmonton streets
The sun was rising over the courthouse to the east of Churchill Square, where Randy Hetchler was pacing back and forth. "I arrived in the city at 6 a.m. I had nowhere to go. Nothing was open," he said. "I didn't walk too far because shoes sucked and had no laces, again." It's been a similar story almost every time Hetchler, whose criminal record consists of theft- and drug-related misdemeanour charges, has been released from the jail or the remand centre outside of Edmonton. Late at night or early in the morning, a cramped van drops him off downtown at a time when not even the homeless shelters are doing intake. It's an abrupt release back into society, one that highlights the lack of protocol to keep people like Hetchler from falling back into the criminal justice system. The result: a haphazard operation that is cost Canadians' safety - and their wallets. To keep people locked up without cause is unconstitutional, but the alternative that Hetchler keeps living also troubles Chris Hay, the executive director of the Alberta chapter of the John Howard Society, a nation-wide prison-reform group. "No one should be held in jail longer than they've been sentenced to simply because they're homeless," Hay said. "Conversely, if that's the case and we've got to punch you out into the streets of Edmonton and you've got nowhere to go, I don't want that either." While jails for inmates with sentences of under two years do some discharge planning, remand centres, where the average stay is less than a month, do even less. (…)Federal prisons, where inmates are serving sentences longer than two years, have more opportunity to plan for release. It's more challenging in provincial jails since the time people spend there is generally measured in months. Remand centres measure in days - and in Alberta, 52 per cent of people in stay fewer than five. CBC News; Radio-Canada

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Cyberbullying Hurts Even More For Teens Facing Mental Illness
An opinion piece states, "ICQ was the big thing when I was a kid. It was one of the Internet's first live chat rooms, very popular with the kids in the early years when it was still referred to as "the Worldwide Web" and your dial-up modem took 10 minutes at minimum to connect, so you had to really want it. (…)Yes, we can share anything now and anyone can see it. This has opened the portal to a new dimension of evil, including (but by no means limited to): body shaming, bullying, psychological torture, self-worth issues, mental illness, sex crimes (including revenge porn), and almost every other form of disturbing behaviour you can think of. (…)Since the rise of social media and widespread information, there have been enough suicides to make you feel ill. They call it cyberbullying now, and it has become a new avenue to psychologically destroy teens that are struggling with mental illness online. From the sex crime surrounding Raetaeh Parsons to the chilling harassment of Amanda Todd, the Internet is the new weapon of choice." Huffington Post

Growing crystal meth use by Filipino community in Banff sparks concern
There are concerns in Alberta's Bow Valley that members of the Filipino community are using shabu - a slang name for crystal meth - to help them work longer hours. "A few clients had reported knowledge of this being used, that it went by a different word than what we've heard before, and that they're facing different kinds of barriers in seeking help and support," said Meagan Stewart, coordinator of the Bow Valley Immigration Partnership. The organization has taken part in two community meetings with local employers, Alberta Health Services and the RCMP this year to discuss the use of shabu. "It seems to be … people in the community are trying to work multiple jobs and then trying to maintain the level of stamina in that work," RCMP Staff Sgt. Eneas said. "Often times, from the discussions, they were working anywhere from 14-, 16 and 18-hour days in two or three jobs." The meetings have been an opportunity for different organizations to share information about the drug. "It seems to be very underground," Eneas said. "We - the police - haven't had a lot of information come to light about it, but other service groups are hearing discussions about it … talking about specific shabu abuses." CBC News

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

MPI needs to rethink survey design
An editorial states, "Maybe Manitoba Public Insurance should have done more homework before implementing its random roadside survey on drug use. It need only have looked south of the border to Washington to see how that state conducted similar research — and here's the kicker — without the police being involved. MPI is facing considerable criticism for its decision to ask participants stopped by police in a random Checkstop to participate in the drug-use research. Some view the research design as coercive and invasive. While MPI has made it clear participation is voluntary and the information gleaned will be kept confidential, the fact the police are involved doesn't sit well. Some are concerned that with police performing the stop, refusing is out of the question. (…) When asked why MPI chose to use the police, spokesman Brian Smiley said: "MPI needed to survey drivers who are on the roadway. Doing so in a parking lot would not be a representative sample of the driving population." Sure. Because those driving in parking lots never drive on the road. There is no doubt the use of drugs while driving is a serious issue, particularly if the federal government moves ahead with plans to legalize marijuana. Unlike alcohol use, which can be determined through a breathalyzer, being high while driving is more difficult to determine.

That's because people metabolize THC — the chemical in pot that makes you stoned — differently. Drug-impairment tests have been deemed untrustworthy and a poor indicator of impairment by Canadian courts, which may explain why there are few drug-impairment charges laid compared with drunk-driving charges. So it's not really clear how a survey on drug use will increase safety. There's still more research that needs to be done." Winnipeg Free Press

PUBLIC SERVICE / FONCTION PUBLIQUE

Former statistics chief questions Liberal promise of more independence
The country's former chief statistician is speaking out to explain what led up to his sudden resignation last week. Wayne Smith quit on Friday afternoon and his resignation letters accused the federal government of hobbling his agency's independence by forcing Statistics Canada to use the government's central IT department, Shared Services Canada. In an interview today, Smith says federal officials told him the centralized IT program could crumble if Statistics Canada left because it would embolden other frustrated departments to demand independence from the arrangement. Canadian Press (CTV News, Winnipeg Free Press)

OTHER / AUTRES

NIL

INTERNATIONAL

Suspect in New York, N.J. bombings taken into custody after shootout
Authorities on Monday apprehended 28-year-old Ahmad Khan Rahami — wanted in connection with two Saturday bombings, in Seaside Park, N.J., and Manhattan — after an apparent shootout with police. Chris Bollwage, the mayor of Elizabeth, N.J. — another city touched by the widening probe — told reporters that Rahami was taken into custody in the neighboring city of Linden. One officer was struck in the hand, another on a protective vest, the mayor said. Rahami was also shot and was taken away in an ambulance, the mayor said. Television footage showed the suspect being wheeled into an ambulance, hands cuffed, eyes open. He was taken to University Hospital in Newark, according to a hospital spokeswoman, but his condition was not immediately available. Police and the FBI had announced early Monday that they were seeking Rahami in connection with the bombings in New Jersey and Manhattan, though his role in the incidents remains unclear. Rahami is a naturalized U.S. citizen born in Afghanistan, according to the FBI. Washington Post

Stabbings of nine at Minnesota mall investigated as possible terrorist act
Authorities are investigating the stabbings of nine people at a Minnesota mall as a potential act of terrorism, a finding that would realize long-held fears of an attack in the immigrant-rich state that has struggled to stop the recruiting of its young men by groups such as Daesh (also known as ISIS, ISIL and Islamic State). A young Somali man dressed as a private security guard entered the Crossroads Center mall in St. Cloud over the weekend wielding what appeared to be a kitchen knife. The city's police chief said the man reportedly made at least one reference to Allah and asked a victim if he or she was Muslim before attacking. The rampage ended when the man was shot dead by an off-duty police officer. None of the injured suffered life-threatening wounds. Associated Press (Toronto Star)

Suspect in New York and New Jersey bombings in custody after shootout with police, officials say
An Afghan immigrant wanted for questioning in the bombings that rocked a New York City neighbourhood and a New Jersey shore town was captured Monday after being wounded in a gun battle with police that erupted when he was discovered sleeping in a bar doorway, authorities said. Ahmad Khan Rahami, 28, appeared conscious, his upper right arm bandaged and blooded, as he was loaded into an ambulance in Linden. Two officers were wounded in the shootout but were not believed to be seriously hurt, authorities said. Associated Press (National Post)

U.S. mistakenly grants citizenship to at least 858 immigrants
The U.S. government has mistakenly granted citizenship to at least 858 immigrants from countries of concern to national security or with high rates of immigration fraud who had pending deportation orders, according to an internal Homeland Security audit released Monday. The Homeland Security Department's inspector general found that the immigrants used different names or birthdates to apply for citizenship with U.S. Citizenship and Immigration Services and such discrepancies weren't caught because their fingerprints were missing from government databases. DHS said in an emailed statement that an initial review of these cases suggest that some of the individuals may have ultimately qualified for citizenship, and that the lack of digital fingerprint records does not necessarily mean they committed fraud. Associated Press (Toronto Sun, CP24)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

News 1130
@RalphGoodale calls NYC/NJ blasts "concerning." Says Canadian officials always cooperate closely with our American counterparts.

620 CKRM
Ralph Goodale says Parole Board decisions must take public safety into mind http://bit.ly/2cKfbdg

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

CBC News Alerts
Water limits placed on Halifax-area homes over drought. No watering lawns, washing cars. BG: http://cbc.ca/1.3767563

NATIONAL SECURITY / SÉCURITÉ NATIONALE

NCCM
Time for answers: Docs show CSIS and RCMP's role in post-9/11 torture of 3 Canadians in Syria #natsec #cdnpoli

CBC – The Current
New docs show how close RCMP/CSIS worked w/ Syrian interrogators torturing Canadians Listen: http://cbc.ca/1.3768531

CBC – The Current
Hear @CBCNews Terence McKenna on RCMP email trail that shows what Cdn Intel officials knew about "interrogation" .."Syrian style " Today AMT

ICLMG
WATCH report on #CSIS & #RCMP's role in post-9/11 #torture of 3 Canadians in #Syria on @CBC http://www.cbc.ca/1.3669425 #cdnpoli #stillnojustice

CBC News
Documents show CSIS and RCMP's role in post-9/11 torture of 3 Canadians in Syria http://www.cbc.ca/1.3669425

Michelle Shephard
#ICYMI. Josh Boyle & Caity Coleman, held by the Taliban with their babies. What they reveal in their writings home.

Rabble.ca
New report reveals potential extent of invasive Stingray surveillance @OpenediaOrg #cdnpoli http://buff.ly/2cPRLpU

Craig Forcese
Good piece. There's risk in treating counter violent extremism as a panacea. Also a risk in not making the effort.

iPolitics
Tackling the complexity of counter-radicalization | iPolitics http://ift.tt/2cWizCk

OAG_BVG
09/20 Hearing-Senate National Security & Defence re: Study on issues related to Defence Policy Review #SECD #SenCa http://ow.ly/4j463048l29

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Border_Services
Buddy the Bear at #YEG had a great time welcoming kids home from @dtf_yeg #dreamstakeflight

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Ray Boisvert
It's the simple stuff that will get y'a: Poor cyber hygiene - not zero days - to blame for high-profile intrusions

CSE_CST
The Quantum challenge:

CSE_CST
How is CSE contributing? We are the centre of the Govt of Canada's activities on quantum

CSE_CST
How do we protect systems and information in the face of emerging quantum technology?

CSE_CST
For most Canadians encryption equals trust and confidence when they are interacting on-line

CST_CSE
Il est clair que pour la plupart des Canadiens qui communiquent en ligne, le chiffrement est un gage de confianc

Blackberry
#BlackBerry10 smartphones got NATO's 1st approval for classified comms up to "Restricted" level #GovTrusted http://blck.by/2cT5lSM

Symantec
Critical bug means #Android devices can be taken over using just an image http://symc.ly/2d23OMW #MobileMonday

Ann Cavoukian
Not to mention lack of #Privacy! Security Shortcomings Could Slow IoT Adoption 09/19/2016

Ann Cavoukian
Beware of all things "smart." http://blog.practicalethics.ox.ac.uk/2016/09/carissa-veliz-on-how-our-privacy-is-threatened-when-we-use-smartphones-computers-and-the-internet/ …

Public Safety Canada
The Government of Canada's public consultation on cyber security is underway. Have #YourCyberSay! http://ow.ly/IB2B304lzcr

Sécurité publique
La consultation publique du gouv. du Canada sur la cybersécurité est en cours. Donnez votre #OpinionCybersécurité! http://ow.ly/1Yy8304lzsw

USA Today
Why you might want to own a 'burner phone' http://usat.ly/2cJ4vel via @marc_saltzman

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

CLMG
Omar Khadr just turned 30 & still hasnt been apologized to & compensated http://iclmg.cfswpnetwork.ca/omar-khadr-just-turned-30/ … #cdnpoli #Gitmo #OmarKhadr #stillnojustice

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

John Howard Society
"A cycle: incarceration, homelessness, incarceration homelessness"
http://www.cbc.ca/1.3764586 @preventcrimenow @JohnHowardAB @YEGJohnHoward

PUBLIC SERVICE / FONCTION PUBLIQUE

Justin Ling
Hey, I'm speaking at this super cool event about Access to Information in Ottawa next week!
http://carleton.ca/sjc/event/celebrating-right-know-week/ …

INTERNATIONAL

OpenMedia
Do you think @Snowden should be granted pardon? Why or why not?

Stewart Bell
Captured. Suspect in New York and New Jersey bombings in custody after shootout with police.
http://natpo.st/2cC10Yo @nationalpost

Washington Post
Three mysterious incidents in New York, New Jersey and Minnesota raise fears of terrorism

CBC News Alerts
New York governor: Manhattan bombing may be act of terror with foreign connection. Had earlier ruled it out. Afghan-born US citizen sought.

CBC News Alerts
FBI wanted poster: New Jersey man being sought after blast in Chelsea area of New York City "should be considered armed and dangerous."

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

Today's News / Actualités
October 26, 2016 / le 26 octobre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Response to Senate's changes to Mountie union bill coming before spring: Goodale
Public Safety Minister Ralph Goodale says he is still looking through recommendations made by the Senate when it studied C-7, the RCMP unionization bill, and he expects to present the government's response to senators before the spring. ***"We've been obviously reviewing it both for its legal and its labour impacts. We're in the process now of analyzing all of the recommended clauses and Minister Brison and I will respond to the Senate report just as quickly as we can,"*** **Goodale** told

iPolitics Tuesday following an appearance at question period in the Senate. ***"This session essentially runs from now until next spring but I don't anticipate it's going to take that long."*** One of C-7's most controversial provisions is a section that includes a long list of workplace issues excluded from collective bargaining. (…) That marks a major difference between the version of the bill passed in the House of Commons and the version passed in the Senate. The government must now report back to senators on whether it will accept their changes. ***"The key question, as was focused on to a certain extent in the House but certainly in the Senate debate, is the set of issues around the prerogatives of management versus the listed exclusions and are those two compatible. We've just got to compare them all and make sure we've got it right,"*** **said Goodale.** The bill's Senate sponsor, former Mountie Larry Campbell, fought hard to remove all of the exclusions from the bill and had warned that leaving them in place could open the bill to a constitutional challenge. iPolitics

Document reveals RCMP strategy for possible 'flood of foreign fighters' fleeing Mosul offensive
Foreseeing a possible "flood of foreign fighters" out of Syria, the RCMP has circulated a strategy that involves trying to understand the returning fighters' intentions and working with communities. The plan calls for monitoring the social media activity of the "returnees," placing them on the no-fly list and asking Passport Canada to revoke their travel documents and flag their future passport applications. (…) According to figures already disclosed by the government, about 60 returnees are now back in Canada. But another 180 Canadians active in terrorism remain overseas, including about 100 in Syria and Iraq, the government has said. A victory by the regime forces in Syria could trigger an exodus of foreign fighters from the region, according to the RCMP report, which said the scenario "would pose an immediate security challenge." "It will be important to enlist the assistance of community engagement specialists as soon as possible once law enforcement becomes aware of a returnee," it said. "They may have a role to play in conducting the basic assessment of indicators noted above, and certainly would assist the returnee in engaging with supportive community resources, including those who would help steer the individual away from criminal activities associated with terrorism." Asked how the RCMP was preparing for the return of foreign fighters in light of the Mosul offensive, Staff Sgt. Julie Gagnon said the police force was "taking active measures through its criminal investigations." **Scott Bardsley, spokesman for Public Safety Minister Ralph Goodale**, said the government used a number of tools to deal with foreign fighters including revoking passports, the no-fly list and criminal charges. The report said police may act on information about returnees it receives from foreign partners but it also warned about the pitfalls. "The RCMP should be wary of utilizing information about subject X when it has been provided by a country's law enforcement forces that are known to use torture, unreasonable detention, or lack of due process." National Post

VICE Media & Civil Liberties Groups Launch Campaign to Protect Press Freedom
VICE Media Canada have joined forces with a coalition of civil liberties organizations to to launchprotectpressfreeedom.ca, a multi-platform campaign to raise awareness about VICE News Journalist and Cyberwar Host Ben Makuch's fight to protect his sources from RCMP interference. "Ben Makuch is standing up for every journalist who believes that source protection is fundamental to a free and independent press," said Ryan Archibald, President, VICE Media Canada. "We've got Ben's back and now we're asking Canadians to join us in this fight." In February of 2015 the RCMP presented VICE News reporter and Cyberwar Host Ben Makuch with a production order to turn over all communications between himself and Farah Shirdon, a source who had allegedly joined the Islamic State and who was later charged in absentia by the RCMP for having terrorism-related activity. The Ontario Superior Court upheld the production order this spring, however, VICE Media has appealed that decision and the Court of Appeal will hear the appeal in February 2017. (…) Protectpressfreedom.ca petitions Attorney General, Jody Wilson-Raybould, **Minister for Public Safety and Emergency Preparedness, Ralph Goodale** and RCMP Commissioner Robert Paulson. It asks them to drop demands for the release of Ben Makuch's private material and correspondence with sources and to amend the statutory framework governing the use of production orders to offer greater protection against a chilling effect on free expression. Broadcaster Magazine

TOP STORIES / MANCHETTES

La GRC lance un guide de prévention du terrorisme et de la radicalisation
La Gendarmerie royale du Canada (GRC) lance mercredi un guide de prévention du terrorisme et de la radicalisation menant à la violence, destiné aux parents, aux enseignants et aux proches des personnes à risque. Le guide, intitulé "Guide de sensibilisation au terrorisme et à l'extrémisme violent", vise à les aider à mieux comprendre et à reconnaître le phénomène de la radicalisation. Il énonce, entre autres choses, les signes avant-coureurs de radicalisation et ceux de la planification d'un attentat. Il discute également du rôle de l'internet et de la propagande. On peut aussi trouver dans ce guide les coordonnées de certains organismes locaux pour obtenir de l'aide ou pour signaler un comportement suspect. Le guide est gratuit et disponible en français et en anglais. Il est offert en livre électronique et est téléchargeable sur le site de la GRC. Il a été préparé par l'Équipe intégrée à la sécurité nationale et le Bureau des communications de la GRC au Québec, avec la collaboration du Comité sur la sécurité nationale et le contre-terrorisme, l'Association canadienne des chefs de police et la Structure de gestion policière contre le terrorisme au Québec (SGPCT). Presse canadienne

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

CN Rail working to reopen tracks near Yale, B.C., after derailment
Crews with CN Rail have made good progress repairing tracks following a derailment in British Columbia's Fraser Canyon. An email from CN spokesman Brent Kossey says crews worked through the night and expect to have tracks five kilometres north of Yale reopened before noon Wednesday. Two locomotives and several cars of a train carrying grain derailed late Tuesday morning, possibly after hitting rocks on the track. Kossey says the locomotives were lifted back onto the rails overnight and have been removed. He says the nine cars and their spilled contents will be removed in the days ahead. No one was hurt, and a boom was set up on the Fraser River below the derailment, but no oil or fuel spill was reported. CTV News; Radio Canada

NORAD exercise puts defence of northern airspace to the test
Defending North American airspace is the no-fail mission of the Royal Canadian Air Force (RCAF). But in recent years, fulfilling the North American Aerospace Defense Command (NORAD) mandate of aerospace warning and control and maritime warning has become a much busier task. In the past three years NORAD has seen a significant increase in the number of bombers, tankers and fighter jets near continental airspace since Russian president Vladimir Putin reinstated long-range air patrols in 2007… Last week, NORAD hosted Vigilant Shield 17, an annual exercise that has become the unified command's largest test of its ability to carry out collective defence of the two countries' airspace. The exercise, which ran from Oct. 17 to 21, blended live-flying with simulated elements in several regions throughout the United States and Canada, including the high Arctic. Although the specific exercise scenarios were kept under wraps, they reflected many of the challenges NORAD faces to detect, identify and intercept the growing range of threats… As a further test of Arctic capability, the RCAF had forward-deployed search and rescue (SAR) assets to the most remote locations over which the fighter jets were training. Although they were only serving in support of Vigilant Shield, a CH-149 Cormorant helicopter was at Canadian Forces Station Alert while a Cormorant and CC-130H Hercules SAR aircraft were at the USAF's Point Barrow Long Range Radar Site in Alaska. "The last thing we want to see is an aircraft go down, but if that happens we have dedicated SAR assets that are forward located to respond," Lavallee explained. Skies Mag

London Hosts Ontario Western Region Search and Rescue Exercise
London Search and Rescue hosted a regional SAR exercise on Saturday, October 22 at Camp Woodeden, Easter Seals Camp, in London. Volunteer search teams from London, Niagara and North Bruce were involved with the scenario, which included searching for four missing subjects. This event was funded by OSARVA obtaining a NIF grant. More than 50 participants were a part of the day, and worked together to highlight interoperability between our SAR teams, regardless of where they train in Ontario. London Free Press

Police partner with Alzheimer's society for 'vulnerable person' search exercise

On Friday, October 28, the Greater Sudbury Police Service Search and Rescue Team will be conducting their annual training scenario. This year, the Greater Sudbury Police Service is partnering with the Alzheimer Society Sudbury-Manitoulin North Bay & Districts to promote awareness of Alzheimer's disease and related dementias and conduct a search and rescue involving a vulnerable person. The training exercise will take place in an area off of Gagnon Street in Azilda, past the Montee Rouleau turn off at around 11 a.m. Sudbury.com

Hikers found swiftly by SAR
Two hikers were lost on Mount Hays Oct. 17 and the ground search and rescue team was called at 3:30 p.m. to find them. "Our subjects did exactly what they should, called for help, stayed in place and signalled our team with fire and a tarp," said the post on the Prince Rupert Ground Search and Rescue Facebook page. In record time, an hour and a half later, the two hikers were found safe and sound. Northern View

Alberta Premier Rachel Notley meeting with Fort McMurray wildfire victims
Alberta Premier Rachel Notley is visiting with people affected by the wildfire in Fort McMurray last spring. Notley is scheduled to meet with high school students and counsellors at Westwood Community High School in the early afternoon Wednesday. She'll also have coffee with first responders, tour a newly-built home, talk with owners, and have a roundtable discussion with social-sector organizations. Global News

Traffic-clogged highway during Fort McMurray wildfire spurs call for 2nd highway
Wood Buffalo is looking to Ottawa, the province and industry for help in building a second highway into and out of Fort McMurray. During the evacuation in May, tens of thousands of people jammed Highway 63, the sole road in and out of the northern Alberta city, as walls of flame showered embers and ash onto the roadway. Vehicles ran out of fuel and were abandoned after sitting in the massive traffic jam for hours... While most residents escaped south, about 25,000 people headed north, where they could be flown out or wait until the wildfire subsided. "We had 88,000-plus near misses. So we have to find out a way to do this better from a safety point of view," Coun. Sheldon Germain said. The municipality's wildfire recovery committee recommended supporting the $1.5-billion project along with a number of other strategies to make Fort McMurray less vulnerable to disasters. The municipality says it will put up $5-million towards the $15-million cost of the pre-design of the proposed East Clearwater Highway, which includes geotechnical work, development of traffic models and consultations, if the province and federal government funds the rest. The municipality said it would also seek help from industry to fund the project. CBC News

Back-to-business results expected from oilsands as wildfire impact dissipates
Oilsands producers are expected to report back-to-business third-quarter results over the next few days as they shrug off lingering impacts of last May's devastating wildfires in Fort McMurray, Alta. While provincial estimates report that Alberta oilsands production dropped by about one million barrels per day in May and by about 700,000 bpd in June, financial analysts say the industry's main players were producing normal volumes in the three-month period that followed. Canadian Press (Winnipeg Free Press)

Stormwater warning: P.E.I. municipalities eager for ideas
You can pardon the sewer and water folks with the City of Charlottetown if they took a moment to celebrate after the Thanksgiving storm. Four years and $18 million later, the Spring Park Combined Sewer and Separation Project had passed its first major test. After more than 74 millimetres of rain, there was no overflow at the city's treatment plant. But there are more storm clouds on the horizon and stormwater will continue to be an issue into the future for all Island municipalities, as climate change brings more unsettled weather patterns.Stormwater is rain or melting snow that runs off the land into waterways instead of soaking in, carrying along whatever debris lies in its path, potentially causing pollution. That's why representatives from Island municipalities, UPEI, the consulting industry, watershed groups, and the provincial government gathered Tuesday to talk about stormwater management. CBC News

BX wildfire safety promoted

Despite the devastation that recently scorched Fort McMurray, and years prior in Kelowna and Falkland, homeowners are failing to learn from the tragedies. But North Okanagan residents have a chance to learn how to snuff out fires before they start. A FireSmart community educational event gets underway at the BX Swan Lake fire hall Saturday from 9 to 11:30 a.m. A one-hour presentation, followed by question and answer session is with one of Canada's leading experts in FireSmart and wildfire risk reduction, Alan Westhaver. Vernon Morning Star

N.W.T.'s monitoring of municipal services gets poor marks in auditor's report
The N.W.T. government does not have a good handle on the state of essential services in many communities and is not doing enough to assist those falling behind, an audit has found. Though the communities provide essential services to their residents such as water, waste and fire protection, it's the territory's responsibility, through the Department of Municipal and Community Affairs, to monitor them to ensure they're meeting requirements and to provide support, such as training, when needed. Fire protection, waste management and emergency preparedness planning all got poor marks in a report by the Auditor General of Canada that was tabled at the legislative assembly Tuesday. CBC News

Saskatchewan changes law to help workers with psychological injuries
Saskatchewan workers suffering psychological injuries — such as post-traumatic stress disorder — won't have to prove that it occurred on the job. The government has changed the *Workers' Compensation* Act to include what is called a rebuttal presumption for all forms of psychological injuries. That means it's presumed the injury is work-related, unless an employer rebuts the position. Labour Minister Don Morgan says the legislation is unique in Canada because it covers other forms of psychological injury that workers could suffer as a result of being exposed to traumatic events or situations at work, not just PTSD. Canadian Press (OHS Canada)

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Thinking Through Reform: Communications Security Establishment
A blog post by Craig Forces, Professor at the University of Ottawa, states, "Green Papers, consultations, discussions, workshops, roundtables, hearings. There is a risk of overdose for a national security law and policy reform enthusiast. And an aching fear that all this is sound and fury that, in the end, will signify precisely nothing. For all the goodwill in the world, reform in this area (even more than most) is course-correcting an oil tanker. But I'm not sure that all of it has to be hard. A few thoughts on the Communications Security Establishment (CSE) and the post-Snowden concerns about oversight: The Problem. Put simply, the issue is this: CSE acquires information that enjoys constitutional protection, without going through the process (or anything approximating the process) that the constitution requires before the state acquires this information. That is, at core, the issue in the BCCLA's constitutional challenge. (In the interest of full disclosure: on behalf of BCCLA, I provided factual background information for use by the court in that proceeding)." National Security Law

NATIONAL SECURITY / SÉCURITÉ NATIONALE

NIL

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

ITAC calls on Ottawa to create a central IT authority for federal government
If Canada wants to remain competitive in the world the federal government must adapt to the digital age – including creating a digital services division, according to a report released today by the the Information Technology Association of Canada (ITAC). "On a global basis, every country in the world is talking digital strategies and innovation agendas," ITAC CEO Robert Watson said in an interview, noting that in

Canada's case any digital strategy should include creating a central IT authority, which he says would make the government and its services more secure, innovative, efficient, and accessible for citizens and businesses than today's piecemeal operations. (…) In the meantime, though running multiple systems makes realizing their dream of a centralized system difficult, ICT managers are used to running multiple systems separately, Watson admits. The consequences for ignoring ITAC's advice could be disastrous. In its report, the organization notes that Canada's aging IT systems have led to data breaches at the National Research Council and cybersecurity risks at the Canada Border Services Agency, to name two. IT World Canada

Un couple mexicain vivant à Toronto avec ses 3 enfants est menacé d'expulsion
L'immigration illégale de Mexicains n'est pas un enjeu seulement aux États-Unis. Un couple mexicain, qui vit illégalement à Toronto depuis 11 ans, en est un exemple. Nora Trueba et Israel Ochoa ont décidé en 2005 de rester au Canada après leur voyage de noces, alors que des manifestations violentes faisaient rage au Mexique. (…)Selon un rapport publié en 2009 par l'Agence des services frontaliers du Canada, l'agence fédérale avait expulsé 4623 Mexicains cette année-là. Ce chiffre ne tient pas compte des enfants de ces couples nés au Canada, qui peuvent rester au pays, sous la garde d'un proche ou de la Société d'aide à l'enfance. Toutefois, dans la presque totalité des cas, les parents expulsés amènent leurs enfants avec eux. Radio-Canada

Bangladesh asks Canada for effective mechanism to deport Bangabandhu killer Noor
Bangladesh has urged Canada to devise an 'effective mechanism' to move forward with the deportation of the killer of its independence architect. Foreign Minister Abul Hassan Mahmood Ali made the proposal at a bilateral meeting with his Canadian counterpart Stephane Dion at Ottawa on Tuesday, his ministry said. They discussed the possible deportation of Noor Chowdhury, the self-confessed and convicted killer of Bangabandhu Sheikh Mujibur Rahman and his family memberse in 1975. Noor is evading the gallows by living in Canada since 1996. BD News 24

Smuggling posh groceries across the border
The US grocery chain Trader Joe's isn't in Canada. But one man has made a business of smuggling their snacks across the border. BBC News

Quebecers accused of drug trafficking in Australia to remain jailed
The two Quebec women who were arrested on a cruise ship in Australia on suspicion of trafficking cocaine appeared in criminal court Wednesday, but have not registered a plea. Melina Roberge, 23, and Isabelle Lagacé, 28, were denied bail pending further proceedings, scheduled for Dec. 7. The next step is for them to inform the court of their plea, said an Australian Justice Ministry spokesperson. André Tamine, 64, was arrested with them on the same luxury ship, the MS Sea Princess, and faces similar charges. The three were arrested Aug. 29 after Australian authorities with the help of a drug-sniffing dog discovered 95 kilos of cocaine in their luggage, worth an estimated $30.5 million Canadian, police said. The three cases of importing a controlled substance with the intention to traffick might be tried separately. Postmedia News (Montreal Gazette); Canadian Press (570 News); The Chronicle Herald; Daily Star

Canada-EU trade deal compromise in works amid 11th-hour talks in Belgium
A planned EU-Canada summit to sign a free trade deal was still possible on Thursday, European Council President Donald Tusk said on Wednesday, as Belgian politicians entered a second day of talks on the future of the pact. Prime Minister Charles Michel hosted talks from early on Tuesday of regional authorities, including of Wallonia and Brussels that have rejected an accord backed by all 27 other EU governments. The talks paused after two hours to allow some of those present to attend a funeral of a Belgian politician. They were scheduled to resume at 9 a.m. ET/3 p.m. CET. Without assent from its regions and linguistic communities, Belgium cannot sign the Comprehensive Economic and Trade Agreement (CETA) at a planned EU-Canada summit on Thursday with Prime Minister Justin Trudeau. "I still hope that Belgium will prove that it is a consensus-building champion and that we will be able to finalize this agreement soon," Tusk told a session of the European Parliament. CBC News; Associated Press (Toronto Star); Reuters; L'Economiste

Canada parliament votes to take in Yazidi refugees
Iraqi activist Nadia Murad was on hand for the unanimous vote in the House of Commons. The government said it is still sorting out a plan for the airlift and does not yet know how many Yazidi refugees Canada will take in over the 120-day period. But Immigration Minister John McCallum reminded that Canada had managed to resettle more than 25,000 Syrian refugees in just a few months at the start of the year. "It is important to emphasize that Canada will always be an open country willing to step up and support people in need from all around the world," Prime Minister Justin Trudeau said in the Commons. "I am pleased to see Nadia (Murad) again today and reassure her that in the coming months we are committed to bringing in vulnerable Yazidi refugees," he said. Your Middle East

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Dyn DDoS Work of Script Kiddies, Not Politically Motivated Hackers
New research on the source of Friday's DDoS attack against DNS provider Dyn indicates that script kiddies are likely responsible, rather than a politically motivated actor. Researchers at Flashpoint dismissed numerous claims of responsibility that separately linked the attack to the Russian government, WikiLeaks or the New World Hackers group. Instead, the threat intelligence company said with "moderate confidence" that the attacks are linked to the Hackforums community. Hackforums is an English-speaking hacking forum and the place where the source code for the Mirai malware was publicly released by a hacker known as Anna-Senpai. Director of National Intelligence James Clapper said today as well that it's likely the attack was not carried out by nation-state actors during testimony at the Council on Foreign Relations. Threat Post; Security Week; Associated Press (Cape Breton Post, Washington Post)

Terabit-scale DDoS events are on the horizon
Corero Network Security has disclosed a new DDoS attack vector observed for the first time against its customers last week. The technique is an amplification attack, which utilizes the Lightweight Directory Access Protocol (LDAP): one of the most widely used protocols for accessing username and password information in databases like Active Directory, which is integrated in most online servers. While experts have so far only observed a handful of short but extremely powerful attacks originating from this vector, the technique has potential to inflict significant damage by leveraging an amplification factor seen at a peak of as much as 55x. Therefore, in terms of its potential scale, if combined with the IoT botnet that was utilized in the recent attack against Brian Krebs, we could soon see new records broken in the DDoS attack landscape, with potential to reach tens of Terabits per second in size in the not too distant future. Help Net Security; International Business Times

Emails containing malware spikes 35% worldwide
DDoS-sourced malware is on the rise, according to AppRiver's Q3 Global Security Report, which analysed malware and spam trends in Q3 2016 (between July and September 2016). For the first time, the web saw disruptions caused by DDoS attacks leveraged by botnets comprised primarily of IoT devices during Q3 of this year. The company's security analyst team quarantined 5.7 billion emails containing malware in Q3, a 35 percent increase over the total they recorded in Q2 2016. This quarterly total is more than triple 1.7 billion emails containing malware that analysts observed during the entirety of 2015. Over two billion spam messages were quarantined as well. Data breaches remained a major concern for organisations worldwide during Q3. The recent breach disclosed by Yahoo and Pippa Middleton's iCloud account hack containing private pictures of her and the UK Royal family just name a few of the noteworthy breaches that occurred during this time period... Various versions of ransomware with specific targets were seen during Q3. Locky and Zepto are still some of the reigning champs when it comes to volume, but others such as EduCrypt, IoT Ransomware and MarsJoke were seen lurking online. SC Magazine

IoT Devices Can Be Hacked in as Little as Three Minutes
With 6.4 billion IoT devices already online, researchers estimate that over 20 billion IoT devices will be connected to the Internet by 2020. That's why many security experts argue that now is the time to make sure that IoT security is taken seriously before it will be too late. Of course, there are those that who think it's already too late, citing the massive DDoS attacks that have pummeled OVH, KrebsOnSecurity, and

most recently Dyn, all carried out with a botnet of unsecured IoT devices. But let's not carried away by the recent media hype. Hijacking IoT equipment for DDoS attacks is only one of the many ways attackers can use IoT devices against a target. As leading IoT security firm ForeScout explains, attackers can also use IoT equipment as pivot points in corporate networks, using them as entry points to breach sensitive servers and steal data undetected. Employing the service of renowned hacker Samy Kamkar, ForeScout says that it generally takes an intruder under three minutes to hack an IoT device. Softpedia; ZDNet; Infosecurity Magazine

WhatsApp Executives Say They're Committed to User Privacy
One of the reasons why WhatsApp is such a popular messaging application is the fact that it uses end-to-end encryption of messages. But in August this year, WhatsApp announced that it would make the first change to its terms and privacy policy in four years, in order to share user phone numbers with Facebook. The measure displeased many and got some users worried about how WhatsApp was handling the privacy of their personal data. WhatsApp did explain that the measure won't affect the privacy of content that users share, since end-to-end encryption is still available inside the application and not even WhatsApp can see messages that users share. Still, the measure displeased some government officials. In September, the Hamburg Commissioner for Data Protection and Freedom of Information ordered Facebook to delete German user data shared from WhatsApp. Softpedia

Roundtable: Former Deputy Director of NSA Talks Insider Threats
When you picture the typical venue for a cybersecurity discussion, the British Museum probably isn't the first place that would spring to mind. However, yesterday, it played host to a press roundtable with Chris Inglis, former deputy director of the National Security Agency (NSA), and other representatives of security intelligence platform provider Securonix to explore the ever-evolving landscape of the insider threat. Infosecurity Magazine

LAW ENFORCEMENT / APPLICATION DE LA LOI

La GRC lance un guide de prévention du terrorisme et de la radicalisation
La Gendarmerie royale du Canada (GRC) lance mercredi un guide de prévention du terrorisme et de la radicalisation menant à la violence, destiné aux parents, aux enseignants et aux proches des personnes à risque. Le guide, intitulé "Guide de sensibilisation au terrorisme et à l'extrémisme violent", vise à les aider à mieux comprendre et à reconnaître le phénomène de la radicalisation. Il énonce, entre autres choses, les signes avant-coureurs de radicalisation et ceux de la planification d'un attentat. Il discute également du rôle de l'internet et de la propagande. On peut aussi trouver dans ce guide les coordonnées de certains organismes locaux pour obtenir de l'aide ou pour signaler un comportement suspect. Le guide est gratuit et disponible en français et en anglais. Il est offert en livre électronique et est téléchargeable sur le site de la GRC. Il a été préparé par l'Équipe intégrée à la sécurité nationale et le Bureau des communications de la GRC au Québec, avec la collaboration du Comité sur la sécurité nationale et le contre-terrorisme, l'Association canadienne des chefs de police et la Structure de gestion policière contre le terrorisme au Québec (SGPCT). Presse canadienne

Does the Surrey RCMP need a surveillance camera database?
Surrey will soon launch Project Iris, which is based on a CCTV program out of Philadelphia. Sometime between April and July, Surrey's director of Public Safety Strategies was spending another evening listening to people. Terry Waterhouse was at a community forum collecting ideas for his comprehensive safety strategy when a business owner started to speak. After a couple of sentences, Waterhouse knew the man was on to something. "There had been an accident and someone was injured in front of his business," Waterhouse said. "His security cameras caught it, but he didn't realize until later that his footage could be used as evidence for a hit-and-run accident." The man told Waterhouse the RCMP should have a database that pinpoints where security cameras are located in the city. That way, police know exactly where to find video footage when a crime is committed. Borrowed idea: Waterhouse started researching surveillance camera databases and came across the SafeCam program in Philadelphia. For the last four years, residents and business owners have been able to register their cameras with the Philadelphia Police Department. Investigators say SafeCam has helped them solve everything from

break-and-enter cases to child abductions. One of the program's biggest successes came in November, 2014 when a woman was randomly snatched off the street. A few days after police released SafeCam footage of the incident, a 37-year-old man was arrested in Maryland. He is now serving a 35-year prison sentence. CBC News

Après les femmes, les hommes demandent des comptes à la GRC
La Gendarmerie royale du Canada (GRC) sera visée par une nouvelle demande de recours collectif d'employés alléguant avoir été victimes d'intimidation et de harcèlement, révèle CBC. Cette fois, les plaignants seront des hommes. Plus tôt ce mois-ci, la police fédérale a annoncé avoir constitué une réserve de 100 millions de dollars pour dédommager des employées disant avoir été victimes de discrimination et de harcèlement sexuels. Elle s'attend à ce qu'un millier de femmes se partagent la somme. C'est une firme d'avocats impliquée dans ce dernier dossier, Kim Orr Barristers, qui a confirmé à CBC qu'un nouveau recours collectif regroupant des hommes se préparait. Selon Me Megan McPhee, ce dossier est en préparation depuis des années. « Nous avons parlé à des centaines de membres, et nous sommes contactés par de nouveaux membres chaque jour », affirme-t-il. Si la demande de recours collectif est acceptée et qu'un tribunal donne raison aux plaignants, la facture pourrait s'avérer particulièrement salée pour la GRC, dans la mesure où les hommes comptent pour environ 80 % de son effectif. Radio-Canada

Death of Burnaby man Tasered by police deemed accidental
50-year-old Maurizio Facchin died after being tasered by Burnaby RCMP in 2014. A coroner's inquest has ruled the death of a 50-year-old Burnaby man, who passed away shortly after police Tasered him, was accidental. It was more than two years ago when Burnaby RCMP deployed a conducted electrical weapon (CEW) on Maurizio Facchin before he died. At a coroner's inquest last week, a jury heard from more than 20 witnesses about the incident at a Burnaby apartment, which many of them called a "chaotic" scene. People who took to the stand included building residents, police officers, firefighters and paramedics. Inquest counsel Bryant Mackey says witnesses recalled a drug-induced Facchin rampaging out of control before police shot him with a Taser. "The immediate cause of death was found to be excited delirium due to a result of cocaine toxicity and cardiomegaly," said Mackey. "That essentially means Mr. Facchin had an enlarged heart," said Mackey. "[The jury] heard from the medical practitioners that suffering from an enlarged heart does make someone susceptible to cardiac arrest at a level greater than those in the population that don't suffer from cardiomegaly." The jury made three recommendations to RCMP as a result of the incident. CBC News

Separate drug busts yield big fentanyl haul for southern Alberta police
Hundreds of fentanyl pills have been seized and five people, including an alleged gang member, are facing charges after separate drug busts in southern Alberta. The Alberta Law Enforcement Response Team says a total of 777 pills were found over the past two weeks as part of an effort to limit the supply of fentanyl hitting the streets of Lethbridge. Investigators say that on Oct. 13, team members seized 193 pills, cocaine and a loaded handgun from two homes and two vehicles in the city. Alleged Mad Cowz gang member Corey Amyotte, who is 29, and associates Ali Zalfo and Jerry Bull were arrested on 32 charges relating to drugs and firearms offences. The following Thursday, officers seized 584 fentanyl pills and arrested two suspects during a vehicle stop in Aldersyde, about 40 kilometres south of Calgary. William Hatch, who is 33, and Awet Abraha, who is 28, were arrested and charged with six drug-related offences. ALERT includes members of law enforcement agencies across Alberta, including the RCMP, the Calgary, Edmonton, Lethbridge and Medicine Hat police services and Alberta Sheriffs. Calgary Herald

Ponoka RCMP search for missing 13-year-old boy
RCMP in Ponoka, Alta., are looking to the public for help finding a missing teen.Dolton Anderson was last seen at a group home in the central Alberta town on Saturday, Oct. 22 at around 12:30 p.m.He is described as 5'4" tall and 90 lbs. with short brown hair, glasses.RCMP said Anderson has a foot scooter with an orange emblem on it.Anyone with information is asked to call Ponoka RCMP at 403-783-4472 or contact Crime Stoppers. Sugar Daily

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Attendance management: Good intentions, discriminatory effects
Attendance managemenet programs are popular among employers for keeping an eye on employee absences and ensuring both good productivity levels and that employees who need accommodation are getting it — particularly for employers where employee absenteeism is a problem. However, such programs can walk a fine line where certain employee absences are related to grounds protected under human rights legislation. If such absences play a role in getting an employee entered into an attendance management program where she receives differential treatement, then it might be discrimination — whether the employer intended it or not. A federal employer's attendance management program discriminated against employees' family status and disabilities by including leaves for those reasons in the threshold for entering them in the program, the Canada Public Service Labour Relations and Employment Board has ruled. Corrections Canada (CSC) implemented a national attendance management policy (NAMP) for employees of its correctional institutions in October 2011. The policy was designed to ensure effective communications between employees and management about absences so CSC could accommodate any needs that contributed to the absences. It was meant to help employees improve their attendance rather than penalize them for absences. Managers were instructed to discuss absences with employees but not to seek medical diagnoses. Canadian Employment Law Today

Developing Assessment and Treatment Practices for Female Sexual Offenders
This impact case study is based on a body of research that has enhanced the assessment and treatment of female sexual offenders internationally. This clinical impact was underpinned by a series of unique qualitative and quantitative studies that led to the discovery of female sexual offenders' offence styles and cognitive characteristics. The work has resulted in the development of effective clinical practice training and guidelines. It has been used by professionals to enhance their assessment and treatment of female sexual offenders whose specific needs had not previously been identified. As noted by the Director General of Women Offender Sector, Correctional Service Canada: Prior to the research by Gannon and colleagues, virtually no studies focused on females in particular and many program or study descriptions even fail to indicate the gender of the participant or the subject group; the assumption of the offender as male is implicit. This research has swiftly led to impact on the assessment and treatment of offenders in the UK and internationally. Since 2010, a number of practitioner organisations worldwide (including both correctional and non-government organisations) have used Professor Gannon's research findings to inform their training, assessment and treatment practices. For example, the Correctional Service of Canada – one of the few worldwide correctional facilities to provide group female sexual offender treatment – now incorporate Gannon and colleagues' (2010, 2012) pathways into their training materials for all new facilitators who work with female sexual offenders. British Psychological Society (2016-09-26)

Broadcast Media / Médias télédiffusés:

CTV News conducted an interview regarding Emma's Acres, a farm where victims and offenders work together. Rough Transcript

Should Oland get a new trial? We have no idea
An opinion piece states, "Dennis Oland was convicted of murder by 12 ordinary folks applying ordinary judgment to the evidence they heard. That conviction was then set aside by three legal Olympians on the New Brunswick Court of Appeal, working with reams of esoteric hair-splitting argument delivered by a phalanx of clever lawyers. That, in a nutshell, introduces the central dilemma of decision-making in our criminal courts: Do we follow the dictates of common sense or complex doctrine? The truth is, nobody knows." Globe and Mail

52 months of torture and the 4 men responsible
An opinion piece states, "There is a man in Thunder Bay who the Province of Ontario has kept in a hole for 52 months. His name is Adam Capay. When he was 19 he was arrested on minor charges and sent to jail. There he got into a fight and another man died. We don't know if Capay is guilty—he has been waiting an incredible four years for his trial. And while he has been waiting, he has been kept in solitary confinement, in a Plexiglas box, in an empty cellblock with no windows, and with the lights kept on for 24

hours. Capay has interacted with so few people over the last four years he is losing the ability to speak. One thousand five hundred and sixty days in solitary confinement. To put this in perspective, consider that the United Nations has declared this form of segregation should never surpass 15 days. They did this because it is considered one of the worst forms of psychological torture. How bad is it? In the 1950s, a well-regarded psychologist named Harry Harlow decided to find out. He placed rhesus macaque monkeys in solitary confinement for twenty days and recorded the effects. Every monkey emerged badly damaged. Harlow was universally condemned for his cruel and unethical experiment, and his reputation was permanently ruined. And yet, the province of Ontario has effectively conducted this experiment on Adam Capay 78 times in a row." Maclean's

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NIL

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

NIL

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

5 Major Issues That Will Affect Cannabis in Coming Years
An opinion piece states, "For marijuana smokers, politics is often viewed as a cut-and-dried proposition. "Legalize it" has long been the one and only rally cry. As some states have legalized it, and others are close behind, it is time to start broadening cannabis political horizons. Now that the path to legalization seems inevitable, it's time to consider more complex political questions. What should the next priorities be for smokers in the coming years? Here are some issues that could make a big difference for America's cannabis community. Trade: One of the most complicated political issues has come to the forefront of this election season: trade. As legalization moves forward in the U.S., countries like Mexico have entered into a bit of a trade arms race to legalize their product, hoping to funnel money from the cartels to the Mexican government. At the same time, less traditional drug importers, like Canada, are exploring revenue possibilities as well." Merry Jane

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

NIL

INTERNATIONAL

Brothers From Michigan Arrested in Tunisia in Terrorism Probe
Two American brothers have been arrested in Tunisia on suspicion of belonging to a terrorist organization, two local sources told NBC News. A senior police official said the brothers were both aged in their 30s and originally from Michigan. A source in the governor's office also confirmed the arrests.

Speaking on condition of anonymity, the police source said one of the men was carrying a U.S. passport that identified him as Patrick Alan Lawwill. NBC News has seen a photocopy of the passport, which was apparently issued in July 2015 and lists Lawwill's place of birth as Michigan. Police were not able to provide a copy of the second suspect's documents. A State Department official said it was aware of reports the pair had been arrested "on suspicion of terrorist activities" but declined to comment further because of "privacy considerations." NBC News

Airstrikes in Syria kill 17 people - most of them children - after warplanes hit school
Airstrikes in Syria killed 17 people, mostly children on Wednesday when warplanes struck a school complex in the northern rebel-held province of Idlib, activists said. The Idlib News network said the strikes hit as the children were gathered outside the school complex in the village of Hass. The activist-operated group put the death toll at 17, and said most of the victims were children. There were fears the death toll could rise further as some of the wounded were reported to be in critical condition, the network added. Another activist group, the Britain-based Syrian Observatory for Human Rights put the death toll at 22. It said 14 children and a woman were among those killed. Associated Press (National Post); Radio-Canada International

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

senatcarignan
#RCMP should have the ability to negotiate basic issues. My question to @RalphGoodale on bill C-7 http://bit.ly/2eLljSi #SenQP

amandacconn
Response to Senate's changes to Mountie union bill coming before spring: Goodale #C7 #RCMP #Cdnpoli #senca https://t.co/SXgJjtaM5K

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

GgNewsCA
Green Shield sets up fund for families affected by Windsor flood https://t.co/wn3qyCLVrF

wildlandfirecan
John Maclean keynote http://fb.me/2WkiuaN5Z

EnviroWonk
#WFC2016 John Maclean speaking this morning about common elements of multiple fatality #wildfires.

Resiliency_CBoC
The common elements of mass fatality fires from John Maclean #WFC2016 @wildlandfirecan #smem #resilience #wildfire

Resiliency_CBoC
Great point from John Maclean - do not underestimate the depth of knowledge indigenous #firefighters have #WFC2016 @wildlandfirecan #smem

davidakin
#SenCA #POFO meets now in Halifax. Maritime search and rescue. Link to details. http://bit.ly/1RNgTKi #cdnpoli

VancouverSun
CN Rail working to reopen tracks near Yale after derailment - YALE — Crews with CN Rail have made good progress... https://t.co/XUlEdxLabg

NATIONAL SECURITY / SÉCURITÉ NATIONALE

StewartBellNP
Are "returnees" who've trained/fought in Syria & Iraq a threat? The RCMP's list of basic indicators. http://natpo.st/2eQRQFX @nationalpost

borealissaves
OK, I have read the McGill survey - not impressed. Attitudes to violence are not acts of violence http://www.sherpa-recherche.com/wp-content/uploads/2016/10/Rapport-de-recherche-CEGEP-FINAL-24.10.2016.pdf …

nataliealcoba
Heads up: civil liberties + media orgs in TO court tmw seeking intervenor status in RCMP v @BMakuch and his notes

cforcese
Thinking Through Reform: Communications Security Establishment (@cse_cst) oversight http://craigforcese.squarespace.com/national-security-law-blog/2016/10/26/thinking-through-reform-communications-security-establishmen.html/ … #intelligence #natsec

Justin_Ling
uh. https://www.cse-cst.gc.ca/en/announcement-annonce/we-are-cyber-security …

CYBER SECURITY / CYBERSÉCURITÉ

StephanieCarvin
Sloly speaking to how cyber is being used to coordinate responses of social services. Share info between policing/health services #srcyber

StephanieCarvin
Peter Sloly from Deloitte's "security and justice" program law enforcement can't just defence, it also must be able to attack #srcyber

StephanieCarvin
Allen Dillon from CyberNB (New Brunswick) speaking on NB's approach. Raises concern re: cyber-vigilantism b/c lack of gvt strategy #srcyber

LAW ENFORCEMENT / APPLICATION DE LA LOI

chrishallcbc
Male RCMP employees prepare for class-action harassment suit against the force https://t.co/YPDQTntS4a

arielleps
Document reveals RCMP strategy for possible 'flood of foreign fighters' fleeing Mosul offensive https://t.co/LmX3SMH4Cf

cbcnewsbc
Death of Burnaby man Tasered by police deemed accidental http://ift.tt/2eFAXl9

TheTorontoSun
Leduc RCMP catch escaped Ontario prisoner http://ow.ly/haVl305yabO

GgNewsCA
Hundreds of fentanyl pills seized in Lethbridge - Globalnews.ca https://t.co/N61KZo0zG2

CBCIndigenous
RCMP search warrant application shows early findings and theory in Colten Boushie shooting http://ift.tt/2e8pcQA

ozhibiige
#RCMP seek public's help to find missing #Yellowknife man http://www.cbc.ca/news/canada/north/wilbert-andre-missing-yellowknife-1.3820831 … #MMIM #WilbertAndre @CBCIndigenous

LP_LaPresse
Meurtre de huit aînés: l'infirmière avait écrit un poème sordide https://t.co/x7kHlbSls0

borealissaves
Why we are so bad at identifying mass killers before they strike https://t.co/QljuL6rwcJ

I_Journalism
Lawyer for Colten Boushie's family says RCMP need to say what happened to car | by @Tamara_APTN https://t.co/gewkGiBxkJ

cbcnewsbc
Does the Surrey RCMP need a surveillance camera database? http://ift.tt/2eG77tU

calgarysun
Former RCMP officer behind class-action lawsuit says concerns in Calgary report are 'tip of the iceberg'. http://ow.ly/pm74305xsSS

MichelleZilio
OPP unveils new text message technology today. Texts will be sent to people who were in identified area on day Hatch went missing #ottnews

alexboutilier
Whhaaa? How did the OPP get that info?

Colinfreeze
@alexboutilier Tower dump by court order?

Justin_Ling
@alexboutilier Tower dumps, bro.

Colinfreeze
Reading @MichelleZilio's the OPP will blitz cells with SMSes for leads, as feds drag feet on doing same to warn https://t.co/TfP2MG4w3q

alexboutilier
@Justin_Ling @Colinfreeze But didn't the Ontario court rule in January that tower dumps violate the Charter?

GgNewsCA
'Go home,' indigenous leader tells protesters after Muskrat Falls meeting https://t.co/YpuD35Oob1

JacobBarkerCBC
Protesters said to be coming out by bus #cbcnl #MuskratFalls

JacobBarkerCBC
Roy Blake just announced the bus will be coming out and there will be no arrests made #muskratfalls #cbcnl

JacobBarkerCBC
Crowd chanted David Nuke's name after protesters came out, says this is just the beginning #cbcnl #muskratfalls

RadioCanadaInfo
Muskrat Falls : des manifestants sceptiques restent sur le site http://rc.ca/MXFT7b

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

rp_browne
There are currently six babies living in federal women's prisons across Canada: https://t.co/wXhttAVP4h

CBCIndigenous
First Nations man spends 4 years in solitary confinement in northern Ontario awaiting trial http://ift.tt/2dVBjmL

AngelaSterritt
Ontario minister refuses to release Indigenous man from solitary who's spent four years in isolation. #canada https://t.co/gVRMiK5773

DesmondCole
Free Adam Capay NOW. @DavidOrazietti https://t.co/Vlqyhv6sZS

citizenduffy
The gunman in one of Ottawa's most shocking murder cases has been released on parole after a troubled prison life. https://t.co/VLTVZIYBXm

CBCTBay
More calls to end solitary confinement in Ontario as details of Adam Capay's 4 yrs in segregation in #tbay emerge http://www.cbc.ca/news/canada/thunder-bay/four-years-solitary-1.3821245 …

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

GgNewsCA
Manitoba college of pharmacists nixes fentanyl tests for drug users https://t.co/IfUOVZVOZJ

AngelaDingwell
@WGHillElem learns WITS w/ RCMP & local football members! Creating responsive communities to prevent peer victimization #wits #goodbehavior

MissionRCMP
@Mission_BC #RCMP volunteers & @icbc handing out pedestrian safety reflectors at the West Coast Express. RCMP also gave 15 speeding tickets

globalnews
ICYMI: Woodstock nurse charged with murder of 8 elderly patients renews focus on violence against seniors https://t.co/Vvb7JK2TFJ

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | ENQUETE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

AngelaSterritt
This is such an important doc series that tries to solve #MMIW cases. Please Watch. Taken | APTN http://aptn.ca/taken/

rachelagiese
Must listen: @connie_walker is one of the best journalists in the country and her new podcast about Alberta Williams and #MMIW is excellent https://twitter.com/Chatelaine/status/791025792763490306

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

vicecanada
How many optimum points do you think you could get for a gram? https://t.co/icH4DQ2f1o

OTHER / AUTRE

globalnews
Aboriginal, environmental groups to launch lawsuit against Ottawa over Pacific NorthWest LNG project http://glbn.ca/Zvw00U

CBCNunavut
Breaking the fast: Smoked char first food for hunger strikers protesting Muskrat Falls http://www.cbc.ca/1.3821743

operationsFC

Le #NCSMEdmonton et le #NCSMBrandon participent aux efforts internationaux de lutte contre la contrebande dans l'Est du Pacifique #OpCARIBBE

GgNewsCA
Mental health advocate aims to show 'collateral damage' caused by suicide https://t.co/7y5A3m7uC5

Reuters
Russia is beefing up its Baltic Fleet to counter NATO's build-up, according to reports: http://reut.rs/2evAMIN

INTERNATIONAL

NBCNewsWorld
American brothers arrested in Tunisia on 'suspicion of terrorism activities' https://t.co/kescznP5ta

abcnews
#Pakistan militants worked with Islamic State to attack police academy killing at least 59, spokesman says https://t.co/TjkqEqSUFX

BBCWorld
Millions of modified mosquitoes to be released in Brazil & Colombia #Zika fight http://bbc.in/2dK40Q3

globeandmail
French authorities declare the Calais migrant camp empty http://trib.al/8tstfaf

AJEnglish
Why ISIL won't be defeated on the battlefield in #Mosul http://aje.io/r89s by @thewarjournal

AFP
Mediterranean migrant deaths in 2016 hit record 3,800: UN https://t.co/zJ6RPd8rwM

cnni
A haul of cocaine worth more than $5m has been found on a beach in Ireland http://cnn.it/2eLXoDl

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

Today's News / Actualités
November 1, 2016 / le 1 novembre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

TOP STORIES / MANCHETTES

NIL

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Seismic rift divides B.C. governments
The provincial government has taken steps to prepare for a major B.C. earthquake, investing millions of dollars in an early warning system and spending billions to seismically retrofit schools and important infrastructure such as bridges. The province recently held an emergency exercise on Vancouver Island to test its response to an earthquake. But it has shown little interest in dealing with thousands of privately owned buildings in the province that were constructed largely before the early 1970s and do not meet modern earthquake safety standards. That job has been left to municipalities, which have relied on passive triggers that only come into effect when building owners change an old building's use or undertake major renovations. Each level of government appears reluctant to tackle the issue head on, instead looking to another level of government to take the lead. Vancouver Province

Worst hit in Sydney flood seek details on compensation
The newly formed Southend Lost Homes Coalition of Sydney wants clarity surrounding compensation for inhabitable homes and is urging a speedier recovery process after members lost everything in the flood on Thanksgiving Day. The 17 homeowners in the group have agreed to allow their houses to be demolished and the entire area declared a no-development zone by the municipality. That agreement, however, came with the understanding that they would be supported in finding or building new homes, but spokesman Terry Drohan said that support has been slow in coming. CBC News

Province middle of the pack for flood preparedness
A new report from the University of Waterloo puts New Brunswick in the middle of the pack for flood preparedness, but the Conservation Council says that doesn't paint a full picture. Louise Comeau, the director of climate change and energy solutions for the Conservation Council of New Brunswick, said while the province received a C plus grade, there's still more work to be done. "We need to move from a reactive point of view, or frame of reference, to proactive, long-term planning and prevention approach to these issues," said Comeau. CBC News

P.E.I. ranks at the bottom for flood preparedness
P.E.I. has a lot of work to do prepare for floods, according to a new report out of the University of Waterloo. P.E.I. scored a D overall in the report, tied with British Columbia for the lowest grade in the country. Overall, Canada scored a C. The Island reached the national average in only two of 12 categories — wastewater systems and drainage system maintenance — and did not exceed the average in any. P.E.I.'s electricity supply and transportation systems were found to be particularly vulnerable, and the province was found to be behind on adaptation audits of both commercial and residential properties. CBC News

A Diesel Spill Is Putting the World's Largest Temperate Rainforest at Risk
In the early hours of Oct. 13, a petroleum tug-barge tanker called the Nathan E. Stewart ran aground near Waglisla (Bella Bella) on the central coast of British Columbia, crashing into one of the richest ecological and cultural treasures in Wax'wuisaxv-s Haiłzakv (Territory of the Heiltsuk First Nation). Almost three weeks later, the sunken tug is still there, still intermittently leaking diesel, and clean-up efforts have barely begun. As someone who works and lives in Bella Bella, and who has spent time as an observer for the Heiltsuk Nation in the aftermath of the crash, what I've been seeing firsthand has left me concerned (…)The risks of marine transport, especially of oil, have been a concern here for years. With eerie timing, a film recently created by students at the Bella Bella Community School summarizing these concerns was released just four days before the Nathan E. Stewart drove into a reef on a calm clear night, in a channel three kilometers wide (…) But the main thing I've seen first-hand is disarray, and the near impossibility of containment, recovery, and cleanup of petroleum once it enters this marine environment. This despite the impressive professionalism of Canada's Coast Guard on the scene, the hordes of experts brought in from around the world, and of course the tireless dedication of members of the Heiltsuk Nation who have dropped everything to devote themselves to the response. Motherboard (2016-10-31)

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Whistleblower Edward Snowden speaks at McGill University Wednesday
The timing couldn't be better. With many Quebecers in an uproar over police spying on La Presse reporter Patrick Lagacé, McGill University on Wednesday will welcome whistleblower Edward Snowden, who is wanted in the United States for giving classified material on U.S. surveillance programs to journalists. Speaking via video link, Snowden, a former government contractor at the U.S. National Security Agency, will discuss surveillance in Canada. The free public lecture is being organized by Media@McGill, an interdisciplinary hub focused on the study of contemporary media. It will take place on Wednesday, Nov. 2, at 7 p.m. in the Leacock Building, 855 Sherbrooke St. W. Seats will be first come, first served, with a lineup starting at 5:30 p.m. Snowden's leaks revealed how the U.S. and other countries monitor global private communications. He is now living in exile in Russia to avoid prosecution in the U.S. Last month, Snowden criticized Prime Minister Justin Trudeau for not repealing Canada's anti-terror law. On Monday, Snowden tweeted about the Lagacé surveillance, quoting a Montreal Gazette story and warning journalists that police are spying on them to identify sources. Montreal Gazette

Montreal police monitored iPhone of La Presse journalist Patrick Lagacé
Montreal police strongly defended a highly controversial decision to spy on a La Presse columnist by tracking his cellphone calls and texts and monitoring his whereabouts as part of a necessary internal police investigation — while the journalist involved called what they did "indefensible." "Lives were not at stake, this was not a question of national security," La Presse columnist Patrick Lagacé said in an interview Monday. "The leaks made them look bad, that's why they decided to go after me in the way they did." Opposition politicians are also condemning Montreal police for spying on Lagacé, though Montreal Mayor Denis Coderre stood by police chief Philippe Pichet on Monday, noting that a mayor should not intervene in police operations, but did say he was troubled by the news. For several months this year, police were monitoring Lagacé's iPhone to determine the identity of his sources, La Presse reported. This was confirmed to Lagacé last Thursday by Montreal police. Montreal Gazette; Radio-Canada

L'ex-chef du SPVM Marc Parent n'a jamais autorisé la surveillance de journalistes
Marc Parent soutient n'avoir jamais autorisé la surveillance électronique d'un journaliste lors de son passage à la tête du SPVM de 2010 à 2015. Il n'a pas davantage été mis au courant de l'existence d'une telle pratique sous sa gouverne. La Presse a croisé M. Parent en marge d'une annonce du premier ministre Philippe Couillard à l'occasion de conférence de l'UNESCO sur la radicalisation des jeunes, mardi. Il n'a pas voulu commenter directement l'espionnage du journaliste Patrick Lagacé par le SPVM, dirigé aujourd'hui par Philippe Pichet. Il a toutefois accepté de répondre à quelques questions sur les pratiques qui ont eu cours sous sa direction. A-t-il déjà été mis au courant d'un mandat de surveillance contre un journaliste ou en avoir autorisé un ? « Non », a-t-il répondu. « Je n'ai pas autorisé de mandat d'écoute électronique sur un journaliste. » Il a offert la même réponse lorsqu'on a abordé la question d'un mandat de surveillance électronique, sans qu'il y ait écoute à proprement parler. Il a précisé que l'écoute et la surveillance électroniques sont « englobées » dans un même moyen d'enquête. La Presse

Défier la «propagande jihadiste» sur internet pourrait être vain
Répondre à la «propagande jihadiste» en ligne en présentant un contre argumentaire officiel ou en désactivant des comptes jugés extrémistes pourrait avoir un effet limité et occulter la lutte contre les éléments à la base de ce radicalisme, selon des experts. À mesure que le groupe État islamique (EI) a étendu son emprise sur l'Irak et la Syrie, sa communication moderne sur internet est apparue comme une arme redoutable qui avait été minimisée par les États ciblés par ses attaques. Des vidéos d'exécutions aux films promotionnels semblant sortis d'Hollywood, en passant par des facilités d'accès à des recruteurs via les réseaux sociaux, l'organisation radicale a étendu le champ de bataille sur le web,

comme aucun autre groupe armé auparavant, ont convenu les participants à la conférence «Internet et la radicalisation des jeunes», organisée lundi et mardi par l'UNESCO à Québec. Agence France-Presse (TVA Nouvelles)

How Canada's Anti-Cyberbullying Law Is Being Used to Spy on Journalists
Patrick Lagacé, a columnist for Montreal's La Presse newspaper, says that police told him he was a "tool" in an internal investigation when they tapped his iPhone's GPS to track his whereabouts and obtained the identities of everyone who communicated with him on that phone. Lagacé alleges that this surveillance was designed to intimidate and discourage potential sources within the Montreal police department from approaching him with information for his story. Police obtained a warrant for this under the hugely controversial Bill C-13, which gave investigators new powers, privacy lawyer David Fraser noted in an interview. The bill was initially sold as combatting cyberbullying and the unwanted publication of intimate images online, also known as "revenge porn (…)"According to Citizen Lab researcher Christopher Parsons, these same powers that target journalists can be used against non-journalists under C-13. And the only reason we know about the aforementioned cases is that the press has a platform to speak out. Motherboard

Bande dessinée et investissement pour lutter contre la radicalisation
Le premier ministre du Québec, Philippe Couillard, a annoncé mardi le lancement d'une bande dessinée, rédigée par des jeunes qui s'étaient radicalisés, ainsi qu'un nouvel investissement de 10 000 $, pour lutter contre la radicalisation. La bande dessinée, nommée Radicalishow, raconte l'histoire de sept jeunes du Centre de prévention de la radicalisation menant à la violence de Montréal qui ont marché sur le chemin de la radicalisation. « C'est fait par les jeunes et pour les jeunes », a souligné M. Couillard. Ces jeunes relatent également ce qui les a incités à quitter cette route. Une édition de l'oeuvre sera publiée en français et en anglais. Radio-Canada

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Canada's dairy industry untroubled by American threats: DFC
Canada's dairy industry says it's not scared by American warnings suggesting new rules on milk classes may violate international trade rules. "We're not scared of threats and we believe whatever we've done inside of our country to deal with our domestic product is something that we have every right to be able to determine for ourselves," Dairy Farmers of Canada President Wally Smith told reporters in Ottawa Tuesday after unveiling the industry's updated blue cow logo. Canada's dairy industry is debating whether to implement a new ingredient strategy after the idea was backed by members at the sector's annual meeting in Charlottetown in July. The strategy, which is not in effect nationally, comes from changes to milk classes in Ontario that tighten import rules in order to dissuade imports of diafiltered milk. (…) Diafiltered milk is a protein ingredient largely being imported from American dairy processors. The Canadian Border Services Agency classifies it as a protein ingredient, while the Canadian Food Inspection Agency says diafiltered milk is milk — a regulatory discrepancy producers say is undermining Canada's supply management system. (…) New York Governor Andrew Cuomo warned Prime Minister Justin Trudeau in a frank October 25 letter the proposed strategy would affect New York milk exports. The letter was made public Monday. iPolitics; Lohud

Firearms, Jewellery, And A Woolly Mammoth Tusk Among Items Seized At Canadian Border
On September 1, CBSA Inland Officers responded to a call from the Chatham-Kent Police Service. CKPS had custody of a United States resident who had been arrested on the evening of August 31 for domestic assault and breaking and entering. The man was a previous deportee who was in Canada on a temporary resident permit, although that permit had expired on August 31. His removal from Canada was stayed pending the outcome of the criminal charges. Also on September 1, a husband and wife from Pennsylvania were referred for an examination at the Blue Water Bridge, after both stating they had nothing to declare. While in secondary, the man admitted that he had an unloaded handgun in a cooler bag in the trailer. The handgun was seized as well as 47 rounds of ammunition that were located near it. He was then arrested for attempting to smuggle a firearm into Canada. Windsor Square; AM800

YYC opens new International Terminal
Calgary International Airport's new International Terminal officially opened for business yesterday morning, marking the completion of the largest single infrastructure program in the airport's history. The new 186,000 square metre terminal at YYC adds 24 aircraft gates and incorporates numerous technologies and processes designed to streamline the passenger experience throughout the airport. These include North America's first call-to-gate passenger boarding system, North America's first full CATSA Plus enhanced passenger screening system, enhanced U.S. and Canadian customs technology, a state-of-the-art Crisbag tote-based baggage system, and the YYC LINK, a custom-designed and Canadian-build passenger shuttle service that transports passengers between the domestic and international facilities. Travel Week

Canada to lift Romania and Bulgaria visa requirement
The Honourable John McCallum, Minister of Immigration, Refugees and Citizenship, announced today the Government of Canada's intention to lift the visa requirements for Romanian and Bulgarian citizens on December 1, 2017. It demonstrates the importance that the Government of Canada places on its relationship with both countries and with the EU more broadly. However, Ottama would reserve the right to reimpose the visa requirement "should irregular migration trends increase significantly from either country." "In the lead-up to the full visa lifts, Canada intends to implement partial lifts for eligible Romanian and Bulgarian citizens travelling to Canada for May 1, 2017," the statement reads. It also says Romanian and Bulgarian citizens who have held a Canadian temporary resident visa in the past 10 years or who currently hold a valid United States (U.S.) non-immigrant visa would not require a temporary resident visa and would be able to fly to or transit through Canada with an Electronic Travel Authorization (eTA) instead of a visa. Canada Journal

In-transit border pilot extended, new ports added
U.S. Customs and Border Protection has agreed to extend and expand a pilot initiative that uses a reduced data set for permitting Canadian carriers to resume in-transit operations for domestic loads. While the program will extend another year until Nov. 28., 2017, the Canadian Trucking Alliance (CTA) also announced that it has recommended the addition of three ports of entry to the program: Portal, ND/North Portal, SK; Sweetgrass, MT/Coutts, AB; and Sault Ste. Marie, MI/ON. It is unclear at this time when the ports may be added to the program. CTA says it will be working with the U.S. agency throughout 2017 to determine the expanded number of carriers allowed to participate in the in-transit process. It is expected an announcement could be made in the fall of 2017. Today's Trucking News

Halloween inspires Brian Masse statement pushing for Gordie Howe Bridge
Windsor West MP Brian Masse used Halloween puns in the House of Commons yeterday to criticize the government for a lack of progress on the new Gordie Howe Bridge. Masse stood to tell the house, "the project seems to have slipped into the Twilight Zone. Whether it's spooky back-room conversations with the ghouls at the Ambassador Bridge, or a zombie-like approach to property acquisition, the government appears lost in a haunted corn maze rather than on track to build a new crossing." With laughter coming from other members, Masse went on to say the government appears to be building its very own Frankenstein and just waiting for a lightning storm to flip the switch. Bridge authority officials have said the progress on the new bridge is on schedule, but they have not said when the Request for Proposals will be released. CBC News

Libre-échange : les tarifs douaniers au coeur des préoccupations de l'industrie des pêches
L'industrie de la pêche québécoise étudie les impacts de l'accord de libre-échange avec l'Union européenne sur le marché québécois. Toutefois, l'abolition des tarifs douaniers est au cœur des préoccupations des industriels. Le directeur de l'Association québécoise de l'industrie de la pêche (AQIP), Jean-Paul Gagné, estime qu'il est prématuré de tirer des conclusions sur les effets de cet accord. Selon lui, il y a encore trop de questions, mais la question des tarifs douaniers constitue un irritant. Radio-Canada

Broadcast Media / Médias télédiffusés :

CBC News reported on the remote processing pilot project at the Morse Line border crossing. Rough Transcript (2016-10-31)

Calgary's new international terminal is home to the Canada Border Services Agency's new flagship operation in the Prairies. It can accommodate up to 5,200 travelers at one time, more than double what the old space could've held in the original YYC terminal. The new space has 54 automated kiosks to help speed up clearance into the country. Connecting travelers benefit with a new secure connection corridor that improves passenger flow. (City TV Calgary, 8h35ET, 10h04ET)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Google discloses Windows zero-day, Microsoft argues disclosure ethics
On Monday, Google disclosed a zero-day vulnerability in Windows, which if exploited will enable an attacker to use it as a security sandbox escape. In response, Microsoft didn't offer details on a fix, instead choosing to promote Windows 10 and argue for coordinated disclosure. Google says the flaw was discovered on October 21, along with a vulnerability in Adobe's Flash. Adobe fixed their software last Wednesday, but since the Windows vulnerability is being actively exploited online, Google disclosed basic details about the flaw on Monday (…) A Microsoft spokesperson said Google's actions have potentially placed customers at risk. The statement goes on to reiterate the software giant's belief in coordinated vulnerability disclosure, along with a brief nudge for everyone to update to Windows 10. "We believe in coordinated vulnerability disclosure, and today's disclosure by Google could put customers at potential risk. Windows is the only platform with a customer commitment to investigate reported security issues and proactively update impacted devices as soon as possible. CSO Online; Threatpost; Dark Reading

Security Awareness Month Tips: Small rewards can go a long way
Cyber security awareness month winds up today, but before it ends we've got more advice from Symantec to pass on to infosec pros that hopefully will be useful in their work. It comes from Jamie Manuel, information protection manager at Symantec, who reminds CISOs that employee awareness training is always worth it. "A lot of companies focus on external threats, which are important," he said in an interview, "but in terms of educating employees they're really the front line and their actions can greatly increase your odds" of being more secure. So it's important to make sure everyone on staff understand the organization's security posture and how how doing – or not doing certain things can put the firm at risk. The trick, of course, is getting the message through. As we've written this month through our interviews and coverage from the SecTor cyber security conference, many experienced in the industry say repeatedly that security awareness training has to done more than once a year. Many think it should be done monthly. IT World Canada (2016-10-31)

MI5 chief not alone in voicing fears about Russian cyber-threat
Worries about Russian spying are nothing new, but the incumbent head of MI5's claim that Moscow now poses a huge threat online, in addition to the traditional arenas of espionage, chimes with a number of recent western assessments of Russia's hacking capabilities. "There is high-volume activity out of sight with the cyber-threat," Andrew Parker told the Guardian. "Russia has been a covert threat for decades. What's different these days is that there are more and more methods available." While the Kremlin swiftly dismissed the allegations that hostile Russian activity is a threat to Britain, Parker is not the first to voice concerns about Russia's online activities. Guardian UK; Reuters

Facebook Messaging Encryption Best to Protect Privacy
Facebook Inc.'s message applications Messenger and WhatsApp have the best encryption security to protect consumer communications privacy, Amnesty International said Oct. 21. Facebook, whose two messaging apps have a total of 2 billion users, is "doing the most to use encryption to respond to human rights threats, and is most transparent about the action it's taking," Amnesty International said. The ranking may not only be important to activists and individual users concerned about keeping their

conversations private, but also to companies seeking to monetize privacy protection in the highly competitive mobile messaging market. Bloomberg Legal

Algorithm Red Flags Potentially Dangerous Domain Names at Time of Purchase
A machine-learning algorithm that can detect malicious domain names as soon as they're purchased has piqued the interest of at least one corporate IT executive. Invented by five researchers at Princeton University and the University of California, the code works by scanning for 22 "features," or red flags that are consistent with suspicious behavior. They include names that are registered in bulk by the hundreds, names that are variations of the same name, random-looking names, and names with numerical characters. The tool would be helpful if it were used by the hundreds of registrars offering domain names for purchase in order to stop cyber criminals planning attacks as they're purchasing the names, said Vincent Weafer, senior vice president at McAfee Labs at Intel Security. Wall Street Journal

LAW ENFORCEMENT / APPLICATION DE LA LOI

Videos show events before B.C. RCMP arrest of elderly couple
The RCMP officers called to the scene of a raucous condo meeting in Coquitlam, B.C. are under investigation for their actions in the arrest of an elderly couple. The contents of a jarring cellphone video showing the elderly man dragged down a flight of stairs prompted not only an internal RCMP investigation, but also involved local police. But new footage has emerged showing pieces of the scene leading up to the arrest. The B.C. Condo Homeowner Association meeting on Oct. 27, held at a Best Western in the Vancouver suburb, heated up over, what appears to be, the results an election. YouTube users Victor Kim and Jee Grace, who attended the meeting, have posted more videos to the social media channel. One video shows a man who appears to be announcing the results of an election to a room full of agitated people. The man seems to have lost control over the crowd and yells over the din. He says that the results are in and will be sent to a lawyer. This is met with shouts and protests from the other members. CTV News

No one injured after RCMP car crashes in dangerous intersection
Winnipeg police said no one was injured following a crash involving an RCMP cruiser and a minivan Monday. Around 12:25 p.m., officers responded to the intersection of Kenaston Boulevard and McGillivray Boulevard following a collision with a police car. WPS said the cruiser, which had two RCMP officers inside, was travelling westbound on McGillivray. They explained the officers were on their way to a service callwith their lights and sirens on and as they attempted to turn at the intersection, the crash occurred. According to police, the collision involved a minivan and light standard. The two officers and the driver of the minivan were not injured. Winnipeg Police Service investigators in cooperation with the RCMP continue to investigate. CTV News; CBC News

Kelowna council wants a return of the RCMP Auxiliary constable program
Kelowna city council wants the RCMP auxiliary constable program back—but it want to see changes. The program, which provided civilian volunteers to support the RCMP by working with community groups, at local events and with the public, was suspended by the federal government in January 2016 pending a review of the program. (…) Tier 2 would be all the activities of the status quo option, as well as traffic and crowd control, parades and public ceremonies as well as foot and bike patrols under the supervision of an RCMP officer. Under this tier, auxiliary constables would be appointed peace officers and wear police-type uniforms, get intervention tools and soft body armour. There would be more training and work would be limited to 96 hours of participation per year. They could not work after 9 p.m. Tier 3 would include tier 1 and 2 duties, as well as general duty patrol in RCMP vehicles, manning check stops and other activities deemed appropriate. Kelowna Capital News

Windsor Mounties Make History
When members of the Royal Canadian Mounted Police participated as part of a Colour Guard during the commissioning of the USS Detroit on October 22, it was history in the making. The three RCMP members, Sgt Diebel, Cst McDonnell and Cst Kukhta, all part of the Windsor Shiprider Unit, donned the red serge for the commissioning and marked the first time for the US Navy that another country had been

included in such a ceremony. Canada-US Shiprider program involves vessels jointly crewed by specially trained and designated Canadian and US law enforcement officers who are authorized to enforce the law on both sides of the international border. "The request to have Canadian participation came from numerous US agencies in the local Detroit area," said John Peracchio, the chair of the USS Detroit commissioning committee. "They pointed out that our Canadian partners play such a vital role in our shared border security interests that they should also share in our celebrations". Windsor Square; Ottawa Citizen

Wellington man charged with running illegal internet drug site
New Zealand Police and Customs have identified and spoken to more than 160 people nationwide for buying illegal drugs via darknet and other illegal sites, with more Police visits to come. Last week law enforcement agencies around the world took part in Operation Hyperion, a coordinated effort to target buyers and sellers of illegal drugs over the internet. From October 22 to 28, agencies focused on packages coming through mail centres, and then tracked these back to buyers and sellers. (…) Several more investigations are in progress with more people yet to be visited. One person faces 13 importing charges relating to ecstasy, LSD and cannabis. As well as Police and Customs, Operation Hyperion involved international partners including; Europol; the United Kingdom's National Crime Agency; Australian Federal Police; U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), U.S. Customs and Border Protection (CBP), U.S. Postal Inspection Service (USPIS), Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), U.S. Secret Service (USSS); Canada's Royal Canadian Mounted Police. Wellington Scoop

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Paul Bernardo's day-parole hearing scheduled for March
Notorious killer Paul Bernardo is scheduled for a day-parole hearing next March. The lawyer for the families of Bernardo's murder victims, 14-year-old Leslie Mahaffy and 15-year-old Kristen French, says he believes Bernardo will never get parole. Tim Danson says there have been many dates set for day-parole hearings, but all of them have been adjourned. Nonetheless, Danson says the process has "gutted" the families of his victims, but he believes Bernardo will die in prison. Canadian Press (CBC News); iNews880; CHCH News; Agence QMI (TVA Nouvelles); La Presse Canadienne (Le Devoir)

Man convicted in Cole Harbour home invasion hauled back to prison
A man serving a 12-year sentence for his part in a deadly home invasion has had his statutory release privileges revoked for a second time by the Parole Board of Canada. Joseph Charles Dawson was sentenced in 2005 for robbery and manslaughter related to a home invasion in Cole Harbour a year before where John Wyllie was stabbed to death. Dawson's accomplice, William Ray Best, was sentenced to life in prison for second-degree murder in Wyllie's death. Dawson was let out on statutory release in April. He was brought back to prison in July after he failed to return to a halfway house before his curfew. When police found him, he was drunk and tried to escape by running away. In a decision released this week, the Parole Board of Canada explained why Dawson was returned to prison. "The board is of the opinion that by your own actions you have aggravated your risk of reoffending to a level where you cannot be safely managed in the community and that the circumstances surrounding this suspension were within your control," the decision says. CBC News

Lessons Learned From 1,500 Days in Isolation
An opinion piece states, "Twenty-three hours a day for 1,500 days. That's how long Adam Capay, a 23-year-old indigenous man, had been held in solitary confinement, bringing Canada's abusive practice of isolating prisoners for prolonged periods of time into the spotlight again. A recent visit by the Ontario Human Rights Commission to a provincial jail in northwestern Ontario revealed that Capay has spent four years confined to a basement cell, alone under the glare of 24-hour artificial light. The length and conditions of this young man's confinement are abhorrent. Indefinite solitary confinement is cruel, inhuman and degrading treatment and can even amount to torture under international law. What is puzzling though is why, despite a public inquest, a Commission of Inquiry, and demands for accountability following suicides in solitary cells, has nothing changed? How have successive governments squared this

inherently cruel and inhuman treatment of prisoners with their professed respect for basic human rights?" Human Rights Watch

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

We Asked Experts How to Solve Canada's Opioid Crisis
Canada is reeling from the opioid crisis. It's a complex issue that has developed into epidemic proportions in past years, leading to a troubling increase in drug-related deaths. It's not a situation that will be easy to get out of. But if you're reading this article, you probably already knew that. When OxyContin was pulled from pharmacy shelves in Canada in 2012 and replaced with a "safer" alternative, the result was far more deadly than anyone could have predicted. Fentanyl, an opioid many times stronger than heroin and morphine, appeared on the black market when the illicit drug market saw an opening. While the drug is available as a prescription, much of what appeared on the streets was a bootleg version. As fentanyl continues to flow into Canadian cities, it has already killed thousands. We don't have a complete picture, but here's what we do know from a couple of provinces that have been hit hardest by the worst drug safety crisis in Canadian history. So far in 2016, British Columbia has reported a record 555 drug overdose deaths, up from 508 from all of last year. In Alberta, the number of fentanyl-related deaths hit 153 at the end of June. And the year is not over yet. Unfortunately, as you're reading this, the death toll has already increased. The federal government has called a national opiate summit in Ottawa on November 18 and 19, but ahead of that, we wanted to allow some of those who have ideas for solutions to speak. Because the opioid crisis is a complicated, multi-faceted problem, we asked people from a variety of disciplines to voice their recommendations. VICE News

Other opioids responsible for more Edmonton deaths than fentanyl
Fentanyl is not the biggest killer for opioid users in Edmonton. New numbers in the government's Opioids and Substances of Misuse Alberta Report show more people in the city are fatally overdosing on other types of opioids. While 52 people fatally overdosed on fentanyl in Edmonton from January through September this year, 63 fatally overdosed on opioids other than fentanyl. Metro News

Tiny Alberta-made sensor may open door to hand-held drug tests
A woman is at a party and realizes someone may have slipped something into her drink. Even if she tosses it, her uncertainty and worry remain. She wonders: Has someone tried to drug me? In the future, it may be possible to get an answer by discreetly dabbing a few drops onto a smartphone and getting an on-the-spot chemical readout of what's in the drink. A portable but sensitive device for performing such tests could be realized with the help of a tiny magnetic sensor developed by a team of Alberta-based researchers. "At this moment we're far from actually doing that, but there aren't any physical reasons why that won't work," said Mark Freeman, a University of Alberta physicist who has worked out the technology that underlies the idea. In 2008, Dr. Freeman and his team developed a tiny magnetic sensing device, called a torque magnetometer, on a piece of silicon chip that is smaller than the diameter of a strand of human hair. The device features a tiny spatula-shaped arm suspended on a narrow band of material that twists ever so slightly when the arm is pulled up or down by a magnetic field. Globe and Mail

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Officer pleads guilty over online remarks following death of indigenous artist
An Ottawa police officer has pleaded guilty to two Police Services Act charges in connection with online comments about the death of Inuk artist Annie Pootoogook. Sgt. Chris Hrnchiar was charged with two counts of discreditable conduct under the act. Pootoogook's body was found in the Rideau River on Sept. 19 — a death that police did not at first treat as suspicious. Several days later, racially charged comments on Facebook suggested Pootoogook's death ought not to be linked to the phonomenon of missing and

murdered indigenous women across Canada. The online remarks sparked outrage in Canada's indigenous community and elsewhere. Ottawa police Chief Charles Bordeleau called the comments inappropriate, saying they had racial undertones and didn't reflect the values of the service. Canadian Press (570 News)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Legal cannabis could be federal cash cow, Parliamentary Budget Officer says
Legalizing marijuana may not provide a major cash boost for governments right out of the gate, but it could generate more tax revenue as consumers move from the illicit to legal market, says Canada's Parliamentary Budget Officer. In a report released today studying the fiscal considerations of legalizing marijuana, the PBO Jean-Denis Fréchette suggests initial revenue for governments from taxation could be in the hundreds of millions of dollars, rather than billions. The report also suggests that 60 per cent of revenues would go to provincial governments, with the remainder going to the federal government. The report also warns that there will be little room to tax legalized marijuana without pushing the legalized price of marijuana much higher than the illegal price. Too high a price could encourage consumers to turn back to illegal sources. CBC News; Radio-Canada; Canadian Press (Castanet)

PUBLIC SERVICE / FONCTION PUBLIQUE

D'ex-militaires et fonctionnaires LGBTQ veulent poursuivre le gouvernement
D'anciens fonctionnaires et militaires qui disent avoir été intimidés et limogés à cause de leur orientation sexuelle ont déposé une requête pour intenter une action collective contre le gouvernement fédéral. Doug Elliott, un avocat torontois, a indiqué que ces gais et lesbiennes ont attendu assez longtemps dans l'espoir d'obtenir une entente négociée, et qu'il est maintenant temps de passer de la parole aux actes. Les libéraux de Justin Trudeau avaient promis de présenter les excuses officielles du gouvernement canadien à tous les membres de la communauté LGBTQ qui auraient été victimes de discrimination au sein de la fonction publique. On ignore cependant si ces excuses seront accompagnées d'indemnisations. Presse canadienne (La Presse); CTV News

LGBT ex-public servants suing Ottawa for $600 million
Former federal civil servants and members of the military who lost their jobs because of their sexual orientation have launched a $600 million class-action lawsuit against the Government of Canada. Doug Elliott, a lawyer with Cambridge LLP in Toronto whose client is a plaintiff in the case, announced the lawsuit Tuesday morning on Parliament Hill, saying statements of claim have been filed in Montreal and Toronto. The statement of claim filed in Ontario Superior Court says the plaintiffs are seeking general and aggravated damages of $500 million, and punitive and exemplary damages of $100 million. Elliott said the damage claim in Quebec does not specify an amount but said it would probably be "proportionate" to the Ontario claim. The practice of dismissing gay and lesbian public servants — what has come to be known as the "LGBT Purge" — began in the 1950s and continued for decades. iPolitics; CBC News

Phoenix by the numbers: Keeping track of the costs, staffing and backlog of cases
It's been 15 weeks since the federal government first gave the public a sense of the scope of the Phoenix payroll system problem. Back on July 18, the government revealed some 82,000 public servants had reported trouble with their pay, with the majority being underpaid. Others were overpaid or not paid at all. Since then, the government has been providing updates every two weeks and a steady stream of numbers to show their progress. Here, we break down some of the essential figures we've learned over the past few months. CBC News; Torstar (Hamilton Spectator, Waterloo Region Record); Postmedia (Ottawa Sun); La Presse; Canadian Press (Maclean's Magazine)

OTHER / AUTRES

NIL

INTERNATIONAL

Russia presents a growing cyber threat, according to UK spy chief
Russia is pushing its foreign policy in increasingly aggressive ways including cyber-attacks and espionage, posing a growing threat to Britain and the rest of Europe, the head of Britain's internal intelligence agency MI5 has said. The Kremlin dismissed the allegations as untrue and challenged its critics to produce evidence. MI5 Director General Andrew Parker said Russia had been a covert threat for decades, but what differed now from the Cold War era was that there were more and more methods available for it to pursue its anti-Western agenda. Reuters (Globe and Mail)

Photos show pain and jubilation as Iraqi forces parry ISIL car bombs, penetrate outer edge of Mosul
Iraqi commanders on Tuesday said they were fighting inside an industrial district on the outer edge of Mosul, making their first breach into the city that has been under Islamic State control for nearly two and a half years. Soldiers from Iraq's elite counterterrorism force said they had entered the neighborhood of Gogjali on Tuesday morning. From the village of Bazwaya, just four miles to the east, jets circled overhead and explosions could be heard from the front lines. "Right now I'm in the middle of Gogjali," said Lt. Gen. Abdelwahab al-Saedi, a commander with the counterterrorism forces, speaking by phone. "We are dealing with pockets of resistance and booby traps." The elite Iraqi troops are making a sharp push into the city from the east, but other forces on other fronts remain farther away, exposing advancing troops to attack from their flanks as they press forward. Washington Post (Leader-Post)

Female Jihadis Give ISIS New Avenues for Attacks
It was early on a Sunday morning in September when French police discovered a Peugeot parked near the Notre Dame Cathedral in Paris with its hazard lights flashing and its license plates removed. The car carried seven gas cylinders, six of them full, and three cans of diesel. The perpetrators had perhaps intended to blow it up with a lit cigarette and a fuel-soaked blanket, but the vehicle failed to detonate. Three weeks after that failed plot, police arrested two teenage suspects accused of planning a violent attack in Nice, the details of which haven't been made public. At the center of both plots: women allegedly inspired or directed by the Islamic State militant group. All had been in contact with a prominent French recruiter for ISIS, Rachid Kassim, who is believed to be in Syria. Roughly a year after the ISIS attacks in Paris that killed 130, France remains in a state of emergency, thanks in part to later assaults inspired by the militant group in Nice and the northern town of Rouen. Now, however, a new threat is emerging: women who want to wage violent jihad just like men. Newsweek (2016-10-31)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Gordon Hoekstra
Seismic rift: Lack of government leadership on upgrades of old, private buildings http://bit.ly/2f3MyL2 #earthquake

CBC Newfoundland
Search continues for #nlmissing man William Snelgrove http://cbc.ca/1.3830512

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Public Safety Canada
Interested in National Security accountability? Join us on Twitter Thursday to discuss with our experts #YourNatlSec

Sécurité publique
La responsabilité en matière de sécurité nationale vous intéresse? Rendez-vous jeudi sur Twitter pour discuter avec nos experts #VotreSecNat

NATIONAL SECURITY / SÉCURITÉ NATIONALE

PhilippeVincentFoisy
Je serai vers 13:30 avec @E_Duhaime et @B_Drainville pour parler de #radicalisation et de la bd lancée par le gvt #polqc

Stewart Bell
Link to unreleased study of Canadian terrorist trends done for Public Safety.
https://www.scribd.com/document/329525040/Pattern-Analysis-of-Events-of-Terrorism-and-Extremism … Story:

Le Soleil
Couillard dénonce la surveillance policière des journalistes

Alex Boutilier
A reminder the Canadian Association of Journalists is putting on a security awareness workshop in Ottawa Friday.
https://www.facebook.com/events/1014858785325935/1014892551989225/?notif_t=admin_plan_mall_activity&notif_id=1477516455346561 …

CJFE
The #SPVM spying on journalist @kick1972 Patrick Lagacé is a grim benchmark for press freedom.
#ProtectPressFreedom http://bit.ly/2fAEJND

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

The National
Canada plans to welcome 300,000 immigrants in 2017 http://www.cbc.ca/1.3829496

MigrantWrkrsAlliance
The federal government has kept immigration levels at 2015 number which is net decrease.

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NSPS (CBoC)
ICYMI: The Dyn #DDoS Attack: Two Key Lessons for #Cyber Security https://www.linkedin.com/pulse/dyn-ddos-attack-two-key-lessons-cyber-security-satyamoorthy-kabilan … by @The_Fuzz74 #infosec #csam

BlackBerry
14,000 Unique Malware Are Threatening Your Android Smartphone. How #BlackBerry's Secure Android Phones Keep You Safe http://blck.by/2f8TiFe

SCMagazine
Latest Joomla flaws exploited to place backdoors, then patched by same attackers

LAW ENFORCEMENT / APPLICATION DE LA LOI

CTV Winnipeg
No one injured after RCMP car crashes in dangerous intersection #ctvwpg http://bit.ly/2f9Xntb

David Pugliese
RCMP takes part in USS Detroit commissioning in what is being called a first for the U.S. Navy

Stephen Puddicombe
RCMP Forensic officer shows a photo of the enclosure which housed the Rock Python that from a distance looks huge #cbc it has it's own door

The Georgia Straight
The irresistible allure of a Hells Angels funeral and the cost of the war on drugs http://ow.ly/Z3RQ305K73M #HellsAngels #Vancouver #drugs

CTV News
Videos show events before B.C. RCMP arrest of elderly couple http://ow.ly/ZfXR305K0EE

RCMP
Spousal Abuse Counselling Program in Rankin Inlet, #Nunavut helps abusers from re-offending. http://rcmp.ca/-Zdh

Great Big Story
Canadian police are handing out thousands of tickets to children — for positive behavior. @ExploreCanada shows us why. #ExploreCanada

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Emma Loop
In fact, statistics show the use of parole in general at the federal level has declined quite a lot.

Emma Loop
I understand why people are outraged, but offenders have a statutory right to parole hearings. It *does not* mean they'll get it.

Emma Loop
This is a situation/story where public understanding of federal parole needs to be better understood.

TVA Nouvelles
Paul Bernardo aura droit à une audience pour faire une demande de libération conditionnelle, en mars 2017.

CTV News
Paul Bernardo's day-parole hearing set; families of victims 'gutted' http://ow.ly/CXXW305JR5I

HuffPost Canada
Paul Bernardo gets date for day-parole hearing http://huff.to/2eXHFQI

Globalnews.ca
School girl killer Paul Bernardo has day-parole hearing set for March

John Howard Society
Watchdog alarmed over use of pepper spray by prison guards

The Globe and Mail
Treatment of Adam Capay 'disturbing,' Ontario Premier Kathleen Wynne admits http://trib.al/PkGIVTD from @adrianmorrow and @Nut_Graf

Angela Sterritt
After 4 years in solitary confinement,Adam Capay has hired one of Canada's most experienced criminal defence lawyers

CDN Civil Liberties
The Number of Female Indigenous Prisoners in Canada Has Doubled in the Last Decade: http://ow.ly/f417305JMhf via @rp_browne @vicecanada

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Sheldon Kennedy
Lets go purple! November is Family Violence Prevention Month and you can show your support by wearing purple Nov.1st! #abfvpm @ShelKenn

OCTEVAW
Join us tonight for the launch of #ShineTheLight on Woman Abuse Campaign. We will learn from advocates, survivors and young women 7.15pm

NCCM
142 Concerned Canadians signed this open letter re: Allegations of Islamophobia & anti-black racism http://tinyurl.com/j7ns7jk #yrdsb #onpoli

Rachel Browne
@allison_elkin rounds up a wealth of concrete, evidence-based solutions for the opioid crisis:

VICE Canada
How the opioid crisis came to be: http://bit.ly/2f5c0ho

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Sheila North Wilson
Great to spend time with ZDF German Television today, talking about #MMIW Thanks Johannes Hano and Suzanne and crew for coming down

Rabble.ca
Why are Aboriginal women experiencing violence at far greater rates? In one word, colonialism. http://buff.ly/2f5Py9X #MMIW #cdnpoli

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

CBC Canadian News
Cannabis cash cow? Canada's parliamentary budget watchdog sees pot potential http://ift.tt/2fAspNg

iPolitics
PBO: governments should expect 'modest' revenue from legal pot http://ipolitics.ca/2016/11/01/pbo-governments-should-expect-modest-revenue-from-legal-pot/ ...

Hill Times
The PBO's report on the fiscal implications of legalizing marijuana is out. Read our feature on Cda 'going green' http://bit.ly/2f8PWSD

CTV News
Legal marijuana tax revenues will be shy of $1B, to start: PBO http://ow.ly/gqq0305JKFr

CBC News Alerts
Legal marijuana won't provide big cash boost for gov't, Parl. Budget Office says. Little room to tax without pushing cost above illegal pot

TVA Argent
Marihuana thérapeutique : la Québécoise Vert Médical est vendue à l'Ontarienne Canopy Growth Corp. http://bit.ly/2f8T4ha

PUBLIC SERVICE / FONCTION PUBLIQUE

iPolitics
#LGBT ex-public servants suing Ottawa for $600 million. @bbritneff reports. http://ipoli.ca/2eRcpp4 | iPolitics Photo #cdnpoli

Maclean's Magazine
Feds blow deadline to fix payroll debacle:

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

Today's News / Actualités
November 2, 2016 / le 2 novembre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

TOP STORIES / MANCHETTES

La famille Shafia n'aura pas de nouveau procès

Mohamed Shafia, son épouse Tooba Yahya et leur fils Hamed n'auront pas droit à un nouveau procès comme ils le réclamaient : la Cour d'appel de l'Ontario a en effet rejeté leur demande, mercredi midi, à Toronto. Rappelons que la justice avait condamné les trois membres de la famille Shafia à la prison à vie, sans possibilité de libération avant 25 ans, pour les meurtres des trois filles du couple et de la deuxième épouse de Mohamed Shafia. Les Shafia souhaitaient qu'un nouveau procès ait lieu. Ils prétendaient avoir été victimes d'erreurs judiciaires et de stéréotypes culturels lors du premier procès tenu à Kingston, en 2012. Le fils, Hamed tentait aussi de convaincre la justice qu'il était mineur au moment des faits qui leur sont reprochés. Radio-Canada ; CBC News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Windsor, Tecumseh flood causes $108M in insurance claims
The heavy rain and flooding that rocked Windsor and Tecumseh, Ont. caused nearly $108-million in insured damages, the Insurance Board of Canada reports. Residents filed nearly 6,000 home, auto and business claims in the five weeks since the flooding struck Sept. 29. The Insurance Board of Canada represents Canada's private home, auto and business insurers. It reports the values of insurance claims following major storms and natural disasters. CBC News; Canadian Underwriter; Windsor Star

Windsor flood victims still waiting on insurance
Several people in Windsor-Essex are still waiting for insurance claims to clear, nearly five weeks since hundreds of homes in the area were devastated by flooding. David Norwood of Tecumseh describes the process as "very frustrating." He still doesn't know how much money he's getting back. "I think we're covered," he said. "I think we're covered appropriately, but because we haven't seen the end result, we're still kind of waiting." CBC News

Canada not prepared for climate change, warns report
A broad survey of most of Canada has found that the country is not well prepared for the effects of climate change, with flooding of particular concern. The report was prepared by Waterloo's Intact Centre on Climate Adaptation which was set up and is partially funded by a leading property and casualty insurance company. Climate change is expected to bring more fire storms, hail, high winds and floods. "No area of the country is immune from flooding," says Blair Feltmate, head of the centre and author of the report. "Floods are occurring now that used to occur once in 100 years. Now, we're getting two or three of those types of floods perhaps in a 10-year period." Flooding in various parts of Canada have already been expensive for the insurance industry. Catastrophic flooding in the province of Alberta in 2013 alone cost it $1.7 billion in paid claims. Radio-Canada International

Alberta gets C+ grade in national flood readiness report
A new report looking at climate change and how well jurisdictions across Canada are prepared for future flooding says Alberta needs to do a lot better. The University of Waterloo report graded all of Canada's provinces and Yukon in 12 key areas, using data gathered in surveys participated in by provincial ministries, departments and agencies. The report gives Alberta a C-plus grade, with the average national score being a C-minus. CBC News

Forest fire season in northwestern Ontario officially over, season report released
Although there were fewer forest fires in 2016 across Ontario than the ten-year provincial average, fire fighters were kept busy with challenging blazes this season, according to the year end report from the Aviation, Forest Fire and Emergency Services (AFFES). The report said that AFFES recorded 636 fires with 83,009.5 hectares burned, compared to last season which saw 667 fires and 39,311 hectares burned. The report cites both human-caused fires that needed aggressive ground and air attack to contain, as well as fires caused by lightning, Nipigon District Fire 12, which forced an evacuation in Geraldton, Ont., and Kenora District Fire 18 were two of the most severe in the northwestern region. CBC News

Coast Guard, CFB Trenton conduct training exercise
The crew from the Canadian Coast Guard ship Cape Mercy was on Lake Ontario about six kilometres

south of Cobourg on Monday practising with members of CFB Trenton. It was the first time the ship has been involved in training with a Globemaster aircraft from 429 Squadron at the base. Canada has five Globemasters which can provide rapid delivery of troops and cargo transport to oversized combat equipment from coast to coast and to anywhere else worldwide. They have a maximum range of approximately 5,500 nautical miles and can carry a payload of up to 160,000 pounds. The Globemaster did two low fly passes over the Cape Mercy, first at 1,000 feet, then at 500 feet. Northumberland Today (2016-11-01)

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Radicalisation sur Internet : quelle est la responsabilité des fournisseurs?
L'Internet et les réseaux sociaux comme agents de radicalisation des jeunes ont été au cœur des discussions dans le cadre de la conférence Québec-Unesco *Internet et la radicalisation des jeunes : prévenir, agir et vivre ensemble*. Que ce soit par la diffusion de discours haineux ou le recrutement sur les réseaux sociaux, plusieurs se questionnent sur la nécessiter de restreindre l'accès à certains contenus. Devant ce nouvel enjeu numérique, quel est le rôle des fournisseurs? Voici l'avis de trois intervenants présents à Québec. Ross LaJeunesse, responsable mondial de la liberté d'expression et des relations internationales, Google Inc. Google interdit certains sites Internet lorsque la réglementation d'un pays l'exige. Toutefois, ce n'est pas l'approche privilégiée par la multinationale pour faire taire les discours haineux. Ross LaJeunesse, qui représentait Google lors de la conférence, explique que le moteur de recherche mise plutôt sur le contre-discours. « Lorsqu'un internaute écrit un mot clé qui nous indique qu'il recherche un contenu radical, nous lui présentons une publicité dont le contenu contredit ce qu'il recherche [traduction] », explique-t-il. Radio-Canada

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

14 travailleurs étrangers arrêtés à Victoriaville
En vertu de la Loi sur l'immigration et la protection des réfugiés (LIPR), des agents de l'Association des services frontaliers du Canada (ASFC) ont procédé, mercredi dernier (26 octobre), à l'arrestation de 14 travailleurs non autorisés lors d'une opération. Au total, une vingtaine d'agents de l'ASFC, assistés de policiers de la Gendarmerie royale du Canada (GRC) et de la Sûreté du Québec (SQ) ont effectué une perquisition dans une agence de placement de Victoriaville. «Cette opération s'inscrivait dans le cadre d'une enquête sur l'embauche de travailleurs non autorisés. Les 14 personnes arrêtées font l'objet de mesures administratives», a indiqué Dominique McNeely, conseiller en communication, région de Québec, à l'Agence des services frontaliers du Canada. L'ASFC a, de plus, mené, le même jour dans le secteur de Victoriaville, une opération de contrôle des travailleurs. (…) Une opération, comme celle de la semaine dernière, n'est pas monnaie courante à Victoriaville. «Ce sont des opérations plutôt périodiques, a précisé M. McNeely. Mais l'ASFC effectue régulièrement des opérations du genre partout au Québec dans des secteurs comme l'agriculture et autres.» La Nouvelle

De jeunes Québécois auraient piraté des guichets aux États-Unis
Un groupe d'étudiants québécois aurait cloné des centaines de cartes bancaires canadiennes, puis effectué plusieurs retraits d'argent massifs dans des guichets automatiques aux États-Unis, rapporte *La Presse*. Leur manière de procéder était ingénieuse, explique le quotidien. Pour contourner les mesures de sécurité en vigueur au Canada depuis l'arrivée des cartes à puces, ils auraient eu l'idée de copier des centaines de cartes sur support magnétique au pays pour ensuite organiser des voyages éclairs de l'autre côté de la frontière. Une fois sur place, ils auraient introduit ces fausses cartes dans des

guichets automatiques locaux, qui utilisent encore la technologie de la bande magnétique, et procédé à de nombreux retraits d'argent sous la forme d'avances de fonds. Les jeunes Québécois se seraient ensuite parfois rendus dans des agences de transfert de fonds électronique, d'où ils auraient envoyé cet argent à des amis. C'est l'Agence des services frontaliers du Canada (ASFC) qui a mis la puce à l'oreille des enquêteurs américains le 29 mars dernier, indique *La Presse*. Ce jour-là, les douaniers canadiens ont fouillé le véhicule de deux Lavallois de 21 ans, Mathieu Baaklini et Ghassan Mitri, qui revenaient au pays après un séjour d'une heure et demie dans le Vermont. Conseiller

Crown seeks prison term for LaSalle mother convicted of gun smuggling
A LaSalle mother convicted of smuggling guns across the border into Canada will learn her fate January 20th. Michelle Downey was convicted of 22 criminal and Customs Act charges in August for attempting to smuggle three loaded, nine-millimetre handguns into Canada. At her sentencing hearing Wednesday, the Crown asked the judge to impose a prison sentence of three to four years. Windsor Star

Rights group urges Canada to protect migrant workers
A caregiver rights advocacy group has asked the Canadian government to give due consideration to the plight of migrant workers in its planned restructuring of the Temporary Foreign Worker Program by year's end. While a House of Commons committee had outlined its recommendations to Ottawa in September for the proposed TFWP revision, Toronto-based Caregivers' Action Center believes migrant workers and their advocates were given insufficient chance to air their side in the review process. The review, led by the Standing Committee on Human Resources, Skills and Social Development and the Status of Persons with Disabilities (HUMA), was held from May to June and heard from 50 witnesses from different sectors. HUMA presented 21 recommendations to the government of Canada touching on staffing caps, permanent residency, reduced processing times, better rights training, emphasis on local Canadian workers, the needs of seasonal industries, among others. Global Nation Inquirer

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

As CIA shifts gears in response to cyber threats, critics call for good old-fashioned spywork
When America goes to the polls on Nov. 8, according to current and former U.S. intelligence officials, it will likely experience the culmination of a new form of information war. A months-long campaign backed by the Russian government to undermine the credibility of the U.S. presidential election — through hacking, cyberattacks and disinformation campaigns — is likely to peak on voting day, the officials said. Russian officials deny any such effort. But current and former U.S. officials warn that hackers could post fictional evidence online of widespread voter fraud, slow the internet to a crawl through cyber attacks and release a final tranche of hacked emails, including some that could be doctored (...)John Brennan, the current CIA director, declined to comment on the Russian efforts. But he said Russian intelligence operatives have a long history of marrying traditional espionage with advances in technology. More broadly, Brennan said, the digital age creates enormous opportunities for espionage. But it also creates vulnerabilities. Reuters (CBC News)

It's Time To Address The Cybersecurity Gender Gap Before It's Too Late
It's well known that women are underrepresented in technology roles. While women make up 47% of the workforce, only 34% of tech industry professionals are women. Within the cybersecurity sector, the numbers are even worse. Only 10% of IT security workers are women, contributing to a projected 1.5 million unfilled positions within the industry by 2020. While it's unfeasible to completely close the cybersecurity gender gap within three years, this should serve as a wake-up call for educators and employers to more seriously address the dearth of women in cybersecurity and technology more broadly. Dark Reading

How Anonymous and Other Hacktivists Fight ISIS Online
Ever since ISIS started its advance in Syria and Iraq, taking control of large swaths of land, the group distinguished itself from previous terrorists groups for its unprecedented reliance on the internet for propaganda, recruitment, and even some low-level hacking. After tragic ISIS-inspired attacks in Europe, and seeing that ISIS was using the internet as another battleground of sorts, the hacktivists group

Anonymous declared war on the islamic terrorists in 2014. Since then, hacktivists claiming to be part of Anonymous have flagged alleged ISIS social media accounts and targeted pro-ISIS websites. Splinter groups such as GhostSec and CtrlSec have also gone after ISIS online, claiming to pass information to authorities, and boasting of having disrupted recruitment efforts and even one real-world terrorist attack. At the same time, factions within Anonymous, whose contours are by definition hard to define, have condemned the hacktivists' collaboration with the authorities. Some within the government, or former government employees, have embraced their activities. Motherboard

LAW ENFORCEMENT / APPLICATION DE LA LOI

Police seize thousands of fentanyl pills in Calgary
Close to 4,000 fentanyl pills have been seized in Calgary. Members of Alberta Law Enforcement Response Teams (ALERT), along with members of the Calgary and Lethbridge police services and the RCMP, seized 943 fentanyl pills on Oct. 26 and 2,771 pills on Oct. 28. The second seizure took place in the Killarney neighbourhood, where police found the pills in a vehicle and 23 grams of cocaine in a home. Police investigated the home based on information from an Oct. 20 arrest in Aldersyde, in which two Lethbridge men were arrested after allegedly picking up 584 fentanyl pills from the Calgary area. Sofonyas Fkade, 24, and Bereketab Gedecho, 30, were arrested. Fkade has been charged with possession for the purpose of trafficking, production of a controlled substance and possession of property obtained by crime. Gedecho has been charged with possession for the purpose of trafficking and production of a controlled substance. The first arrest on Oct. 26 took place in the Hillhurst area. In addition to the fentanyl pills, officers seized $6,000 in cash proceeds of crime. Cody Bryant, 22, was arrested. He is facing charges including possession for the purpose of trafficking, possession of controlled substances and possession of property obtained by crime. Calgary Herald

Police Agencies Want an Easier Time Serving Warrants to ISPs
For pretty much any crime involving the internet, often the first step in an investigation is trying to figure out who is behind an IP address. But, according to the FBI and other law enforcement agencies, there is a problem: often it's unclear which organisations are actually in a position to respond to legal orders for information, because of the way that IP addresses are distributed by internet service providers (ISPs). In the most innocuous cases, this problem can just be a waste of time, but in others it can present an urgent dilemma, FBI Supervisory Special Agent Robert Flaim told Motherboard in a phone call. According to a presentation from Flaim and other staff from the DEA and the Royal Canadian Mounted Police (RCMP), one case involved the online sexual extortion of a young girl. Because the WHOIS information was inaccurate, it took three months before law enforcement found the right ISP, all the while the girl was continually victimised. (…) So the FBI, DEA and RCMP have proposed a solution: each time an ISP sub-allocates some addresses, that is recorded in the WHOIS. This way, agencies won't have to go asking around trying to find the ISP that just happens to have this data. They can just go to whoever is actually handling the respective IP address. Motherboard

RCMP seek help in Mill Cove vehicle fire investigation
RCMP is investigating an early morning vehicle fire which occurred in Mill Cove Tuesday. Shortly after midnight officers and the Hubbards Volunteer Fire Department responded to the fire along Highway 329 and extinguished the blaze which was behind a residence. The neighbouring property received no damage but the vehicle was destroyed. Lunenburg District RCMP said in a release the home owner heard a noise and when he looked outside, he saw his vehicle in flames with three people standing nearby. The three suspects fled on foot when the owner ran outside. Chronicle Herald

Red Deer runner and police get their man
A champion cross-country runner teamed up with a police officer for a 30-minute chase to bring down a bike thief last Thursday. Red Deer resident Devin Woodland said he recognized his wife's distinct mountain bike while he was out for a run Thursday morning. A man who was likely homeless had it outside the downtown McDonald's and rode off on it after Woodland asked him to give it back. That's when Woodland, the 2012 Alberta Colllege Athletic Conference provincial champion, gave chase on foot and called the RCMP. "He started off really fast and was going through a bunch of back alleys. Then he

thought he lost me, but that didn't last too long," said Woodland, 25, on Tuesday. The chase took him mostly down walking trails and through parks around the downtown. All the while, Woodland was on the phone with RCMP Const. Trevor Naldrett who was tracking the chase in a police vehicle. Red Deer Advocate

Property crime a challenge
The head of the Vernon/North Okanagan RCMP detachment won't be asking city council to fund more police officers in the coming year despite a big jump in calls for service. The detachment received just under 29,000 calls for service in 2015, but requests have increased approximately four per cent so far this year, said Supt. Jim McNamara in an interview with Castanet. MacNamara blamed much of the hike on increased property crime. "Property crime is our biggest challenge," he acknowledged. "We're in the midst of a pilot project where we've started an enhanced day shift to try to better respond to the increase in calls...so far it is working quite well." Just last week, the City of Vernon's crime prevention officer issued yet another plea to Vernon residents to lock vehicle doors and keep garage doors closed after a series of thefts from vehicles in certain neighbourhoods. Castanet

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

La famille Shafia n'aura pas de nouveau procès
Mohamed Shafia, son épouse Tooba Yahya et leur fils Hamed n'auront pas droit à un nouveau procès comme ils le réclamaient : la Cour d'appel de l'Ontario a en effet rejeté leur demande, mercredi midi, à Toronto. Rappelons que la justice avait condamné les trois membres de la famille Shafia à la prison à vie, sans possibilité de libération avant 25 ans, pour les meurtres des trois filles du couple et de la deuxième épouse de Mohamed Shafia. Les Shafia souhaitaient qu'un nouveau procès ait lieu. Ils prétendaient avoir été victimes d'erreurs judiciaires et de stéréotypes culturels lors du premier procès tenu à Kingston, en 2012. Le fils, Hamed tentait aussi de convaincre la justice qu'il était mineur au moment des faits qui leur sont reprochés. Radio-Canada ; CBC News

Former Oshawa politician Robert Lutczyk, jailed for kidnapping and weapons offences, denied parole
A bid for release by Robert Lutczyk, the former Oshawa councillor convicted last year of kidnapping and weapons offences, has been denied by the Parole Board of Canada. The board rejected Lutczyk's applications for both day and full parole following a video conference at Warkworth Penitentiary on Monday, Oct. 31. Lutczyk pleaded guilty last December and was sentenced in February to eight years and four months in federal custody. In a written decision released following the hearing, parole board members cited what they perceive as a failure on Lutczyk's part to take responsibility for his offences and the effect they had. In a written decision released following the hearing, parole board members cited what they perceive as a failure on Lutczyk's part to take responsibility for his offences and the effect they had. The Correctional Service of Canada, which is responsible for federal prisons, recommended Lutczyk's parole application be denied, citing his lack of accountability for his crimes. CSC also questioned the feasibility of Lutczyk's release plan, which was based on residency at a halfway house or with relatives. Oshawa This Week (DurhamRegion.com)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

NIL

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Missing and Murdered: Canada's Lost Indigenous Daughters
An opinion piece states, "Canada's aboriginal population is just over 1.4 million, making up just 4 percent of the populace. Despite the tiny ratio, more than half of the sex trafficking victims in Canada are indigenous. For over three decades, more than 1000 indigenous people have gone missing or have been murdered, according to the Royal Canadian Mounted Police (RCMP). However, civil rights organization believe the number is many time higher, probably closer to 4000. The reasons for the disproportionately huge number of indigenous women that have become victims of sex trafficking are wide and varied, but they all ultimately point to a history of racism, poverty and abuse. "If you're not beat up, then you would get raped by a few of them at once," said a victim."There is a debt bondage that's between $1,000 and $2,000 a day that these girls must bring, must hand in to their trafficker or else," explained Diane Redsky, an advocate for indigenous women and children. Additionally, there have been concerns about the use of excessive force in the RCMP dealing with indigenous people and a broken relationship with their communities. Danny Smyth, Winnipeg's deputy police chief, stated in the past a legacy of bias and racism prevented police officers from understanding the risks to indigenous girls, but he said they were taking steps to address it." Carbonated TV

Canada's Trudeau Should Step Up Efforts to Protect Indigenous Women's Rights
Canada's Prime Minister Justin Trudeau should back up his feminist rhetoric with concrete action on women's rights – particularly when it comes to protecting indigenous women and girls from police violence, according to the statement of Human Rights Watch. Canada's Prime Minister Justin Trudeau must do more to deliver on the promises he made last year to protect indigenous women, specifically from police violence, a rights advocacy group said Wednesday. This Friday marks a year since Trudeau, a self-proclaimed feminist, took the office and launched an inquiry into the missing and murdered First Nation women. "But after a year in office, Trudeau's critics are beginning to question whether he is backing up his feminist rhetoric with concrete action on women's rights – particularly when it comes to protecting indigenous women and girls from police violence," Human Rights Watch stressed. An investigation by the HRW in northern British Columbia found that police officers had been using excessive force and sexual violence against indigenous women and girls. It said First Nation women were also overrepresented among homicide victims and their distrust of police left them in a near constant state of insecurity. Sputnik News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Marijuana : des entreprises du N.-B. se préparent à la légalisation
Des entrepreneurs du Nouveau-Brunswick contemplent sérieusement la possibilité de se lancer dans la production de produits comestibles au cannabis dans un contexte de légalisation. Les ventes de marijuana à usage récréatif pourraient atteindre de 5 à 10 milliards de dollars annuellement au Canada, selon les projections de la CIBC. Ginette Ahier, copropriétaire d'Adorable Chocolat à Shediac, fait beaucoup de recherche ces jours-ci sur l'industrie de la marijuana à usage récréatif. Elle croit que le potentiel pourrait être très important pour les entreprises qui décident de saisir l'occasion. Elle s'inspire de l'expérience américaine. Au Colorado, par exemple, les ventes de produits comestibles à base de cannabis ont dépassé celles des produits à fumer du côté récréatif. « Moi, quand j'ai vu des chiffres l'année passée que 27 % des produits marijuana comestibles vendus au États-Unis étaient des palettes de chocolat, c'est sur qu'il y a une lumière qui s'est allumée », explique Ginette Ahier. Radio-Canada

Should Coors Be Concerned You'll Choose Cannabis Instead?
Molson Coors says it is looking to Colorado for insight on the possible effects the legalization of marijuana in Canada could have on its beer sales. Stewart Glendinning, CEO of Molson Coors International, was asked by an analyst Tuesday during the company's quarterly earnings conference call for his opinion on the potential impact the legalization of marijuana could have on Canada's beer sector. "Cannabis is something we are thinking very carefully about, not only as a business but also as an industry, Glendinning, who was the former head of Molson Coors' operations in Canada, said in response. "There's just a lot we don't know at the moment...It's steady as she goes because of the lack of clarity about the deployment of the drug itself." It's not clear whether Glendinning's comments are a signal that Molson Coors views a recreational marijuana industry as a threat or opportunity. He did not elaborate and the

company did not return calls seeking clarification. But during the call, Glendinning said Molson Coors (NYSE:TAP) is looking to Colorado, the state where the recreational use of marijuana was legalized in 2013 and where the company is headquartered, for guidance. The federal government has said it plans to introduce a bill in the spring to legalize the recreational use of marijuana. Civilized (Times Colonist)

Too legit to quit: Former drug smuggler Brian O'Dea cashing in on marijuana legalization
St. John's native Brian O'Dea was one of the world's biggest drug smugglers in the 1970s and 80s. Today, after leaving the illicit pot trade behind, he's created a new career in the world of legal pot, partnering with some of the biggest names in hip hop. "I don't know if I'm using that [smuggling] experience per se, but what I do is connected to that kind of world," O'Dea told CBC News. "I have a branding company and I'm currently working with the Wu-Tang Clan, Kurupt of the Dogg Pound, Snoop's Dogg Pound, and I'm branding them in the cannabis world." O'Dea teamed up with the rappers to brand their names on cannabis products being sold legally in the U.S. Wu-Tang co-founder Ghostface Killah is marketing a concentrated marijuana called Wu Goo. Kurupt, the Dogg Pound rapper and former vice-president of Death Row Records, is selling Moonrock, one of legal pot's strongest strains. (…) Cannabis is an increasingly legitimate business in North America these days as more jurisdictions legalize marijuana. Now change is coming to Canada. Justin Trudeau promised to legalize marijuana when he was campaigning to become prime minister last year. CBC News

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Prime Minister Justin Trudeau appoints six new senators for Quebec
Prime Minister Justin Trudeau has announced six new senators to fill vacancies in Quebec, including a doctor, an environmental scientist and a mayor. Rosa Galvez is a professor at Laval University and is originally from Peru who has focused much of her research on pollution. Other appointees include Eric Forest, the mayor of Rimouski and Dr. Marie-Francoise Megie, a longtime family physician and professor at the Universite de Montreal. Canadian Press (Globe and Mail, Global News); CTV News

Trudeau urged to follow in his father's anti-nuclear footsteps and support UN disarmament treaty
Even as Foreign Minister Stéphane Dion called a recently announced nuclear disarmament negotiation "more symbolic than real" Tuesday, experts were urging Prime Minister Justin Trudeau to step up and make Canada a bigger part of the movement to ban nuclear weapons — just like his father did during the Cold War. Last week, 123 countries voted in a UN committee to begin negotiations on a nuclear disarmament treaty next year. Canada was among more than 30 countries that voted against, including major nuclear powers and most members of NATO. The vote will be confirmed at the general assembly in December, where Canada could, but isn't likely to, change its vote. Postmedia (National Post)

Military college under microscope over suicide, sexual misconduct reports
Senior Canadian Armed Forces commanders have ordered a complete review of the Royal Military College of Canada following a number of suspected suicides and allegations of sexual misconduct at the prestigious institution in Kingston, Ont. The rare move highlights the growing concern among top brass about the way the 140-year-old college — where future generations of military officers are groomed — is being run. "It's unusual," Vice-Admiral Mark Norman, the military's second-highest-ranking officer, acknowledged in an interview earlier this week. "But with that unusualness comes an indication of how seriously the chief of defence staff and the entire senior leadership are taking this issue." (…) Norman described the college as a "national institution," and said closing it is not an option. However, he said the top brass is prepared to do whatever is necessary to ensure it lives up to its promise and responsibility to both the cadets and Canadian Armed Forces. iPolitics

INTERNATIONAL

U.S. militia girds for trouble as presidential election nears
Down a Georgia country road, camouflaged members of the Three Percent Security Force have mobilized for rifle practice, hand-to-hand combat training -- and an impromptu campaign rally for Republican presidential candidate Donald Trump. "How many people are voting for Trump? Ooh-rah!" asks Chris Hill, a paralegal who goes by the code name "Bloodagent." "Ooh-rah!" shout a dozen militia members in response, as morning sunlight sifted through the trees last weekend. Reuters

Indonesian ISIS sympathisers expected at Anti-Ahok rally on Nov 4
Indonesian police are expecting local sympathisers of the Islamic State in Iraq and Syria (ISIS) to join thousands of Muslim hardliners at a protest against Jakarta Governor Basuki Tjahaja Purnama later this week. National Police Chief Tito Karnavian, who was speaking on the sidelines of the World Peace Forum on Wednesday (Nov 2), said the police has information of ISIS supporters from domestic extremist groups planning to join the rally on November 4. "But the question is whether they are going to commit any violence," he added. Strait Times

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

APTN
Cree Elder charged w smuggling after @CanBorder confiscates ceremonial tobacco
https://goo.gl/STkwOC @RalphGoodale @MattDube @ErinOTooleMP

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Canadian Forces
Crew member in medical distress rescued from fishing vessel at sea #SAR http://ow.ly/TLPb305LX14

Jason Contant
#Windsor #floods spur insured damage of almost $108M to date: @InsuranceBureau @CatIQ_Inc
http://www.canadianunderwriter.ca/catastrophes/windsor-floods-spur-insured-damage-almost-108-million-date-ibc-1004102896/ … … via @CdnUnderwriter

IBC_West
How much do U think an #earthquake could cost #canadians? #canada @AIRWorldwide #EQready
http://goo.gl/jlrZTR

IBC_West
Do you have an #emergency kit? It's never too late - shop or build your own! Easy as ABC123. http://goo.gl/jZFUVl

IBC
Clocks back = time to change batteries in your smoke alarms & carbon monoxide detectors. #DaylightSavings

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Global Montreal
Whistleblower Edward @Snowden to speak at @McGillU

VICE Canada
Canada's anti-cyberbullying law is being used to spy on journalists: http://bit.ly/2foeQkT

The CyberWire
Canadian anti-bullying law may be seeing anti-journalism applications. http://goo.gl/f0Wx9O #cybersecurity #infosec

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CBC Canadian News
Canadian couple faces charges in U.S. for allegedly smuggling fentanyl http://ift.tt/2f0TBRW

Steven Chase
Ottawa to offer compensation to Canadian dairy industry even though it doesn't see losses for them from CETA deal but only reduced growth

Steven Chase
CETA compensation package for Canadian dairy farmers and processors to be announced in days, govt official says.

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

OSC News
We will be holding a hackathon from Nov. 25-27. We are looking for reps from start-ups, banks, developers and more! #OSCDialogue

CSE_CST
Did you know future quantum computers could break the most complicated encryption in minutes? Learn more from our quantum experts @GTEC

CST_CSE
Saviez-vous que l'ordinateur quantique pourrait percer le chiffrement le plus complexe en quelques minutes? Visitez nos experts à la @GTEC.

CSE_CST
We're excited to be participating @GTEC again this year. http://ow.ly/Z1p7305MfGI

CST_CSE
Le CST est heureux de participer à la @GTEC encore une fois cette année. http://ow.ly/MBWV305MfUJ

NSPS (CBoC)
#CyberSecurity talent shortage on the radar of government, business: http://www.cbc.ca/news/canada/ottawa/cybersecurity-talent-shortage-1.3831541 … via @CBCOttawa #cyber #infosec

CBC News
1.5 million cybersecurity professionals needed globally by 2020, Ottawa conference hears

Kaspersky Lab
Microsoft fingers #Sofacy as actors behind #0day attacks via @Mike_Mimoso https://kas.pr/3vbj #zeroday #netsec

The CyberWire
Researchers consider the scope, threat, and mitigation of the Mirai IoT botnet.

Dark Reading
It's Time To Address The Cybersecurity Gender Gap Before It's Too Late

SC Magazine
UK Government launches new National Cyber Security Strategy today

Infosecurity
MI5 Boss Warns of 'Aggressive' Russian Cyber Threat

LAW ENFORCEMENT / APPLICATION DE LA LOI

Yahoo
Elections Yukon refers use of proxy votes to RCMP for investigation

RCMP Alberta
Student's get a closer look at what goes into the making of a cop car. #KidsToWork

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Tonda MacCharles
A devastating story. A son fears father's return, 20 years after watching his mother murdered.

CRCVC
'That's not a human, that's a monster:' Son fears father's return, 20 years after watching mom's murder

Globalnews.ca
A plan to make Naloxone "immediately accessible" in Nova Scotia prisons is underway.

John Howard Society
MUST READ EDITORIAL: The indifference that hurt Adam Capay starts at the top in Canada /via @globeandmail

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

The National
Spike in Calgary's domestic violence rate 'incredibly concerning,' advocate says http://www.cbc.ca/1.3830427

Hakique Virani
And If we charge ppl who MAY or SHOULD have known their actions would result in death.../4

Hakique Virani
In #YEG, #opioids other than bootleg #fentanyl are involved in more deaths this year. How about the dealers or prescribers of those? /3

Hakique Virani
If criminalizing was effective prevention, that'd be one thing. But it isn't. So it's another. A horribly sad case all around. /2

Hakique Virani
I'm no fan of drug dealers, but you can treat many people in trouble w/#addiction for the cost of prosecuting one /1

VICE Canada
Why an accused drug dealer's manslaughter charge sets a bad precedent: http://bit.ly/2fa7RrT

OTHER / AUTRES

CBC News Alerts
PM nominates 6 new Senators, all from Quebec. In past week, 21 vacancies filled. Independent Senators now hold plurality of 44 seats.

Marie-Danielle Smith
Trudeau urged to follow in his father's anti-nuclear footsteps and support UN disarmament treaty http://natpo.st/2fhJPu3 #cdnpoli

INTERNATIONAL

Phil Gurski
Indonesian officials expect IS supporters at rally protesting Jakarta governnor

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

Today's News / Actualités
November 4, 2016 / le 4 novembre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Goodale says CSIS 'taking steps' to comply after court rules it broke law
The New Democrats are calling for "strong, new oversight" of the Canada's spy agency in the wake of a court decision that has found that the organization illegally kept electronic data about people for 10 years. In a news conference on Parliament Hill on Friday, NDP justice critic Murray Rankin called the judgment "very disturbing" and said it reveals "gross abuse of power by Canada's spy agency." (…) Speaking to reporters on Friday about the ruling, **Public Safety Minister Ralph Goodale** said he is taking ***"very***

seriously" the finding that ***"CSIS had failed in its duty to be candid" with the court. "(CSIS) has confirmed to me that it is taking immediate steps to address the court's decision,"*** **Goodale** said. ***"It has blocked all access to, and analysis of, any associated data while it considers its next steps to comply."*** **Goodale** also said he is asking the Security Intelligence Review Committee (SIRC) to "monitor the situation carefully to ensure compliance." SIRC is an independent review body that reports to Parliament on CSIS operations. In a ruling made public on Thursday, Justice Simon Noel said CSIS illegally held on to potentially revealing electronic data about people over a 10-year time period. The court found that the spy agency breached its responsibility to inform the court of its electronic data collection, given that the information was gathered using judicial warrants. CTV News

CSIS metadata breach: Ralph Goodale 'pursuing criticism' with spy agency management - 'I take very seriously the explicit finding ... that CSIS had failed in its duty,' public safety minister says
Public Safety Minister Ralph Goodale suggested today that there may be more fallout for the senior management of Canada's spy agency after a Federal Court decision found CSIS broke the law in failing to destroy potentially sensitive information about Canadians. ***"I take very seriously the explicit finding by [Federal Court] Justice Noel that CSIS had failed in its duty to be candid with the court,"*** he told reporters before entering question period. ***"I will be pursuing that criticism with the executive management of the service,"*** he said. ***"In matters of security and intelligence, Canadians need to have confidence that all the departments and agencies of the government of Canada are being effective at keeping Canadians safe, and equally that they are safeguarding our rights and freedoms, including privacy and the rule of law. "From the service and from the department of justice, a strong and timely remedial plan is required to reassure the Federal Court about the issue of candour,"*** he said. CBC News

Judge slams spy agency for keeping data illegally
Federal Court Justice Simon Noel sharply criticized the domestic spy agency, CSIS, for illegally keeping electronic data on people even though they posed no security threat. Noel said the intelligence service was not truthful with judges who were called on to authorize warrants for its data-collection program. (...) This is the second time in three years that a judge of the Federal Court has ruled that CSIS did not meet its "duty of candour" in applying for wiretaps. So far, no sanctions have been applied. In a similar ruling in 2013, Justice Richard Mosley wondered whether it would take a contempt of court proceeding to ensure that such decisions are taken seriously. (...) At a news conference, the director of CSIS, Michel Coulombe said the agency had stopped accessing and analysing the data, but did not say they would be destroyed. **Public Security Minister Ralph Goodale** said the court's ruling would not be appealed. He said he would discuss it with the security agency's management and that Canadians need to have confidence that all departments and agencies of the government are safeguarding rights and freedoms. Radio-Canada International

Goodale dit que la surveillance du SCRS fonctionne bien et fonctionnera mieux
Dans un jugement rendu public jeudi, la Cour fédérale a statué que le Service canadien du renseignement de sécurité (SCRS) avait manqué à son devoir d'informer le tribunal de ce programme de collecte de données, qui durait depuis 10 ans. Le juge Simon Noël estime que le SCRS aurait dû communiquer ses activités à la cour puisqu'elles ne concernaient pas directement la sécurité nationale. Le **ministre Goodale**, responsable de la Sécurité publique et de la Protection civile, a dit vendredi que le rapport du CSARS et l'intervention de la Cour fédérale sont la preuve que le SCRS est gardé à l'oeil. **M. Goodale** a ajouté que son projet de loi C-22 qui crée un comité de députés et de sénateurs pour surveiller les agences comme le SCRS et la GRC renforcera le système. Ce comité aura accès aux opérations en cours de ces agences alors que le CSARS ne peut que revenir sur le passé du SCRS. Par ailleurs, le **ministre Goodale** a dit avoir rappelé au SCRS son « devoir de franchise » avec les tribunaux. **M. Goodale** n'a pu dire combien de Canadiens ont vu des informations les concernant être stockées pendant 10 ans par le SCRS, mais c'est un nombre « excessif », selon lui. Presse canadienne (Radio-Canada), 1

Le fédéral dit avoir les espions à l'oeil
Ottawa promet d'avoir les espions canadiens à l'oeil à la suite des révélations découlant d'un jugement de la Cour fédérale rendu public jeudi. En point de presse vendredi matin au Parlement, le **ministre de la**

Sécurité publique Ralph Goodale a martelé que le Service canadien du renseignement de sécurité (SCRS) a la responsabilité de respecter la loi. «***Cela est absolument fondamental pour garantir la confiance des Canadiens»,*** a-t-il déclaré. Interrogé à savoir si des fonctionnaires seront congédiés, **M. Goodale** s'est toutefois gardé de répondre directement à la question. ***«Je discuterai avec les gestionnaires du SCRS pour savoir comment ils comptent réagir au jugement en consultation avec le ministère de la Justice»***, a-t-il offert. (…) **Ralph Goodale** dit avoir été mis au courant de «l'ampleur du problème il y a quelques semaines», après avoir reçu une version préliminaire du jugement. Le **ministre Goodale** a voulu se faire rassurant, en rappelant que le Parlement souhaite bientôt mettre sur pied un comité pour surveiller les agences de sécurité. Ce comité parlementaire doit toutefois avoir plus de dents que ne le prévoient actuellement les libéraux de Justin Trudeau, a signalé le NPD. «Je pense que les Canadiens devraient être inquiets que l'agence de sécurité nationale ait menti devant la cour. C'est extrêmement préoccupant», a souligné Matthew Dubé. «Quand les agences demandent aux élus d'avoir plus de pouvoirs, le minimum qu'ils doivent faire c'est de gagner la confiance du public, et ils l'ont perdue selon moi avec un tel comportement.» Vendredi, le **ministre Goodale** a confirmé qu'il était ouvert à modifier la loi afin de rendre légal la conservation et l'utilisation des données connexes par le SCRS. TVA Nouvelle

Surveillance de journalistes: pas d'assurances sur le passé à Ottawa
Si aucune surveillance de journalistes ne se produit ***«actuellement» au niveau fédéral, le gouvernement Trudeau n'a pas demandé ni obtenu l'assurance de la GRC et du SCRS que les corps policiers fédéraux n'ont pas mis des journalistes sous surveillance au cours des cinq dernières années. «L'enjeu, c'est que ce qui se passe maintenant»,*** a dit le **ministre fédéral de la Sécurité publique Ralph Goodale** en point de presse ce matin à la Chambre des communes. Le gouvernement Trudeau n'a pas l'intention de demander à la Gendarmerie royale du Canada (GRC) et au Service canadien du renseignement de sécurité (SCRS) si des mandats de surveillance ont été émis ou si des journalistes ont été surveillés au cours des cinq dernières années. ***« L'enjeu, c'est que ce qui se passe maintenant, et nous pouvons offrir l'assurance que ce genre d'activités ne se produit pas actuellement. Je n'ai pas connaissance de choses qui se sont produites quand nous ne formions pas le gouvernement du Canada »***, a dit le **ministre Goodale.** Le gouvernement Trudeau a indiqué avoir reçu l'assurance cette semaine qu'aucune journaliste n'est surveillé «actuellement» par les corps policiers fédéraux. En réponse à une question en point de presse ce matin, le **ministre Goodale** a précisé que cette assurance des corps policiers fédéraux comprend seulement la situation actuelle. Au Québec, la Sûreté du Québec a confirmé cette semaine avoir surveillé une demi-douzaine de journalistes au cours des dernières années, certains comme le journaliste Alain Gravel (Radio-Canada) pendant plusieurs années (2008 à 2013 dans son cas). ***«La réponse, autant de la GRC que du SCRS, est que rien de la sorte ne se produit actuellement. L'enjeu au niveau fédéral n'est pas le même qu'au Québec, dit le ministre Goodale. [...] C'est la responsabilité du directeur du SCRS de répondre aux questions opérationnelles. Vous allez sur une pente très dangereuse quand vous invitez les politiciens à aller dans ce domaine.»*** (…) Le **ministre Goodale** qualifie les ***«révélations au Québec»*** sur la surveillance de journalistes de ***« très inquiétantes »*** et a l'intention de ***«réviser [les] balises fédérales en place pour s'assurer qu'elles soient assez fortes et efficaces, et nous sommes plus qu'ouverts à recevoir les représentations et les conseils du public, des organisations journalistiques et le communauté juridique pour savoir s'il faut, le cas échéant, faire des changements à nos lois.»*** La Presse

Broadcast Media / Médias télédiffusés

CTV News provided coverage of the NDP reaction to the Federal Court ruling on CSIS data storage. Rough Transcript

CTV News provided coverage and analysis of Public Safety Minister Ralph Goodale's press conference in response to a Federal Court decision on CSIS data retention. Rough Transcript

TOP STORIES / MANCHETTES

Goodale says CSIS 'taking steps' to comply after court rules it broke law
The New Democrats are calling for "strong, new oversight" of the Canada's spy agency in the wake of a court decision that has found that the organization illegally kept electronic data about people for 10 years. In a news conference on Parliament Hill on Friday, NDP justice critic Murray Rankin called the judgment "very disturbing" and said it reveals "gross abuse of power by Canada's spy agency." (…) Speaking to reporters on Friday about the ruling, **Public Safety Minister Ralph Goodale** said he is taking ***"very seriously"*** the finding that ***"CSIS had failed in its duty to be candid" with the court. "(CSIS) has confirmed to me that it is taking immediate steps to address the court's decision,"*** **Goodale** said. ***"It has blocked all access to, and analysis of, any associated data while it considers its next steps to comply."*** **Goodale** also said he is asking the Security Intelligence Review Committee (SIRC) to "monitor the situation carefully to ensure compliance." SIRC is an independent review body that reports to Parliament on CSIS operations. In a ruling made public on Thursday, Justice Simon Noel said CSIS illegally held on to potentially revealing electronic data about people over a 10-year time period. The court found that the spy agency breached its responsibility to inform the court of its electronic data collection, given that the information was gathered using judicial warrants. CTV News

CSIS metadata breach: Ralph Goodale 'pursuing criticism' with spy agency management - 'I take very seriously the explicit finding … that CSIS had failed in its duty,' public safety minister says
Public Safety Minister Ralph Goodale suggested today that there may be more fallout for the senior management of Canada's spy agency after a Federal Court decision found CSIS broke the law in failing to destroy potentially sensitive information about Canadians. ***"I take very seriously the explicit finding by [Federal Court] Justice Noel that CSIS had failed in its duty to be candid with the court,"*** he told reporters before entering question period. ***"I will be pursuing that criticism with the executive management of the service,"*** he said. ***"In matters of security and intelligence, Canadians need to have confidence that all the departments and agencies of the government of Canada are being effective at keeping Canadians safe, and equally that they are safeguarding our rights and freedoms, including privacy and the rule of law. "From the service and from the department of justice, a strong and timely remedial plan is required to reassure the Federal Court about the issue of candour,"*** he said. CBC News

CSIS law-breaking shows need for stronger parliamentary oversight: NDP
The NDP says revelations that Canada's lead spy agency illegally kept sensitive data for years underscores the need for stronger parliamentary oversight. The New Democrats are pushing for changes to a bill that would create a committee of parliamentarians to keep an eye on the Canadian Security Intelligence Service and other spy services. NDP MP Murray Rankin says the proposed model would allow the government to arbitrarily deny crucial information to the committee. A Federal Court judge says CSIS violated the law by keeping potentially revealing electronic data about people who posed no security threat over a 10-year period. Canadian Press (Chronicle-Herald, Metro News, 680 News, Global News, Huffington Post)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

The Beast is alive - How the fire that tried to destroy Fort McMurray is still burning near the Saskatchewan border
Six months after it sent the population of Fort McMurray fleeing, the wildfire known as MWF-009 is still burning. The fire can no longer be seen visually; there is no smoke or open flames. But in a remote section of Alberta and Saskatchewan far from the city it tried to destroy, the blaze is still being carefully watched. "Just given the size, scope and complexity of the Fort McMurray wildfire, firefighters will continue to monitor the area," said Laura Stewart, Wildfire Information Officer with the Government of Alberta. Known by firefighters as the Horse River Fire, it is so named because the fire began May 1 near a small waterway known as Horse River. The fire was not an act of nature. By June, fire investigators were definitively saying that somebody who visited the Horse River trail system on the Sunday before the evacuation was responsible. However, it is not known what exactly sparked the fire. Given the searing, tinder-dry conditions on May 1 in Northern Alberta, it could have been caused by anything from a discarded cigarette to the spark from an ATV. Just two hectares in size when it was first spotted, it only

took three days to expand into 10,000 hectares and swoop into Fort McMurray. The blaze has been declared "under control" since July 4. Nevertheless, in the months since, the fire has entered a kind of hibernation that may allow it to survive the winter. The phenomenon is known as a "holdover fire." Long after the flames and smoke of a out-of-control wildfire have died down, the fire persists by smouldering underground. National Post

Les municipalités se penchent sur le transport ferroviaire de matières dangereuses
Des représentants de municipalités du Nouveau-Brunswick et du Québec rassemblés vendredi, à Edmundston, réfléchissent à la sécurité ferroviaire dans le contexte du transport de matières dangereuses. Il y a trois ans, l'explosion de wagons de pétrole à Lac-Mégantic et l'incendie qui a suivi ont causé la mort de 47 personnes. D'importants déraillements se sont aussi produits ces dernières années à Edmundston et à Plaster Rock, au Nouveau-Brunswick, mais sans faire de victime. « On s'est dit qu'il fallait rassembler les gens pour faire une journée de réflexion sur l'état de la situation, explique Luc Desjardins, maire de Petit-Rocher et président de l'Association francophone des municipalités du Nouveau-Brunswick. Premièrement, c'est une mise au point. On veut savoir où c'est rendu et où ça s'en va. C'est plutôt un partage d'informations. » Les gouvernements ont resserré les règles du transport ferroviaire depuis ces accidents, souligne Luc Desjardins. Il pourrait y avoir d'autres changements à venir, car, dit-il, des comités municipaux au pays formulent toujours des recommandations pour améliorer la sécurité. Les municipalités et les organisations des mesures d'urgence veulent aussi mieux se préparer à répondre aux besoins en cas d'accident. Radio-Canada

Frustration growing over lack of financial assistance for Sydney flood victims
People whose homes were hardest hit by flooding in Cape Breton on Thanksgiving are being told their cheques will soon be in the mail, but most say they won't be satisfied until the money is in their pockets. On Thursday, those most affected were meeting again with CBRM Mayor Cecil Clarke. Many wondering when they will start receiving more money through the province's disaster financial assistance program. "Now, we're at a critical point. A lot of people are finding that time has moved on and pressures are mounting, and costs are mounting," says CBRM Mayor Cecil Clarke."We're trying to respond jointly with the province so their assistance can flow as fast as possible." On Thursday, the Nova Scotia government said many property assessments are being finalized and payment is the next step, but it's still unclear when that will happen. "Once people know what their market value is for their home, what the value of the contents that they lost is for the home, then they can move on to really getting the individual conversations going with EMO, with the provincial government, to figure out what exactly that settlement is going to look like," says Transportation Minister Geoff MacLellan. CTV News

Cause of British Airways emergency landing at YVR still a mystery as plane returns to service - Flight diverted to Vancouver after crew and passenger became ill due to a 'strong noxious smell'
The British Airways aircraft that made an emergency landing in Vancouver last week has returned to service — even though authorities were never able to find the exact cause of the problem. Initial reports suggested smoke in the cabin, but that was never the case, according to Bill Yearwood of the Transportation Safety Board. "British Airways and Airbus have exhausted their techniques to find any clues or cause of the reported and apparent odour, [but] there is no definitive answer," he said. According to a Transport Canada incident report, flight BA286 bound from San Francisco to London was diverted to Vancouver for an emergency landing after several cabin crew members and a passenger became ill due to a "strong noxious smell" on the upper flight deck. The aircraft — an Airbus A380, the largest passenger jet in the world — was carrying 388 passengers at 25 crew. All 25 crew and one passenger were hospitalized when the plane landed, and were later released with no apparent lasting illness. The flight was initially diverted to Calgary, but then diverted again to Vancouver, where the airport is better equipped to handle an A380. CBC News

UPDATED: Hunting guide found in good health
The Bay St. George RCMP advised at 9:10 a.m. today the search for the lost hunting guide in the Jeffrey's area of has ended with a fantastic outcome. The 49 year old resident of Codroy Valley, NL., walked out of the woods and appears to be in good health. A helicopter from the 103 Search and Rescue Squadron is still en route and may assist with an extraction of the adult male. St. John's Telegram; CBC News

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

CSIS law-breaking shows need for stronger parliamentary oversight: NDP
The NDP says revelations that Canada's lead spy agency illegally kept sensitive data for years underscores the need for stronger parliamentary oversight. The New Democrats are pushing for changes to a bill that would create a committee of parliamentarians to keep an eye on the Canadian Security Intelligence Service and other spy services. NDP MP Murray Rankin says the proposed model would allow the government to arbitrarily deny crucial information to the committee. A Federal Court judge says CSIS violated the law by keeping potentially revealing electronic data about people who posed no security threat over a 10-year period. Canadian Press (Chronicle-Herald, Metro News, 680 News, Global News, Huffington Post)

What Snowden Had to Say at the McGill Videoconference
Thousands of people lined up on the McGill campus Wednesday night waiting hours for a chance to be part of a videoconference with Edward Snowden. (…) We can't trust intelligence officials to respect the spirit of the law; in fact, we can't even trust them to respect the law itself, argued Snowden. Intelligence gathering programs have broken the law more than once, he reminded, often without consequences. "What we can do," he continued, "is put processes in place to ensure that we don't have to." He believes the key of these processes is an independent judicial authority able to oversee intelligence gathering operations and prosecute them when needed. "Canada actually has the weakest intelligence oversight out of any major western country." "Now they're not the most aggressive," he conceded, "they don't have the largest scale, but…. no one is really watching." The powers of the Canadian Security Intelligence Agency (CSIS) have drastically increased in the last 15 years. Law C-51, in particular, allows them to decide under any motive – however far-fetched – who constitutes a threat to national security and can thus be spied on. "The current Prime Minister did campaign to reform [C-51] and has failed to do so," reminded Snowden. The resources to oversee the CSIS, meanwhile, have decreased. The office of the Inspector General, which used to be a major part of it, was simply cut by Stephen Harper. This left the Security Intelligence Review Committee (SIRC) as the sole entity reporting to parliament on intelligence agencies. Its members are politically appointed. CSIS is not the only intelligence gathering agency. The Canadian Border Security Agency, Global Affairs Canada and the National Defense Department all have the power to infringe on the rights of people, including the right to privacy, in certain circumstances and there is no credible authority overseeing them. Retired Deputy Director of Foreign Intelligence Kurt Jensen pleaded for changing this situation in an article published last January. "Remember the old adage of who will watch the watchers? In Canada the answer is no one," he wrote. Forget the Box

Three New Scandals Show How Pervasive and Dangerous Mass Surveillance is in the West, Vindicating Snowden
An opinion piece state, 'While most eyes are focused on the presidential race between Hillary Clinton and Donald Trump, three major events prove how widespread, and dangerous, mass surveillance has become in the west. Standing alone, each event highlights exactly the severe threats which motivated Edward Snowden to blow his whistle; taken together, they constitute full-scale vindication of everything he's done. Earlier this month, a special British court that rules on secret spying activities issued an emphatic denunciation of the nation's domestic mass surveillance programs. The court found that "British security agencies have secretly and unlawfully collected massive volumes of confidential personal data, including financial information, on citizens for more than a decade." (…) On Thursday, an even more scathing condemnation of mass surveillance was issued by the Federal Court of Canada. The ruling "faulted Canada's domestic spy agency for unlawfully retaining data and for not being truthful with judges who authorize its intelligence programs." Most remarkable was that these domestic, mass surveillance

activities were not only illegal, but completely unknown to virtually the entire population in Canadian democracy, even though their scope has indescribable implications for core liberties: "the centre in question appears to be the Canadian Security Intelligence Service's equivalent of a crystal ball – a place where intelligence analysts attempt to deduce future threats by examining, and re-examining, volumes of data."" The Intercept

Laws on protecting journalists' sources not being followed, says retired justice John Gomery
The creation of a commission of inquiry into spying by Quebec police on journalists is a necessary step, but the public shouldn't expect it to solve the problem, says retired Quebec Superior Court justice John Gomery. Gomery, who led the commission of inquiry into the federal sponsorship scandal between 2004 and 2006, said such bodies are essential to help restore public confidence in the rule of law. "A public inquiry is a good way to find out what happened, but as far as developing policy for the future, I'm not sure it's the best way to go," he told CBC News. Gomery said one of the commission's useful functions will be to shed light on the role played by justices of the peace in the growing scandal. CBC News

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

End November 10 entry visas exemptions in Canada
All travelers from countries normally exempt from entry visas to Canada, as European citizens, must present from November 10 to the Canadian border police an electronic travel authorization (AVE). (…) For Immigration Minister John McCallum, the electronic travel authorization "increases the safety of Canadians by enabling us to verify the eligibility of travelers before they take their flight and to stop immediately those territory forbidden to travel to Canada. " The Canadian government, however, had difficulties in setting up the platform to issue the document electronically, requiring several months to postpone the requirement for passengers to be provided on arrival at the border. In September, Canada was again rejected this requirement, he said, "give travelers and airlines more time to prepare for the changes." According to the Department of Immigration, 2.3 million AVE have been issued since 1 August 2015 and is valid for 5 years. US citizens or passengers of a plane calling impromptu in Canada are exempt from this AVE. Silver Times

Canada issues 54% more work permits to U.S. residents in 2016 in face of heated election
Canadian work permits for highly skilled workers from the United States jumped in the first half as companies lured applicants with the country's calm political climate in the face of a raucous U.S. election. Canadian immigration data showed new work permits issued to U.S. residents jumped 53.8 per cent in the first eight months of 2016 from the same period last year, though renewals were down. (…)Separate government data also showed permits for international students looking to attend Canadian schools jumped in the first quarter to 42,737, up 42 per cent from a year earlier. In the second quarter, student permits jumped 63 per cent, to 56,329. While the government doesn't ask why students choose Canada, consulting firm Intead, which advises postsecondary institutions looking to recruit international students, warned in June that a Trump win could hit U.S. enrollment numbers. Reuters (BNN)

Second foreign student sent home after gun threat
The second international student under investigation related to an alleged gun threat at Seycove secondary has been sent back to his home country. North Vancouver school district confirmed Wednesday that his student visa had been revoked and he has flown home under the supervision of the homestay agency acting as his custodial guardian. Another student was arrested on Oct. 25 when he allegedly threatened to "bring a gun to school and do harm to a teacher." The student was sent home less than 24 hours later. Later, on Oct. 26, police recovered a gun somewhere off of school grounds. Police had requested charges of possession of a prohibited firearm and uttering threats for the second boy, although the Crown declined. "Because Crown didn't approve charges, there is no more criminal investigation happening. It will still try to be determined how the gun surfaced," said Cpl. Richard De Jong, North Vancouver RCMP spokesman. "We still have a concern, obviously as police, how a young person can have access to a gun." Police could confirm that the gun did not come from any of the homestay families. All other aspects of the investigation aren't being disclosed, De Jong said. Both students were subject to background checks by the school district as well as screening by the Canada

Border Services Agency and Citizenship and Immigration Canada, according to Deneka Michaud, North Vancouver school district spokeswoman. North Shore News

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

NIL

LAW ENFORCEMENT / APPLICATION DE LA LOI

Stolen semi found stuck in slough with murder suspect inside: Saskatchewan RCMP
A 26-year-old man is now facing a second-degree murder charge after RCMP launched a suspicious death investigation in Saskatchewan. At around 4:20 a.m. CT on Wednesday, RCMP received a complaint about a semi that had been stolen from a farm yard north of Kerrobert, Sask. The complainant also provided a description of a suspect. A short time later, another complaint was received by police about a sudden death at a residence in Kerrobert. Members attended and found Johan Klassen Sr., 53, deceased. Investigators determined the death was suspicious in nature and identified a person of interest who matched the previous description given. Kindersley RCMP said they immediately began searching for the semi and quickly found it stuck in a slough northwest of Luseland, Sask. The vehicle was in approximately 1.2 metres of water, about 30 metres from shore. The man inside the semi refused to exit. RCMP immediately contained the scene to ensure public safety and the emergency response team (ERT) was deployed to the scene to assist. At around 2 p.m., the man was taken into custody without incident. Sughar Daily; CTV News; 650 CKOM; Star Phoenix

Bomb threat Romeo jailed, ordered to pay $89,100
P.E.I. man who called in a bomb threat to Walmart in Charlottetown because he wanted his girlfriend to get the day off was sentenced to 60 days in jail and ordered to pay $89,100 in restitution. Logan Richard Arsenault, 19, appeared before Chief Judge Nancy Orr in provincial court in Charlottetown Friday after previously pleading guilty to calling in the bomb threat. In handing down the sentence, Orr said we don't live in a society where that type of behaviour is considered a joke. "It's never been a joke," she said. Arsenault used a payphone in Stratford on Aug. 2 to call in the bomb threat, saying he knew people who worked at the store and they needed to get out. The store was evacuated and closed for about six hours while Charlottetown police, an RCMP explosives unit, Island EMS and firefighters responded. NG News

Man charged for gym mischief
A man has been arrested in relation to a break-in that ended in the vandalism of a local school gymnasium. The incident took place in the early morning of Aug. 29, when a man entered Lakeland Ridge School, and was caught on surveillance video pulling a fire extinguisher off the wall. He then used the extinguisher to spray down the school gym, causing what the RCMP noted as "several thousands of dollars' worth" of repairs made necessary by the damage. A suspect turned himself into police on Oct. 29. Charges are pending against the 19-year-old man, from Sherwood Park, for one count of mischief under $5,000. He is scheduled to appear in Sherwood Park Provincial Court on Wednesday, Nov. 30 at 9:30 a.m. The man's identity has not been released by Strathcona County RCMP. Sherwood Parknews

Lawrencetown man arrested after indecent act complaints
A Lawrencetown man has been arrested and charged after RCMP received complaints about a man committing indecent acts in front of children. Annapolis County District RCMP started an investigation after receiving a complaint Tuesday afternoon about a man masturbating while fully undressed in front of a window as children walked by. A second similar complaint was received at about 8:30 the next morning. Assisted by the RCMP Internet Child Exploitation Unit and RCMP Technological Crime Unit, officers executed a search warrant at a Sunvalley Street residence. They arrested Chester Terry Thibodeau and charged him with three counts of committing an indecent act. Thibodeau has been remanded into custody after appearing in Annapolis Royal Provincial Court Thursday. He is scheduled to return Nov. 14 for a bail hearing. Chronicle Herald; Metro News

RCMP investigating separate indecent act incidents
A woman was shaken up but not injured when she was grabbed while jogging in Spruce Grove Thursday afternoon. RCMP said the woman was running near the soccer field on Heatherglen Drive around 4:30 p.m. when she was approached by the male suspect. She told police he talked to her briefly before grabbing her buttocks and shoulder and touching her face. He's described as 5'10", with a medium build and dark skin. The victim said he was wearing a black Nike jacket, black pants, a black hat, and thick black sunglasses. iNews 880

Twilling ate RCMP Members Prepare Time Capsule
Members of the Twillingate RCMP detachment are creating a time capsule as they prepare to move into a new building in 2017. Constable Greg Bowie thought of the idea as a way to show future residents of the area a brief overview of the RCMP in Twillingate in 2016, as well as some information about the town that they serve. In the not too distant future the Twillingate RCMP will be ready to move from what is currently the oldest detachment in Newfoundland, to the newest. The idea of a time capsule seemed quite fitting for the occasion. Currently, the capsule will include a letter from Bowie with a brief history about himself and the other members he serves with. He plans to also include a current RCMP shoulder flash, a 2016 loonie, RCMP pin as well as newspaper clippings, both local and national from present day. They would also like to include photos or small mementos reflecting current life in Twillingate/Durrell. Bowie said the capsule is going to be very compact, as it will be packaged in a coffee can, therefore any donated items need to be small enough to fit inside. Pilot NL

Police seize drugs, handgun, cash during Sooke raid
Police seized drugs, a handgun, body armour and cash during a raid on a suspected drug house in Sooke. Sooke RCMP teamed up with the RCMP Island District General Investigation Section to execute a search warrant on a home in the 6700 block of Eustace Road in Sooke early Thursday. The raid followed a several-month investigation into drug trafficking. Police said they seized several ounces of cocaine, several pounds of psylocibin mushrooms, drug trafficking paraphernalia, a pistol and loaded magazine, a ballistic vest and more than $7,000 in cash. A 30-year-old man was arrested as a result of the investigation, and faces charges of possession of a controlled substance for the purpose of trafficking, unsafe storage of a restricted weapon, unlawful possession of body armour, and possession of prohibited weapons. The suspect remains in custody, but is expected to be released on bail. "This joint investigation has curtailed the activity of a high volume, and diversified drug trafficker who deals primarily to other dealers and users within the community of Sooke." said Staff Sgt. Jeff McArthur. Sooke News

Broadcast Media / Médias télédiffusés

CBC News interviewed reporter Mark Kelley on his Fifth Estate report on police use of body cameras. Rough Transcript

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Woodville arena attacker will spend at least one more year in halfway house
The man who viciously attacked a four-year-old girl at the Woodville arena in 2010 is still considered to be a moderate to high risk of re-offending and will spend at least one more year at a halfway house, according to records obtained from the Parole Board of Canada. A recommendation for overnight leave privileges was also brought - and rejected - by the board. Tyson Leeder, now 23, pled guilty to aggravated assault, forcible confinement and invitation to sexual touching in October of 2011 after he abducted the girl from the washroom at the arena where he worked. Leeder's sentence officially ended Dec. 1, 2015, according to the Correctional Service of Canada, but on Oct. 26, 2016, the Parole Board of Canada recommended a residency condition - for the second time - on his Long Term Supervision Order for another year. The order, which started as soon as his sentence ended, will remain in place until Nov. 30, 2025. Kawartha Lakes This Week (myKawartha.com)

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Calgary police support province's move towards safe consumption sites
The Calgary Police Service is putting their support firmly behind the province's decision to explore the use of supervised safe consumption sites to combat the ever-growing opioid problem in Alberta. Staff Sgt. Martin Schiavetta said CPS will act as a supporter as the sites are set up. He said it will be one service in what he hopes is a multi-faceted approach in dealing with the issue. Metro News

For victims of domestic violence, aid organizations can be lifelines
Note to readers: Unless otherwise indicated, the names of the women who shared their stories of abuse for this article have been changed. As well, one of the counsellors is identified only by her first name. "On average, a woman will try to leave an abusive partner seven times before she leaves for good," Karina, a counsellor, tells the women gathered around two tables in the meeting room at Auberge Transition, one of about 20 Montreal-area shelters for women and children who are fleeing abusive relationships. Karina is leading a "café-rencontre" — a weekly session for residents of the shelter. Today, some former residents have come to the café-rencontre, too, to share their stories and offer hope to the new arrivals. Montreal Gazette

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

CBC adds oldest Manitoba case so far to MMIW database: 56 years later, still no answers: Flora Muskego was found frozen to death in 1960 near Norway House
Flora Muskego was found frozen to death in a snow drift near Norway House First Nation 56 years ago. Her family is still wondering what happened to the 22-year-old on Thursday, December 9, 1960. There was a small newspaper clipping from 1960 in the Winnipeg Free Press stating when Muskego was found and that she was last seen just the day before. It also said a coroner's inquest was pending on the police investigation. Muskego is buried in Norway House today. As part of continuing CBC's coverage of missing and murdered Indigenous women and girls, Muskego is the latest case to be added to its database and oldest case uncovered by CBC in the province of Manitoba. Sylvia Grier, 64, of Saskatoon remembers her aunt. "I remember how beautiful she was," said Grier, also a Norway House community member. At the young age of eight, Muskego introduced Grier to make-up. Grier remembers her aunt wearing beautiful clothes and always having nice shoes. CBC News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Ottawa police raid pot shops across city
Ottawa police have arrested at least one person during Friday morning raids at marijuana dispensaries across the city. The raids at the Wee Medical Dispensary Society shop at 358 Rideau Street, and the Green Tree Medical Dispensary shops at 290 Montreal Road, 256 Bank Street and 352 Preston Street come following a volume of complaints about the growing number of dispensaries across the city. One person was seen being escorted out of the shop on Montreal Road by police and shuttled into a cruiser. Ottawa police tweeted that there were operations underway "at several locations in Ottawa" but refused to comment further "so as not to jeopardize ongoing investigations." The federal government has promised to introduce legislation to legalize marijuana by the spring of 2017 but possession, production and trafficking of marijuana remains illegal. CBC News; Ottawa Sun

BC doctors, police worried about uptick in deadly pot-related crashes
BC's biggest doctors' group is worried about what will happen on our roads once marijuana is legalized in Canada, pointing to a jump deadly pot-related crashes south of the border. The federal government has promised to make the move by next spring. "In Washington State, fatal crashes among drivers who tested

positive for marijuana doubled from 8 per cent in 2013 to 17 per cent in 2014. In Colorado the number of drivers in fatal crashes who tested positive for marijuana without other drugs in their system tripled between 2005 and 2014 from 3.4 per cent to 12.1 per cent," writes Chris Rumball with Doctors of BC. Rumball — an emergency room doctor in Nanaimo — calls the statistics "sobering" in an opinion piece published this week in the BC Medical Journal, calling for a "clear-headed" assessment of the impact of legalization on road safety. News 1130

PUBLIC SERVICE / FONCTION PUBLIQUE

Millennials demand better treatment to join government ranks
Nicolino Frate spends his day job as a director at the Canada Revenue Agency, but on the side, this millennial is trying to make building a career in government an attractive concept to members of the digital generation. After hours, Frate and 31 fellow public servants from more than a dozen different departments across the country work on a project called Leaders GC — a monthly social media chat that hosts government executives to talk about what they do, on Twitter. "Millennials do make up a good percentage of our followers," said Frate, who is in his early 30s. "You have to show people what your environment is like so that they have an interest to actually join, and actually come in to the public service." But Frate's Twitter chats notwithstanding, governments tend to be "woefully behind" when it comes to digital transformation and turning on millennials, according to a recent report out of IBM global business services. Millennials — people between 18 and 35 — are replacing baby boomers in the workforce and after growing up digital, this new cohort has different expectations. The next generation of public service leaders is demanding certain conditions when it comes to joining the federal government workplace, according to Beth Bell, vice president of the public sector for IBM. CBC News

OTHER / AUTRES

NIL

INTERNATIONAL

N.Y. authorities warned of terror threat around U.S. election
Federal officials have warned New York City authorities about possible attacks by the al Qaeda militant group around Election Day, putting local law enforcement on alert the weekend before Tuesday's vote, officials said on Friday. Both the New York Police Department (NYPD) and the Port Authority of New York and New Jersey were given the information, the local agencies said. "We are continuing with the high level of patrols at all of our facilities that we have had in place for some time now," said spokesman Steve Coleman of the Port Authority, which operates airports, tunnels and bridges around the New York City area. He declined to offer specifics of the warning. The NYPD said the threat report lacked specifics and was still being assessed. "We are aware of the information. We have been working with the FBI through the Joint Terrorism Task Force and our Counterterrorism and Intelligence Bureaus," the NYPD said. Reuters

Sanglant attentat en Turquie après l'arrestation de 12 députés prokurdes
Le premier ministre turc, Binali Yildirim, a précisé qu'un séparatiste du Parti des travailleurs du Kurdistan (PKK) était au nombre des tués. L'attaque a été imputée au PKK, classé organisation terroriste par le gouvernement turc, mais aussi par les États-Unis et l'Union européenne. L'explosion s'est produite dans le quartier de Baglar, près d'un commissariat de police où sont gardés à vue plusieurs des élus du HDP arrêtés la veille dans le cadre d'une enquête antiterroriste, a-t-on appris de sources proches de la sécurité. Au total, douze députés du HDP ont été arrêtés, suscitant la préoccupation de l'Union européenne déjà inquiète de l'évolution de la société turque depuis le coup d'État manqué du 15 juillet dernier. Les autorités turques, qui leur reprochent d'avoir refusé de témoigner dans des dossiers liés à « la propagande terroriste », assurent que la loi a été respectée. « Les parlementaires qui ont été arrêtés ont ignoré la loi », a expliqué le ministre de la Justice, Bekir Bozdag, cité par l'agence de presse Anatolie.

« Ils ont reçu une invitation mais ne se sont pas manifestés. Quelle autre solution avions-nous? Les faire venir de force. » Reuters (Radio-Canada)

US intelligence 'warns of possible Al-Qaeda attacks' on day before election
With just a handful of days before the US presidential election, a potential threat has reportedly emerged in the form of possible Al-Qaeda plot to target New York, Texas and Virginia. Much of the run-up to polling day has until now been dominated by coverage about possible attempts to intimidate voters by white supremacists and reports of efforts to keep certain communities, particularly African Americans, from casting their vote. But CBS News said it had learned of a potential threat that could be timed for 7 November, the day before millions of Americans cast their vote after what has been a bitter, ugly election battle. UK Independent

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

CTVCalgary
Goodale says CSIS 'taking steps' to comply after court rules it broke law: https://t.co/pKcO9FBpAj

Claire_Wahlen
.@RalphGoodale is speaking now in the House of Commons re: #CSIS. He will be having #SIRC follow along, but let's be serious, LOL #cdnpoli

Claire_Wahlen
Goodale won't commit to any heads rolling, suggest they'll wait to see what SIRC says. I expect little in way of major player change.

Claire_Wahlen
On the bright side though, dim as it is, Goodale insists he will be speaking with senior management at #CSIS for this shitstorm

I_stone
Goodale says he welcomes the federal court decision - says its timely as it comes in midst of security consultations #cdnpoli

I_stone
Goodale doesn't answer directly if anyone will be fired or if there will be an inquiry. Repeatedly says decision will be followed

I_stone
CSIS and all security agencies need to comply w law, Goodale says. Judge made clear what law is

I_stone
Goodale says he takes very seriously the finding that CSIS failed in its duty to be truthful w court

I_stone
Goodale asked if he knew about this - says its in a report that was filed in Parl on Jan 28

Justin_Ling
"A strong and timely remedial plan is required to assure the court on the issue of candour," says Goodale.

Justin_Ling
Goodale says he only because aware of this massive CSIS spying campaign in early October when this judgement came out. Wow.

Justin_Ling
"The review process, in terms of SIRC, has worked," says Goodale. Which is wooooboy quite a whopper.

chrishallcbc
Goodale asked if anyone will be fired for failing to inform court that data retained... says he will discuss matter with CSIS execs.

chrishallcbc
Goodale says he will pursue with CSIS execs the failure to properly inform court that data retained #hw

ShirleeEngel
Goodale says Canadians need to have confidence all agencies being effective at keeping Canadians safe while safeguarding freedom #cdnpoli

NATIONAL SECURITY / SÉCURITÉ NATIONALE

GgNewsCA
Statement - CSIS Director statement regarding decision of the Federal Court - Canada NewsWire (press release) http://ift.tt/2fp59hk

globalnews
WATCH: NDP blasts "gross abuse of power by Canada's spy agency" following judge's ruling on CSIS

HuffPostCanada
TW: CSIS law-breaking underscores need for oversight: NDP http://huff.to/2elFuoV #cdnpoli

MattDube
Liberal government must reveal details surrounding CSIS ruling https://t.co/2oWaHxmzOD

vicecanada
There's a secret Canadian spy database that we just found out about: http://bit.ly/2eZuzF3

vicecanada
Edward Snowden speaks out on Quebec police surveillance of journalists: http://bit.ly/2elaXrc

mtlgazette
Police surveillance scandal: Judge orders columnist's phone records sealed https://t.co/leQSNle2zU

LP_LaPresse
Surveillance policière: 50 % des Québécois contre la commission, selon un sondage https://t.co/LoufXxml2Q

StewartBellNP
A year ago today Canadian army veteran John Robert Gallagher died in Syria. Reposting the story of how it happened. https://t.co/G3KzpdHENA

globalnews
WATCH LIVE: Whether national security agencies should monitor Canadians expected to dominate question period https://t.co/wGOloBFT4t

cath_cullen
Timely: National security was perceived as a Liberal strength in the government's own poll of Canadians. More here: https://t.co/1eh7DOCXv8

CYBER SECURITY / CYBERSÉCURITÉ

GetCyberSafe
Remember to change your clocks on Sunday! It's a good time to check and update your privacy settings too: https://www.getcybersafe.gc.ca/cnt/prtct-yrslf/prtctn-dntty/scl-ntwrk-en.aspx …

motherboard
Inside Anonymous' "civil war" over its fight against ISIS, as some members resist aiding intelligence agencies http://bit.ly/2fLn3ih

SCMagazine
MySQL bugs could allow full server compromise https://t.co/v1tAvnmR92

OpenCanada
"We need to save the Internet from the Internet of Things." Why this poses a unique challenge for policymakers: https://t.co/KqeUdOX1jb

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

CBCTheNational
Ontario doctors investigated for large opioid prescriptions http://www.cbc.ca/1.3834874

mtlgazette
For victims of domestic violence, aid groups can be lifelines https://t.co/iJQXNMsp5l

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

GgNewsCA
CBC adds oldest Manitoba case so far to MMIW database: 56 years later, still no answers https://t.co/2vhVopVUOh

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

ctvottawa
Ottawa Police are conducting city-wide raids of marijuana dispensaries. There are 17 illegal dispensaries in the city. #ottnews

joannelaucius
#ottcity Police move into Green Tree cannabis dispensary with more equipment.

INTERNATIONAL

ReutersUS
New York authorities warned of terror threat around U.S. election: http://reut.rs/2elwEaF

Independent
US intelligence 'warns of possible Al-Qaeda attack' on Tuesday http://ind.pn/2fjWEVJ

SkyNews
Explosion hits mainly Kurdish city of #Diyarbakir in southeast #Turkey

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

Today's News / Actualités
November 10, 2016 / le 10 novembre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

La GRC a-t-elle espionné des journalistes?
Sur un ton qui se voulait rassurant, le Commissaire de la GRC, Bob Paulson, le premier ministre, Justin Trudeau, et le **ministre de la Sécurité publique, Ralph Goodale**, ont tous répondu que ça ne se faisait pas actuellement. ***« Mais allez-vous vérifier les cinq dernières années? »*** a lancé un journaliste au **ministre Goodale.** Ce à quoi le **ministre a répondu*:« Regardez, l'enjeu c'est ce qui se passe maintenant et je peux vous assurer que ce type d'activité ne se produit pas maintenant. Je ne suis pas au courant de choses qui se sont passées quand on ne formait pas le gouvernement du***

Canada. » Face à cette absence de réponses, nous avons demandé directement à la GRC si, par le passé, elle avait fait de la surveillance des journalistes, qu'il s'agisse de surveillance des relevés des appels téléphoniques ou de surveillance physique (filature) ou autre. Par courriel, la GRC a répondu notamment : « Les cas où des enquêtes de la GRC concernant des journalistes ont eu lieu sont extrêmement rares, et le cas échéant, celles-ci sont menées avec des paramètres de surveillance étroite selon les directives ministérielles. » Radio-Canada

TOP STORIES / MANCHETTES

Obama says Trump meeting was 'excellent'
In a cordial beginning the transfer of power, President Barack Obama and President-elect Donald Trump met at the White House Thursday. Obama called the 90-minute meeting "excellent," and his successor said he looked forward to receiving the outgoing president's "counsel." (…) In Washington, Trump's scant transition team sprang into action, culling through personnel lists for top jobs and working through handover plans for government agencies. A person familiar with the transition operations said the personnel process was still in its early stages, but Trump's team was putting a premium on quickly filling key national security posts. The person was not authorized to discuss details by name and spoke on condition of anonymity. According to an organizational chart for the transition obtained by The Associated Press, Trump was relying on experienced hands to help form his administration. National security planning was being led by former Michigan Rep. Mike Rogers, who previously worked for the FBI. Domestic issues were being handled by Ken Blackwell, a former Cincinnati mayor and Ohio secretary of state. Trump was expected to consider several loyal supporters for top jobs, including former New York Mayor Rudy Giuliani for attorney general or national security adviser and campaign finance chairman Steve Mnuchin for Treasury secretary. Former House Speaker Newt Gingrich and Tennessee Sen. Bob Corker were also expected to be under consideration for foreign policy posts. Associated Press (ABC)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Slight respite in flooding near Port Alberni but new storm due to hit
Waters of the swollen Somass River near Port Alberni have receded slightly overnight, but the next wave of wet weather is on the way, meaning more flooding is possible on central Vancouver Island. Single lane traffic is moving again on Highway 4 just west of Port Alberni, after the only route to and from Tofino and Ucluelet was closed for several days as the Somass burst its banks. But Environment Canada has issued a special weather statement warning a new system will hammer north, central and western Vancouver Island by Thursday night, dumping as much as 100 to 150 millimetres of rain through Friday. Eleven homes are evacuated on the Tseshaht First Nation and a state of emergency remains in effect, while on the mainland near Pemberton, an evacuation alert continues for homes on the Lil'Wat First Nation and for some properties along the Lillooet River. The River Forecast Centre issued a flood warning for the Lillooet River and its tributaries late Wednesday afternoon as heavy rain and warm temperatures melt recent snowfalls. A Flood watch is also in effect for the Squamish River near Brackendale, north of Vancouver, but forecasters expect waters in most areas to recede through the day, offering a respite before the next storm system hits. Postmedia Network (Vancouver Sun; Metro News); Global News

Important glissement de terrain à Saint-Luc-de-Vincennes
Un important glissement de terrain est survenu tôt jeudi matin, à 7h25, sur le rang Saint-Joseph-Ouest à Saint-Luc-de-Vincennes. Deux résidences ont été évacuées, alors qu'une importante section de terrain s'est détachée pour tomber dans la rivière Champlain, qui serait présentement complètement bouchée. Selon le directeur de la Sécurité civile de la Mauricie, Sébastien Doire, la partie de terrain qui s'est détachée serait de la grandeur d'un terrain de football. La Sûreté du Québec, la Sécurité civile, la Municipalité, le service des incendies ainsi que le ministère de l'Environnement sont sur place. Un périmètre de sécurité de près de 200 mètres a été érigé autour du terrain touché. Trois personnes sont présentement évacuées. Le Nouvelliste; Postmedia Network (Gazette)

$33M for 2 Calgary flood mitigation projects announced

Officials from all three levels of government announced almost $32 million in funding Thursday for a pair of flood mitigation projects in Calgary. A new pump station will be built in Sunnyside, one of the communities that saw major flooding in the 2013 disaster. The new infrastructure will direct water away from the low-lying district into the Bow River. The second project is a flood protection berm, east of the Bonnybrook wastewater treatment plant in southeast Calgary, which was inundated during the 2013 emergency, forcing the city to discharge untreated sewage into the Bow River for a brief time. The project also includes upgrades to the groundwater and storm water infrastructure to help keep the plant from flooding again... Ottawa will contribute about $10.5 million towards the cost of both the Bonnybrook and Sunnyside improvements. CBC News

Federal plan calls for more northern coast guard auxiliaries
The Canadian Coast Guard is looking to expand its auxiliary programs across the North and the idea was announced this week as part of the Oceans Protection Plan. The agency doesn't know where exactly the new volunteer organizations will be, or how many, but says it is consulting with communities. "It really has to do with where we're likely to have enough volunteers, where there's an interest in doing this," says deputy commissioner Jeffrey Hutchinson. "Then we'll look at it also from a risk perspective in terms of where traffic is happening and where we get the greatest number of search-and-rescue calls." Hutchinson says volunteers respond to about a quarter of the coast guard's search and rescue calls in southern Canada, and that they're especially important in remote areas where the agency may not be able to respond quickly. CBC News

14 Wing Greenwood personnel to conduct search and rescue exercise
Royal Canadian Air Force members from 14 Wing Greenwood will be conducting a search-and-rescue exercise in Atlantic Canada starting on Nov. 14. The exercise will run from November 14 to 18. It will involve personnel and aircraft from 413 Transport and Rescue Squadron at 14 Wing Greenwood, including a CC-130 Hercules and the CH-149 Cormorant helicopter, according to a news release from the RCAF. The SAREX is primarily based out of the Summerside, P.E.I. airport, but also will include the airports and surrounding regions of Miramichi, N.B. and Sydney, N.S. Postmedia Network (Ottawa Citizen)

'For our children': Labrador firefighters learning to help people with autism in emergencies
When it comes to dealing with an emergency, people with autism can have a unique reaction that requres a unique response, according to the Autism Society of Newfoundland and Labrador. Firefighters in western Labrador are taking the society's training to teach them how to handle non-typical responses from those with autism - training first responders across the province are welcoming. CBC News

Canadian makes breakthrough in potential Zika vaccine
In the race to develop vaccines for the Zika virus, researchers faced an early hurdle that Canadian Gary Kobinger set out to overcome as swiftly as he could. The challenge? Mice, the animals used in early tests of vaccine candidates, are too hardy to be sickened by the Zika virus. So Dr. Kobinger genetically engineered a line of mice that would fall ill when exposed to Zika. Then, the Quebec-based microbiologist and his research partners in Philadelphia tested a DNA vaccine on the modified rodents, and, later, on rhesus macaques. The experimental DNA vaccine, known as GLS-5700, shielded all the mice from Zika infection, brain damage and death, according to a new study published Thursday in the journal npj Vaccines. The vaccine also provoked a strong immune response in the monkeys; like wild mice, they are naturally resistant to Zika. Globe and Mail

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Nil

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Nil

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Huge spike in U.S. web traffic before immigration site crash
Newly released statistics show Canada's citizenship and immigration website experienced a huge spike in web traffic from the U.S. just before it crashed on Tuesday, as results from the American presidential election were rolling in. Immigration, Refugees and Citizenship Canada says there were more than 200,000 users accessing the site around 11 p.m. on election night and American IP addresses accounted for about half of that figure. (…) She says the web traffic figures for Tuesday night -- when the election results were starting to indicate a Donald Trump presidential victory -- were significantly higher than the same time the previous week, when the website saw just over 17,000 users. (…) A number of U.S. citizens have said they may consider applying to move to Canada if Trump follows through on proposed policies such as mass deportations of illegal immigrants or the reopening of international trade agreements. Immigration lawyers have warned, however, that the process to move to Canada can be long and complex and may cause a number of potential U.S. emigrants to reconsider their plans to move north once they learn more. Canadian Press (Calgary Sun, Edmonton Sun, Ottawa Sun, Toronto Sun, Winnipeg Sun, Chronicle Herald, iPolitics); TIME, Hamilton Spectator, Toronto Star, 1, Vancouver Province, National Post, Yahoo

Canada: Flying To Canada? Electronic Travel Authorization Becomes Mandatory On November 10, 2016
Immigration, Refugees and Citizenship Canada (IRCC) has introduced an Electronic Travel Authorization (eTA) initiative to pre-screen visa-exempt foreign nationals travelling to or transiting through Canada by air. The eTA was introduced in March 2016. The mandatory implementation of the eTA has been delayed a number of times, as indicated in our September and October bulletins. However, effective November 10, 2016 all visa-exempt nationals, with limited exceptions, must have an eTA in order to travel to Canada by air. Mondaq (Lexology)

Canadian Immigration Lawyer Advises on Best Practices
An opinion piece states, "As an immigration lawyer, Catherine Sas of Sas & Ing wants to warn prospective newcomers against placing undue trust in immigration professionals. In many cases, people are being advised in ways that do not align with best practices. This can lead to complications and delays in the application process. (…) The penalty for misrepresentation -- either direct or indirect -- is a five-year ban from applying for immigration. IRCC and CBSA officers routinely hear stories from applicants that claim they were only following the advice or recommendation of immigration professionals. In instances where such cases have ended up in court, responsibility has historically been placed squarely on the applicant. Ultimately, an immigration application is the applicant's responsibility." SYS-CON Media Inc. (Digital Journal)

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

French plan for biometric database of 60 million people sparks outcry
When the French government quietly announced, in the middle of a holiday weekend, the merging of two files to create a megadatabase holding the biometrics of almost 60 million French citizens, it was clearly hoping to avoid an outcry. It failed. Among those lining up to criticize the government's move are its own minister of state for the Digital Sector and Innovation, and the National Digital Council, a body created by the government to provide independent recommendations on all matters relating to the effect of digital technologies on society and the economy. Minister of State Axelle Lemaire told French journalists the megadatabase used 10-year-old technology and had real security problems. For the Council, the creation of TES (from the French abbreviation for Secure Electronic Identity Documents) will result in abuses "as inevitable as they are unacceptable." CSO

German cabinet approves cyber security strategy
Germany's cabinet has approved a new cyber security strategy amid a growing number of attacks. Many of the cyber attacks are directed from China and Russia. The German cabinet on Wednesday adopted a new cyber security strategy to counter a rising number of threats targeting government institutions, critical infrastructure, businesses and citizens. The strategy calls for the creation of a mobile Quick Reaction Force housed within the Federal Office for Information Security (BSI), as well as similar teams within the federal police and domestic intelligence agency that are able to respond to cyber threats against government institutions and critical infrastructure. Germany's Cyber Defense Center will fall under the authority of the Interior Ministry, which will seek to foster inter-agency coordination and cooperation. Deutsche Welle

Yahoo Reveals More Details About Massive Hack
Yahoo provided more details on Wednesday about an epic hack of its services, including that the culprits may have planted software "cookies" for ongoing access to users' accounts. In revelations that could jeopardize the company's pending $4.8 billion acquisition by US telecom giant Verizon, the internet pioneer said it was trying to pin down when it first knew its system had been breached and whether hackers gave themselves a way to get back into accounts whenever they wished. "Forensic experts are currently investigating certain evidence and activity that indicates an intruder, believed to be the same state-sponsored actor responsible for the security Incident, created cookies that could have enabled such intruder to bypass the need for a password to access certain users' accounts or account information," Yahoo said in a filing with the US Securities and Exchange Commission. There is no evidence the state-sponsored actor is still active in the California-based company's network, Yahoo told regulators. AFP (Security Week); CSO

Yahoo: Verizon Could Pull Out of Deal
Yahoo has admitted its $4.8 billion sale to Verizon might not go through, as it emerged that the firm knew a state-sponsored attacker had accessed its network as far back as 2014. The internet pioneer claimed in an SEC filing yesterday that "there is no assurance that the sale transaction will be consummated in a timely manner or at all." That's mainly due to revelations of a massive data breach which exposed the account details of 500 million users, including names, email addresses, bcrypt encrypted passwords and security Q&As. In the filing, it admitted for the first time that staff may have known for two years that an attack had taken place before the company finally revealed the news in September this year. Infosecurity Magazine; CNET

Facebook buys black market passwords to keep your account safe
For a data-saturated company of its size and scope, Facebook has markedly managed to avoid the kind of security scandals, breaches and hacks that have affected many other major web companies. Take a closer look, and you'll see why. Though on the surface all seems calm, below the waves the social network is kicking its legs frantically and working around the clock to keep users' accounts safe. Keeping Facebook safe and keeping it secure are two different things, the social network's chief security officer, Alex Stamos, said Wednesday at Web Summit in Lisbon. Security is about building walls to keep out threats and shore up defenses, but according to Stamos, safety is bigger than that. CNET

Cyber-attaque d'ampleur contre les grosses banques en Russie
Une cyber-attaque d'ampleur, lancée depuis des milliers d'ordinateurs piratés dans plus de 30 pays, vise depuis mardi plusieurs grandes banques de Russie, a indiqué jeudi le laboratoire Kaspersky, spécialiste de sécurité informatique. Le plus gros établissement du pays, la banque publique Sberbank, a précisé avoir été ciblée et avoir réussi à neutraliser l'attaque sans perturbation sur ses activités. Selon Kaspersky, les attaques «complexes» de type DDoS, qui consistent à rendre un serveur indisponible en le surchargeant de requêtes, ont commencé mardi à 13H00 GMT et se poursuivaient jeudi. D'une durée moyenne d'une heure mais pouvant atteindre près de 12 heures, elles ont touché «les sites internet d'au moins cinq institutions financières connues parmi les dix premières» russes, a précisé la société dans un communiqué. AFP (Journal de Montreal)

Criminals Distribute Locky Ransomware To 2014 OPM Data Breach Victims

Locky is one of the most potent forms of crypto-ransomware in existence today. Even though security researchers try to combat this malware, the developers remain one step ahead. In fact, a new phishing campaign distributing Locky ransomware has been discovered, which targets 22 potential victims. All of these users were part of the US Office of Personnel Management data breaches in 2014 and 2015. Criminals always find news ways to target potential victims with malware and ransomware. Even though the data breaches affecting the Office of Personnel Management took place nearly two years ago, the information remains valid to this day. A lot of sensitive personal information was obtained by hackers, and they will direct target campaigns to different types of victims. One of those campaigns is already underway, as criminals impersonate OPM representatives. These individuals target government contractors and workers whose information was stolen during the attack. By sending phishing messages to these victims, recipients are asked to examine an attached file. This particular file is a ZIP file which executes the Locky payload when opened. Bitcoin News Service; Threat Post; Bleeping Computer

Dyn, Liberia DDoS Attacks Were Just Test Runs

The Mirai-fueled DDoS attacks that took the entire country of Liberia offline last week are waning—but researchers say the offensive was merely a test run for something much bigger... One particular group, operating what MalwareTech.com dubbed Botnet 14, has taken on significantly bigger targets than most of the Mirai dabblers out there. "Many of the botnets are simply attacking Minecraft servers and doing technically terrible attacks on websites, e.g. a Farming Simulator game mod site," said independent researcher Kevin Beaumont, in a posting. In contrast, "it is clear [Botnet 14 is] extremely successful at attacking things....it is the largest of the Mirai botnets and the domain controlling it pre-dates the attacks on Dyn. The capacity makes it one of the biggest DDoS botnets ever seen. Given the volume of traffic, it appears to be the owned by the actor which attacked Dyn." Transit providers have confirmed that over 500Gbps of traffic is typically output during attacks, which last a short period but can be enormously crippling. In Liberia, continued short-duration attacks on its infrastructure overwhelmed the African nation's single internet cable, with various websites hosted in the country going offline and telcos reporting widespread outages for internet access. Infosecurity Magazine

Competing hackers dampen the power of Mirai botnets

The malware behind last month's massive distributed denial-of-service attack in the U.S. appears to be losing its potency. Ironically, hackers are to blame for diluting its power. The malware known as Mirai -- which is now available on the internet -- has become a bit too popular in the hacking community, according to security firm Flashpoint. Competing hackers have all been trying to take advantage of Mirai to launch new DDoS attacks. To do so, that means infecting the poorly secured internet-connected devices, such as surveillance cameras, baby monitors, and DVRs, that the malware was designed to exploit. The problem is the malware may have run out of new devices to infect, forcing the hackers to vie for control over a limited resource pool. That competition appears to be stiff. On Tuesday, Flashpoint said it found that the Mirai malware is probably being used across 52 different networks of enslaved devices, often called botnets. However, that competition is also fracturing Mirai's full power. Newly formed botnets created through Mirai are becoming smaller in size, ever since the source code to the malware was released back in late September. CSO

Finns have their heating systems knocked offline by a DDoS attack

Finnish news website Etelä-Saimaa is reporting that a DDoS attack on the internet-connected building management system of two tower blocks in the district of Lappeenranta, Finland, had taken their building management systems offline for three days. The primary systems affected were the heating and water systems. With temperatures in Finland below freezing, disruption in the heating could cause both material damage as well as force residents to relocate. The building, managed by property management company Valtia, had its internet connection blocked by the attack, which meant the building management system kept rebooting itself in an attempt to reconnect to the internet. As a result, the building was not able to supply heating into the building because it was not able to start the relevant systems. SC Magazine UK

The Internet of Things Is Just a Pit Stop On the Way to Smart Dust

As processors get faster and smaller we seem to reach points of inflection, our technological progress allows us to do something that wasn't really possible before, or at least wasn't practical. We've seen this before: computers the size of rooms gave way to ones that fit under the desk. In time those too gave way

to slabs of aluminium and glass that we carried around in bags, and then to computers that fit in our pockets, and just happen to also be able to make phone calls. Known as Bell's law, this proposition is intimately intertwined with the far more well known Moore's law. But while Moore's law may be dying, Bell's law, at least for one last turn of the wheel, seems to be holding. You might think the change I'm talking about is the arrival of the much hyped Internet of Things, but the connected devices we see today are really only the first clumsy steps towards something else. They're transition technology. Over the next decade or two we can, perhaps, expect to see general purpose computing, sensors, and wireless networking, bundled up in millimeter-scale sensor motes that can drift in the air currents around us. The dust around us will soon become smart. If you think this is just a technological fantasy, it's not. Motherboard

LAW ENFORCEMENT / APPLICATION DE LA LOI

RCMP's handling of python case challenged by Jean-Claude Savoie's lawyer
Police reneged on written assurance snake owner wouldn't be charged if he answered 4 questions. Jean-Claude Savoie's lawyer says the RCMP violated his client's constitutional rights by filing a criminal charge against him after giving written assurance Savoie would not be charged in relation to his python's killing of two young boys in Campbellton in 2013. Savoie was found not guilty by a jury Thursday on the charge of criminal negligence causing death that was eventually laid by the RCMP. With the verdict, a publication ban was lifted on an April 2016 motion by Savoie's lawyers to have the court issue a stay of proceedings in the case because of what the defence called misconduct by the police and Crown. At issue was the lead investigator in Phase 1 of the investigation, Cpl. Gabriel Deveau, who gave defence lawyer Leslie Matchim written confirmation Savoie would not be charged in the case if Savoie answered four questions for the RCMP. CBC News; Financial Newspress

Amber Alert update: Girl missing, father found dead
A man suspected of taking his seven-year-old daughter from Nipawin, Sask., and sparking an Amber Alert was found dead this morning, the RCMP said. Adam Jay Eastman appears to have died from self-inflicted injuries, police said. The search for his missing daughter, Nia Eastman, is ongoing and an Amber Alert is still in effect. Nia is described as a Caucasian female, approximately 120 centimetres tall and weighing 22.7 kilograms. She has blonde, shoulder length hair and was last seen wearing pink eye glasses, a purple long sleeved shirt decorated with butterflies, a pink skirt and purple leggings with silver trim at the bottom. RCMP said the girl was supposed to be returned home to her mother by 7 p.m. on November 9. A vehicle believed to be operated by the girl's father was located on a rural property east of Smeaton near Snowden at approximately 10 p.m. Wednesday. Nipawin is approximately 140 kilometres east of Prince Albert. CTV News; Globe and Mail; Canada News; Castanet

'Please don't hate us': 2nd officer testifies at inquest into Felix Taqqaugaq's shooting death by police
The RCMP officer who narrowly missed being stabbed by Felix Taqqaugaq said the initial plan that night wasn't to arrest him, but rather a surveillance mission to assess the situation. Peter Marshall, who was a sergeant in Igloolik at the time and has since been promoted to staff sergeant, testified Wednesday by video at the coroner's inquest into Taqqaugaq's shooting death by police in 2012. The inquest is examining how the 30-year-old Inuk man with schizophrenia was shot in his own home. Marshall told the jury that he and his partner, Const. Jason Trites, were trying to locate Taqqaugaq after he made threats against the police on local radio. Marshall suspected, correctly, that Taqqaugaq was in mental distress. (…) After his testimony, before the phone line was cut, Taqqaugaq's brother in attendance yelled out a sincere: "Thank you Peter," providing a rare moment for the family in this inquest where, for a second, some members smiled. CBC News

RCMP locate Amber Alert subjects
A province-wide Amber Alert reached its conclusion in Sicamous on Friday Nov. 4. The RCMP de-activated the amber alert for Sofia and Mateo and their mother April Pastor-Ruiz after the trio were stopped by an RCMP officer near the Esso station in Sicamous at approximately 9 p.m. on Nov. 4. An RCMP spokesperson said the stop occurred without incident. The Amber Alert was issued by the

Coquitlam RCMP at approximately 4:30 p.m. on Nov. 4. Pastor-Ruiz alegedly abducted the children near Fraser Avenue and Larch Way in Coquitlam. 36-year-old Pastor-Ruiz, is in police custody and charges are pending. The children were found safe and will be reunited with their family. Salmon Arm Observer

Two meth labs busted
Four arrests were made as two drug labs were busted in Richmond this week. The alleged meth labs were on the 7000 block of Schaefer Avenue and the 7500 block of Lucas Road. The raids were made Monday and Wednesday. In the first case, the RCMP's Clandestine Laboratory Enforcement and Response Team said the entire home was "contaminated with the products of the ongoing illicit and toxic operation." A substantial amount of chemicals and lab equipment were seized. Three people were arrested, and more arrests are possible. On Wednesday, another arrest was made at the second home, where a smaller drug lab was found. A "significant amount" of the drug was seized. Charges are pending in both cases. Castanet

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Nil

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Opioid use taking toll in Ontario with hundreds of overdose deaths: report
A study has found the use of prescription opioids varies dramatically across Ontario, but overall the potent and addictive drugs are responsible for hundreds of overdose deaths in the province. The study by researchers at the Ontario Drug Policy Research Network found 638 people died in 2013 from opioid overdoses - a rate of about one death for every 20,000 residents in the province. Lead researcher Tara Gomes says coroners' reports show almost 13 per cent of those overdose deaths were suicides. Gomes says the Thunder Bay District and Timiskaming District had the highest rates of opioid-related deaths in Ontario, about four times the provincial average. The researchers found there were 3,200 opioid-related emergency department visits in Ontario in 2014, which resulted in about half of those patients being admitted to hospital. Canadian Press (Globe and Mail); CBC News

How Nova Scotia pharmacists help in the fight against opioid addiction
Plenty of discussion about how to deal with the opioid addiction crisis in Canada has focused on the role of doctors, even though some patients see their pharmacist more often than any other health-care professional. That's why a Nova Scotia pharmacist and professor believes pharmacists play a key role in dealing with this issue. Every prescription involves "a pharmacist, a physician and a patient, so there's a natural triad there," said Dr. David Gardner, who works in the department of psychiatry and college of pharmacy at Dalhousie University. In Atlantic Canada, the opioids in question are not smuggled medications— they're prescribed. Gardner said pharmacists usually have daily interactions with patients coming in for drugs like methadone to deal with opioid withdrawal. They may also see patients who are receiving medication for pain but using it for other reasons, or are on a medication that may not be safe for them, he said. CBC News

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Nil

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Seven states say Yes to marijuana, so now what's in it for Canada?
While Donald Trump was winning one of the biggest upsets in American political history, other ballot measures were quietly tallying wins alongside the Donald. Americans in 7 states have now voted to enact legislation that will, to varying degrees, legitimize marijuana for medical and/or recreational purposes. With a combined market value estimated at US$7.4 billion annually, and an expected growth rate of 28 per cent annually, the U.S. combined market for marijuana is expected to be worth US$21.2 billion by 2020. The significance of these measures to Canadian marijuana users and growers is substantial. The more states that adopt marijuana usage rules, the closer weed comes to becoming a national export crop for Canadian growers. And that, as much as anything, explains the ongoing surge in marijuana stock prices here. With the Canadian dollar steady for the last few years at an average 25 per cent discount to the greenback, Canada is well positioned to compete with domestic production in the United States, should that market open up to Canadian imports. Financial Post

PUBLIC SERVICE / FONCTION PUBLIQUE

PSAC pulls out of bargaining session with federal government
The Public Service Alliance of Canada is pulling out of the latest 10-day marathon session of collective bargaining with the federal government and is seeking a mediator to help sort the differences in a bid to reach a settlement. The union's various bargaining groups met today and decided that the differences between the parties were such that a mediator was needed to make any further progress. The giant union says it is still open to further talks and is not declaring an impasse at this point. Ottawa Citizen

«L'offre de 0,75% par année est nettement insuffisante»
La nouvelle offre de 0,75% par année pour un contrat de trois ans déposée par le gouvernement à l'Alliance de la fonction publique de Canada (AFPC) est loin d'être suffisante, selon l'Institut professionnel de la fonction publique du Canada. Alors que l'AFPC négocie maintenant depuis plus de neuf jours consécutifs sans avoir confirmé publiquement les détails du nouveau mandat des négociateurs du Conseil du Trésor, un autre syndicat membre du front commun syndical, l'Institut professionnel, a révélé la nouvelle offre salariale du gouvernement faite depuis la reprise des discussions le 1er novembre. «Le gouvernement fédéral, qui négocie avec nos collègues de l'AFPC, a présenté une nouvelle proposition, assortie d'une augmentation salariale de 0,75% par année pour trois ans. Malheureusement, cette nouvelle offre ne compense même pas la hausse du coût de la vie et reconnaît encore moins la valeur des professionnels de la fonction publique», a révélé Debi Daviau, présidente de l'Institut professionnel, dans un bulletin émis à ses 55 000 membres. Le Droit

OTHER / AUTRES

Nil

INTERNATIONAL

Obama says Trump meeting was 'excellent'
In a cordial beginning the transfer of power, President Barack Obama and President-elect Donald Trump met at the White House Thursday. Obama called the 90-minute meeting "excellent," and his successor said he looked forward to receiving the outgoing president's "counsel." (...) In Washington, Trump's scant transition team sprang into action, culling through personnel lists for top jobs and working through handover plans for government agencies. A person familiar with the transition operations said the personnel process was still in its early stages, but Trump's team was putting a premium on quickly filling key national security posts. The person was not authorized to discuss details by name and spoke on condition of anonymity. According to an organizational chart for the transition obtained by The Associated

Press, Trump was relying on experienced hands to help form his administration. National security planning was being led by former Michigan Rep. Mike Rogers, who previously worked for the FBI. Domestic issues were being handled by Ken Blackwell, a former Cincinnati mayor and Ohio secretary of state. Trump was expected to consider several loyal supporters for top jobs, including former New York Mayor Rudy Giuliani for attorney general or national security adviser and campaign finance chairman Steve Mnuchin for Treasury secretary. Former House Speaker Newt Gingrich and Tennessee Sen. Bob Corker were also expected to be under consideration for foreign policy posts. Associated Press (ABC)

Paris, Brussels attacks 'ordered by top ISIL leaders'
The cell that launched deadly attacks on Paris and Brussels had received its orders from "very high" in the Islamic State of Iraq and the Levant (ISIL) command, according to Belgium's federal prosecutor. Late last year a wave of bombings and shootings killed 130 people and injured hundreds more across the French capital. And in March suicide blasts struck an airport and a metro station in the Belgian capital, leaving about 30 people dead. "We know that the orders came from the Islamic State zone ... We know that it went very high in the command," Frederic Van Leeuw said in an interview with the AFP news agency in Brussels on Wednesday. Aljazeera

Man held in Wrexham on suspicion of terrorism offences
A 48-year-old man has been arrested in Wrexham on suspicion of terrorism offences. Police said the man, whom they did not identify, was held on Thursday on suspicion of being concerned in the commission, preparation and instigation of acts of terrorism, under section 41 of the Terrorism Act 2000. He was arrested as part of a joint operation between the Welsh extremism counter-terrorism unit, North Wales police and the West Midlands counter-terrorism unit. A police spokesman said: "The man is being questioned at a police station in the West Midlands. The arrest was preplanned and intelligence-led. There was no threat to the public's safety. An address in Wrexham is the subject of an ongoing search." Guardian

Israel, Russia affirm anti-terrorism alliance
The Russian and Israeli leaders have declared themselves partners in a battle against global terrorism. Dmitry Medvedev told his Israeli counterpart, Benjamin Netanyahu, that terrorism threatens Israel in a "very unique way." But Russia also suffers from terror with what he called "common roots," he added at a meeting in Jerusalem on Thursday. "This is why there is a need to fight terror together," Medvedev said. Netanyahu said the two countries, along with the United States and other nations, share a struggle against radical Islam and the Islamic State group. Canadian Press (Chronicle-Herald)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

RalphGoodale
Garde du drapeau-Légion royale canadienne au service du Souvenir-Queen Victoria Estates à Regina. N'oublions jamais

Lactualite
Ralph Goodale ne cherche pas à faire toute la lumière sur les agissements passés de la GRC et du SCRS #polcan #SCRS https://t.co/StDmp4c8tG

lulex
Thanks to @RalphGoodale & @csiscanada for moving forward to allow public participation without the needless spying. My heartfelt thanks.

bcpffa
We hope some money is directed to helping #firstresponders. @JustinTrudeau @RalphGoodale @MHCC_ Help fund our plan! @bcpffa @IAFFCanada

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

davidakin
#NewsNOW in Percé, QC: Revenue Minister @DiLebouthillier announces funding for shoreline rehabilitation.

globeandmail
Canadian makes breakthrough in potential Zika vaccine http://trib.al/osGfcwM From @kellygrant1

LP_LaPresse
Important glissement de terrain à Saint-Luc-de-Vincennes https://t.co/hE1Dla9Zxr

CBCAlerts
A landslide has cut off a road between Saint-Maurice and Saint Luc de Vincennes in Quebec. Some homes evacuated as a safety measure

J_Roberge
Deux propriétés évacuées. 2e glissement à survenir dans le secteur en peu de temps. Ingénieurs sur place. @TVA3R

OttawaCitizen
Have you seen Peter Stevenson? The 60-year-old has been missing from his #Tweed home since Wednesday. http://ow.ly/3Llq3062QH5 #ottnews

KelownaNow
Residents facing extreme flooding in #Pemberton https://t.co/GqNFPzk8Ux

CTVNewsVI
Highway 4 completely open right now west of Port Alberni, after being closed due to flooding. However, more rain forecast for tonight #yyj

jarmstrongbc
You need a canoe to access North Arm Farms #Pemberton @GlobalBC

HuffPostCanada
Making Fort McMurray home again (blog) http://huff.to/2fnRwzA

NATIONAL SECURITY / SÉCURITÉ NATIONALE

amandacconn
Very excited to be part of this important conversation happening next week at University of Ottawa on journalist surveillance!

nationalpost
With Trump about to learn America's deepest secrets, the nation's worried spymasters may have reason to fear http://natpo.st/2g18qri

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

RobertFife
Americans eye move to Canada, but immigration not so easy #cdnpo https://t.co/8tW7z0uziz

RobertFife
Ottawa offers to renegotiate NAFTA in effort to warm ties with Trump #cdnpoli #cdnecon https://t.co/HvBs9Zeywx

CBCTheNational
Federal aid not meeting needs of refugees, internal review finds http://www.cbc.ca/1.3842247

motherboard
US Customs police paid contractors to monitor the dark web http://bit.ly/2fFQrCr

CYBER SECURITY / CYBERSÉCURITÉ

motherboard
Here's how a Trump presidency could destroy net neutrality http://bit.ly/2fFLg5E

dnvolz
Guliani on Fox, when asked possible role in Trump admin: "I'd love to become the person that comes up with a solution to cybersecurity."

LAW ENFORCEMENT / APPLICATION DE LA LOI

RadioCanadaInfo
La GRC a-t-elle espionné des journalistes? http://rc.ca/MdZqC0

cbcreporter
Fund us or disband us, Nishnawbe Aski police say at suicide inquest @CBCWorldReport http://www.cbc.ca/1.3844452

CBCCanada
'Please don't hate us': 2nd officer testifies at inquest into Nunavut man's shooting death… http://www.cbc.ca/news/canada/north/felix-taqqaugaq-inquest-2nd-police-officer-testifies-1.3845086?cmp=rss …

globeandmail
Nanaimo, B.C. city council asks RCMP to investigate Mayor Bill McKay http://trib.al/BmZYdlK From @markhumeglobe via @GlobeBC

JJLye980
1184 guns seized in 31 days in BC gun amnesty, Morris says

CKNW
.@SCC_eng won't hear a Toronto police board bid to quash two class-action lawsuits arising out of the G20 summit 6 years ago.

CBCAlerts
Supreme Court of Canada won't hear Toronto police appeal, so class-action suits over G-20 detention can proceed. BG: https://t.co/KeZEsjZwkj

CdnPress
Have you seen Nia Eastman? There's an Amber Alert for her right now in Saskatchewan: http://on.thestar.com/2eNyrlV

metromontreal
Saskatchewan: le père d'une fillette disparue est retrouvé mort http://bit.ly/2fAiZOX #AlerteAmber

JillMacyshonCTV
Search planes now over area where father's body was found. There is a fast flowing creek nearby. @CTVNews #AmberAlert

JillMacyshonCTV
RCMP seem focused on a rural property near a creek, off Hwy 55. #AmberAlert continues for Nia Eastman @CTVNews

globeandmail
Toronto police arrest two in Toronto beating death of American man http://trib.al/DlsSvQh From @TuThanhHa via @GlobeToronto

CTVNews
N.B. Mounties broke deal in python-deaths case, defence lawyer says http://ow.ly/OLSH3062V7P

KelownaNow
.@bcrcmp take on babysitting duty after injury at daycare https://t.co/cAGOPw9rpN

CBCToronto
Toronto council is asking the police service to hit the brakes on its new grey and white scout cars http://bit.ly/2fo9FgH

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

dianamehta
'Strong support' for reopening prison farms, government consultation finds http://www.thespec.com/news-story/6956578--strong-support-for-reopening-prison-farms-government-consultation-finds/ …

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

GgNewsCA
Children 'at risk' unless changes made to provincial protective services: auditor general https://t.co/z5Jb90dZP6

GgNewsCA
Opioid use, addiction, taking its toll on northeastern Ontario: report - CBC.ca https://t.co/3Kdd3VLTq0

CBCCanada
Test results confirm Winnipeg baby exposed to carfentanil, police say
http://www.cbc.ca/news/canada/manitoba/winnipeg-police-baby-possible-fentanyl-exposure-1.3845198?cmp=rss …

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

JimBronskill
Latest U.S. marijuana votes could bolster Canada's legalization effort: law professor
http://nationalnewswatch.com/2016/11/10/lat … #cdnpoli #hw

vicecanada
Can Canadians cash in on America's pro-weed vote? http://bit.ly/1TdtUiO

OttawaCitizen
Midas Letter: Seven states say Yes to marijuana, so now what's in it for Canada? http://natpo.st/2fG2S1h #business

PUBLIC SERVICE / FONCTION PUBLIQUE

OttawaCitizen
A mediator is needed to make any further progress https://t.co/bP2dp5v4Xh

Clerk_GC
Great discussion at INAC Leadership Conference on PS priorities and building a healthy and respectful workplace.

OTHER / AUTRE

CBCPolitics
Justin Trudeau invites Donald Trump to visit Canada http://www.cbc.ca/news/politics/trudeau-trump-visit-canada-1.3845013?cmp=rss … #hw #cdnpoli

RobertFife
Trump win puts pressure on Ottawa to boost NATO spending #cdnpol

guardianworld
Madeleine Albright warns Trump against isolationist posturing on Nato https://t.co/3EDabLA69t

CKNW

Anti-Trump protests spread to Vancouver http://bit.ly/2g1efoS

INTERNATIONAL

SkyNewsBreak
South Wales Police says a 48-year-old man has been arrested in Wrexham on suspicion of terrorism offences

CBCWorldNews
Thousands join anti-Trump protests around U.S. http://www.cbc.ca/news/world/trump-protests-1.3844926?cmp=rss ...

France24_en
Estonia parties seal coalition deal supporting NATO, EU ties http://f24.my/2fAfHvm

tvanouvelles
Des islamistes extrémistes célèbrent la victoire de Trump http://bit.ly/2fUJBOK

nvanderklippe
New Interpol head is Chinese former deputy head of paramilitary police. Amnesty: "This is extraordinarily worrying" https://t.co/LatapvvRLq

lesoirplus
#Entretien Une série documentaire nous plonge au coeur de Molenbeek après les attentats de Paris http://bit.ly/2eWaCw3 par @DZacharie

nationalpost
Russia says warships drove away 'clumsy' Dutch submarine stalking squadron in Mediterranean Sea http://natpo.st/2g1dMTl

Reuters
Year-old Paris attack probe sights new suspect, but mastermind elusive https://t.co/b2OmtkWeLF

AJENews
Paris, Brussels attacks were 'ordered by top ISIL leaders' http://aje.io/dkmn

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

Today's News / Actualités
December 1, 2016 / le 1 décembre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Mentally ill deportee transferred to Alberta Hospital
A deportee with severe mental illness who was held at the Edmonton Remand Centre for 10 months without charge has been transferred to the Alberta Hospital. Abdikarim Gelle arrived at the psychiatric hospital last Friday. His mother was relieved, as she was worried he might be transferred to a facility in Quebec. "I am so happy that my son is not leaving Edmonton and I will be able to see him," said Asili Gelle, who also thanked people advocating on their behalf. Advocates have been urging authorities to relocate Abdikarim Gelle, 31, to a secure facility that could meet his mental health needs. Up until last

week, Alberta Hospital didn't appear to be an option. Looking for an alternative, authorities raised the possibility of transferring him to a psychiatric hospital in Montreal. The potential move concerned advocates. (...) "**The minister [Ralph Goodale**] has been making continuous efforts in order to remove the person concerned to Somalia," said hearings officer Sébastien Thibodeau at Monday's review. "However, due to mental health issues of the person concerned, his removal has been very complicated to execute. The detention of the person concerned is becoming lengthy and the removal is not likely to occur in the foreseeable future." Thibodeau said Alberta Health Services advised government officials that if Gelle was released they had a team ready to assess Gelle's mental health needs and the danger he represents to the public. Ufuoma Odebala-Fregene, an immigration consultant with Black Lives Matter Edmonton, said Gelle's move to Alberta Hospital was "the right decision, reflecting the compassionate and humanitarian objectives of our immigration and refugee system. "Abdi and his family can now focus on him getting better with our outstanding medical and social services support." CBC News

Trump's election should prompt Canada to rethink its complicity with U.S. mass surveillance
President-elect Donald Trump. It's still a phrase that takes some getting used to. Trump's pronouncements on issues of online privacy, surveillance and net neutrality -- among many other topics -- should send a shiver down the spine of anyone who cares about preserving basic democratic freedoms in a digital age. For Canadians these concerns strike particularly close to home. Already, federal government ministers are grappling with the implications of the impending Trump presidency and, for **Public Safety Minister Ralph Goodale** and Justice Minister Jody Wilson-Raybould, these implications are especially profound. For many years Canada's spy agencies have worked extremely closely with their U.S. counterparts, not least as part of the decades-old "Five Eyes" surveillance alliance between the U.S., U.K., Canada, Australia and New Zealand. This co-operation is so tight that over the years the Five Eyes have evolved into what whistleblower Edward Snowden describes as "a supranational intelligence organization that doesn't answer to the laws of its own countries." Rabble

TOP STORIES / MANCHETTES

Victoria police seize 'major' fentanyl shipment from China
Victoria police have intercepted a shipment of 1.45 kilograms of fentanyl bound for Victoria from China. Police estimate the drugs are worth about $400,000. CBC News

Mexican visa lift expected to cost Canada $262M over a decade
Canada's decision to lift the visa requirement for Mexican travellers is expected to cost about $262 million over the next decade, in part to deal with a potential surge in asylum seekers, according to an internal government analysis. A regulatory impact analysis statement, just published on a Canadian government website, pegs the overall cost of the policy change that kicks in today at $433.5 million over 10 years due to extra enforcement resources and added costs associated with a potential spike in refugee claims. The analysis predicts those costs will be partially offset by an estimated $171.6 million in economic benefits through increased tourism from Mexico and a boost in trade and investment opportunities. The federal government will need to make significant investments in immigration and border control processes to support a sustainable visa lift," the report reads. "Federal and provincial/territorial governments will need to manage potential increases in asylum claimants from Mexico who may seek to exploit their new visa-free status in an attempt to migrate to Canada permanently." While the majority of costs for dropping the visa requirement, and replacing it with an electronic travel authorization, will be borne by the federal government, provincial and territorial governments will also be impacted by increased asylum claims, the report says. CBC News

Canada prepares for surge of Mexican immigrants after visa lift and Trump win
Officials in Canada are readying for a potential surge in Mexican migrants, as a promise to scrap a visa requirement comes into effect amid uncertainty over Donald Trump's promises to crack down on undocumented immigrants. From Thursday, Mexican visitors to Canada will no longer need visas. The move has left the government anticipating an increase in Mexican tourists and business travellers, a spokesperson for Canada's immigration ministry said. The visa was put in place in 2009 by the previous Conservative government to address an increase in what it described as bogus refugee claims. But the

timing of the visa lift – following on the heels of Trump's vows to expel millions of illegal immigrants – has sparked concerns among officials that Canada could again see a substantial increase in Mexican asylum seekers, government sources told the Guardian. Between 2005 and 2008, Canadian officials said refugee claims from Mexico nearly tripled, making Mexico the number one source country for claims. Of the more than 9,400 claims filed by Mexicans in 2008, just 11% were accepted. The visa was embraced as a means of border control by the Conservative government. "The visa requirement I am announcing will give us a greater ability to manage the flow of people into Canada," the then immigration minister Jason Kenney said in a statement. "In addition to creating significant delays and spiralling new costs in our refugee program, the sheer volume of these claims is undermining our ability to help people fleeing real persecution." The Guardian

At one small border post in Quebec, Canada tests the idea of automated drive-through entry
First there were automated drive-through carwashes. Then automated drive-through banks. Now, the Canadian government is experimenting with an automated drive-through border crossing. While the fate of the wall along the U.S.-Mexico border promised by President-elect Donald Trump remains uncertain, Canada is carrying out a pilot project with an opposite aim: to use the latest technology to ease the flow of traffic across the United States' northern frontier. If you drive into the province of Quebec via the crossing at Morses Line, Vt., after 4 p.m. on any day, no live Canadian customs agent will stop and interrogate you. Instead, a gate opens and you drive into a large, garage-like building. There, under the gaze of several TV cameras, you are invited by a customs officer to insert your passport or other border ID into a document reader and are asked the usual questions put to visitors seeking to enter Canada. Washington Post (National Post)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Wet, windy weather causing travel delays in Maritimes for 2nd day
High winds, rain and some snow in parts of Nova Scotia and most of New Brunswick are causing travel delays for the second day in a row. High winds cancelled Bay Ferries' service between Digby, N.S., and Saint John, N.B. on Thursday. Marine Atlantic said its morning crossings were going ahead, but it won't sail at 11:45 p.m. Thursday. Northumberland Ferries said travellers should check with the company before departing. A few flights were delayed, and one was cancelled out of Halifax Stanfield International Airport Thursday morning. Most of Nova Scotia can expect a windy and wet day. Environment Canada has issued a special weather statement for all of Cape Breton and Guysborough County. Snow is expected to develop over Cape Breton Thursday near noon and will likely mix with or change to rain over areas near the coast. "However, over higher terrain, snowfall amounts may approach warning criteria," says the special weather statement. It's also going to be dangerous near the coast. "Rough pounding surf combined with higher than normal water levels may cause minor flooding along east and southeast facing shorelines of eastern shore Nova Scotia and Cape Breton, the statement said. CBC News; St. John's Telegram

Winter storm leaves thousands without power in Quebec City area
Hydro-Québec is working to restore power to thousands of homes and businesses across the province this morning as strong winds and snow caused outages in several regions. Shortly after 7 a.m. Thursday, there were just over 40,000 outages across the province, with the bulk of them in the Quebec City area. The Chaudière-Appalaches, Lanaudière, Mauricie and Montérégie regions are also affected
It's not clear when power will be restored. Updates can be found on the Hydro-Québec website. A powerful weather system is moving eastward over the southern part of the province. CBC News; Montreal Gazette

Procès de Tom Harding : le Tribunal veut comprendre pourquoi c'est si long
Les parties impliquées dans le dossier des accusations liées au déraillement du train de Lac-Mégantic ont été convoquées au tribunal jeudi matin. Le juge Gaétan Dumas souhaite comprendre pourquoi les procédures sont si longues. Il leur a également demandé de coordonner leurs efforts afin de faire avancer les choses plus rapidement. Mardi, on apprenait que le conducteur du train, Tom Harding, déposerait, en janvier prochain, une requête en arrêt des procédures. Ce dernier invoquera l'arrêt Jordan pour mettre fin

aux procédures judiciaires en raison de délais déraisonnables. Jeudi matin, Tom Harding était représenté par Me Charles Shearson. Il a expliqué au juge que cette requête ne visait pas à attaquer le système de justice lui-même, mais plutôt qu'avec les délais encourus, son client subissait des préjudices importants. Radio-Canada

Man located after massive multi-team search - Missing person found Wednesday morning
A search involving multiple search and rescue teams from at least four counties was focused on the Weaver Settlement area in Digby County on Tuesday night. A man who went in the woods to check his property was reported missing Tuesday afternoon. Clare, Digby, Yarmouth and Valley ground search & rescue teams participated in the search. Members from the Civil Air Search and Rescue Association and the Department of Natural Resources helicopter were standing by for a break in the weather. RCMP and EHS were also on the scene. The rescue team that discovered the missing man on Wednesday morning brought him out on an eight-wheel Argo. Yarmouth County Vanguard; Cape Breton Post

Rescue aircraft dispatched as fishing boat takes on water off Yarmouth - Joint Task Force Atlantic says pump has been dropped to vessel and situation is 'stable'
A Hercules aircraft has dropped a pump to a 13-metre fishing vessel taking on water off Yarmouth, N.S., and the situation is "stable," according to the military's Joint Task Force Atlantic. Canadian Navy Lt. Len Hickey said a call to the Joint Rescue Coordination Centre came in around 8:30 a.m. AT about the fishing vessel Tide 'N Knots taking on water about 32 kilometres off the coast. The Hercules, along with a Cormorant helicopter and several Canadian Coast Guard vessels have been dispatched to the scene to help. "The latest update that I received noted that the Herc has dropped a pump to the vessel — that's in addition to their own existing pumps. They've got a couple running right now and the situation is stable," Hickey said. There's no word on how many people are on the vessel or whether anyone has been injured, though Hickey underscored the situation is "stable." CBC News

Nanaimo SAR recruiting new volunteers
The Nanaimo Search and Rescue group (NSAR) is looking for some additional volunteers and are holding a membership meeting next month. The group has been around since 1991 and have provided assistance to Nanaimo RCMP on countless ground and inland water searches and rescues. They are actively recruiting for community minded individuals, who are willing to be trained in a variety of areas such as first aid, rope rescue, climbing, swift water rescue, tracking and fund raising. Crew members require specific training over the course of several months, and upon completion, would be available for on-call shifts. CHEK News

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Can cell providers tell when police spy on their networks? - New research shows it's possible to tell when police use IMSI catcher surveillance technology
For years, police and government agencies around the world have used a controversial investigative technique to spy on cellular phones, often disrupting cellular networks in the process. But one wireless carrier has had enough. T-Mobile Austria, which is a fully-owned subsidiary of Deutsche Telekom, teamed up with academics at SBA Research in Vienna to study the effects of electronic surveillance devices known as IMSI catchers on cellular networks — and most importantly, whether the use of such devices can be reliably detected. The researchers propose using the network monitoring systems that most carriers already have in place to look for tell-tale signs that an IMSI catcher may have been used. Their paper was presented at a computer security conference in France this past September. In Canada, IMSI catchers are technically illegal to possess or use, but documents shared with the CBC suggest that the

government may have granted the RCMP and CSIS an exception. In response to questions, Bell spokesperson Jacqueline Michelis wrote in an email that "the use of IMSI catchers is illegal in Canada. We don't publicly disclose the measures we take to ensure the security of our networks." TELUS and Videotron did not respond to a request for comment, while Rogers declined to comment. In the U.S. Verizon and T-Mobile USA declined to comment, AT&T did not respond to questions, and Sprint merely linked to the company's privacy policy. CBC News

Ismael Habib disait faire partie du groupe armé État islamique
Le suspect de terrorisme Ismael Habib avait confié à un agent d'infiltration de la GRC qu'il souhaitait partir en Syrie et qu'il faisait partie du groupe armé État islamique. C'est ce qui ressort du témoignage de l'agent en question ce matin au palais de justice de Montréal dans le cadre du procès de l'homme de 29 ans. «Il m'a indiqué qu'il voulait partir. J'ai demandé où. Il a dit la Syrie. J'ai demandé s'il faisait partie d'un groupe. Il a dit oui. J'ai demandé lequel? Il a répondu l'État islamique», a raconté le policier, caché derrière des paravents dans la salle de cours parce que son identité doit être protégée. Dans le cadre d'une enquête policière aux multiples scénarios, l'agent jouait le rôle du patron d'une organisation criminelle de passeurs illégaux et de fabrication de faux passeports. La Presse

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Victoria police seize 'major' fentanyl shipment from China
Victoria police have intercepted a shipment of 1.45 kilograms of fentanyl bound for Victoria from China. Police estimate the drugs are worth about $400,000. CBC News

Mexican visa lift expected to cost Canada $262M over a decade
Canada's decision to lift the visa requirement for Mexican travellers is expected to cost about $262 million over the next decade, in part to deal with a potential surge in asylum seekers, according to an internal government analysis. A regulatory impact analysis statement, just published on a Canadian government website, pegs the overall cost of the policy change that kicks in today at $433.5 million over 10 years due to extra enforcement resources and added costs associated with a potential spike in refugee claims. The analysis predicts those costs will be partially offset by an estimated $171.6 million in economic benefits through increased tourism from Mexico and a boost in trade and investment opportunities. The federal government will need to make significant investments in immigration and border control processes to support a sustainable visa lift," the report reads. "Federal and provincial/territorial governments will need to manage potential increases in asylum claimants from Mexico who may seek to exploit their new visa-free status in an attempt to migrate to Canada permanently." While the majority of costs for dropping the visa requirement, and replacing it with an electronic travel authorization, will be borne by the federal government, provincial and territorial governments will also be impacted by increased asylum claims, the report says. CBC News

Canada prepares for surge of Mexican immigrants after visa lift and Trump win
Officials in Canada are readying for a potential surge in Mexican migrants, as a promise to scrap a visa requirement comes into effect amid uncertainty over Donald Trump's promises to crack down on undocumented immigrants. From Thursday, Mexican visitors to Canada will no longer need visas. The move has left the government anticipating an increase in Mexican tourists and business travellers, a spokesperson for Canada's immigration ministry said. The visa was put in place in 2009 by the previous Conservative government to address an increase in what it described as bogus refugee claims. But the timing of the visa lift – following on the heels of Trump's vows to expel millions of illegal immigrants – has sparked concerns among officials that Canada could again see a substantial increase in Mexican asylum seekers, government sources told the Guardian. Between 2005 and 2008, Canadian officials said refugee claims from Mexico nearly tripled, making Mexico the number one source country for claims. Of the more than 9,400 claims filed by Mexicans in 2008, just 11% were accepted. The visa was embraced as a means of border control by the Conservative government. "The visa requirement I am announcing will give us a greater ability to manage the flow of people into Canada," the then immigration minister Jason Kenney said in a statement. "In addition to creating significant delays and spiralling new costs in our

refugee program, the sheer volume of these claims is undermining our ability to help people fleeing real persecution." The Guardian

At one small border post in Quebec, Canada tests the idea of automated drive-through entry
First there were automated drive-through carwashes. Then automated drive-through banks. Now, the Canadian government is experimenting with an automated drive-through border crossing. While the fate of the wall along the U.S.-Mexico border promised by President-elect Donald Trump remains uncertain, Canada is carrying out a pilot project with an opposite aim: to use the latest technology to ease the flow of traffic across the United States' northern frontier. If you drive into the province of Quebec via the crossing at Morses Line, Vt., after 4 p.m. on any day, no live Canadian customs agent will stop and interrogate you. Instead, a gate opens and you drive into a large, garage-like building. There, under the gaze of several TV cameras, you are invited by a customs officer to insert your passport or other border ID into a document reader and are asked the usual questions put to visitors seeking to enter Canada. Washington Post (National Post)

Additional Charges Expected Against Man Charged In Fatal North London Crash
Additional charges are expected to be laid today against a 23-year-old man charged in connection with an alleged fatal drunk driving crash that killed a 60-year-old woman one week ago. It was exactly one week ago that 60-year-old Gloria Chivers was killed in an early morning crash at the intersection of Richmond and Sunningdale. Investigators say an SUV driving on Sunningdale collided with a vehicle that was stopped at a red light. Police say Chivers was pronounced dead at the scene. 23-year-old Jinghao Zhou faces multiple charges in that case, but was granted bail on Tuesday. However, soon after that decision was made, he was taken back into custody by immigration officials. Zhou's lawyer Jim Dean says he's been in contact with officials with the CBSA who tell him additional charges will be laid. "I don't know what those charges specifically are going to be but I understand they're federal immigration charges and we'll get more details." 640 News

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Worldwide cyber-crime network hit in coordinated raids
One of the world's biggest networks of hijacked computers, which is suspected of being used to attack online banking customers, has been taken down following police swoops in 10 countries, German police said on Thursday. In an internationally coordinated campaign, authorities carried out the raids on Wednesday, seized servers and website domains and arrested suspected leaders of a criminal organisation, said police and prosecutors in northern Germany. Officials said they had seized 39 servers and several hundred thousand domains, depriving criminals of control of more than 50,000 computers in Germany alone. These hijacked computers were used to form a "botnet" to knock out other websites. Two people who are believed to have been the administrators of the botnet infrastructure known as "AVALANCHE" were arrested in Ukraine, investigators said. Another person was arrested in Berlin, officials added. The strike came in the same week that hackers tried to create the world's biggest botnet, or an army of zombie computers, by infecting the routers of 900,000 Deutsche Telekom with malicious software. Reuters

Cyberattacks Strike Saudi Arabia, Harming Aviation Agency
Saudi Arabia's aviation agency was attacked last month by an aggressive computer virus intended to disrupt high-profile government targets, officials and experts said on Thursday. The attack, which experts say emanated from outside the country, used a version of Shamoon, malware used to target the Saudi energy sector four years ago. Similar kinds of data-clearing software were used in 2014 against the Las Vegas Sands and Sony. The Saudi government confirmed the latest breaches on Thursday, after several cybersecurity firms noted them. Bloomberg News reported that thousands of computers were damaged at the headquarters of the General Authority of Civil Aviation starting in mid-November, "erasing critical data and bringing operations there to a halt for several days," although operations at Saudi airports did not appear to be affected. New York Times

Everyone is worried about internal cybersecurity threats, report

There are few things everyone can agree upon, but according to a new study almost all security professionals are concerned about insider threats. The study The Growing Security Threat From Insiders of 317 independently identified IT security professionals, from companies with more than 1,000 employees, conducted by Dimensional Research found 99.7 percent are concerned about internal security threats. The insider threats that particularly worry these execs are malware being installed by workers, 73 percent; stolen or compromised credentials, 66 percent; stolen data, 65 percent; and abuse of administrative privileges, 63 percent. Even when asked to consider both internal and external threats, 49 percent said the former were more worrisome. SC Magazine

Europol announces 5 arrests in 'unprecedented' cybercrime op
Europol says five arrests have been made in connection with a massive operation aimed at knocking out a cybercrime group accused of inflicting hundreds of millions of euros in losses worldwide. The European Union police agency says the sweep was "unprecedented in its scale" and resulted in the seizure of 39 servers used by the group, nicknamed Avalanche. Hundreds of thousands of domains associated with the group have been seized or blocked. Fernando Ruiz, the head of operations at Europol's Cybercrime Center, says the arrests were made Wednesday following months of work by law enforcement agencies from 30 different jurisdictions. He declined to say where the suspects were detained. Senior European justice official Michele Coninsx said Thursday the bust "marks a significant moment in the fight against serious organized cybercrime." Associated Press (St. John's Telegram)

New Proteus Malware: Jerk of All Trades?
Based on the ancient Andromeda botnet, new malware family Proteus is going for broke. According to Bleeping Computer, the code can transform infected devices into proxy servers, mine for cryptocurrencies, log keystrokes and check whether stolen account credentials are valid. In effect, it's a jerk of trades. Here's a rundown of the newest, multifunctional malware risk. Malware efforts have diversified over the past few years. Cybercriminals are no longer satisfied with simply shutting down PC functions or demanding small ransom payouts. They are getting adventurous, looking for ways to steal social data, redirect security efforts even as distributed denial-of-service (DDoS) attacks take place or lock down mobile devices with seemingly impenetrable ransomware. Few of the functions built into Proteus are new. As noted by Cointelegraph, for example, certain Android devices are shipped with firmware that could compromise bitcoin accounts. CIO, meanwhile, pointed out that the recent Dyn DDoS attack leveraged a host of compromised Internet of Things (IoT) devices to achieve massive traffic volumes at high speed. Security Intelligence

LAW ENFORCEMENT / APPLICATION DE LA LOI

Suspected impaired driver crashes car into RCMP cruiser in Langley
A suspected impaired driver has been arrested after allegedly crashing his car into a RCMP cruiser in Langley. It happened Wednesday night near 208 Street and 76 Avenue. The RCMP officer was not injured but the car suffered some damage. Several liquor bottles could be seen on top of the vehicle once the suspected impaired driver had been taken into custody and the car was searched. The car also has Saskatchewan licence plates. Global News

Les libéraux retirent leur soutien au projet de loi Wynn
La femme de l'agent de la Gendarmerie royale du Canada (GRC) de Saint-Albert en Alberta tué en janvier 2015 promet de poursuivre le combat pour faire adopter un projet de loi nommé en l'honneur de son mari après que le gouvernement libéral du Canada eut indiqué ne pas soutenir le projet. C'est un coup à l'estomac. Nous avons travaillé si fort. Shelly Wynn, épouse de l'agent tué David Wynn Le projet de loi S-217 prévoit d'amender le Code criminel pour rendre obligatoire la présentation du passé criminel, des chefs d'accusation et des omissions d'apparaître en cour lors des audiences de libération sous caution. Pour l'instant, la présentation de ces preuves est laissée à la discrétion de la Couronne qui peut être représentée en Alberta par des policiers. Le passé criminel du meurtrier de l'agent David Wynn n'avait ainsi pas été présenté au juge de paix qui avait décidé de sa libération sous caution. Shawn Rehn avait cependant 68 condamnations à son actif et faisait face près d'une trentaine d'accusations, dont le non-respect d'une interdiction de posséder une arme à feu. « Nous ne voulons pas que ça arrive à qui

que ce soit d'autre. Et si changer un mot peut faire une différence pour une autre famille, c'est ce que nous voulons », a indiqué Shelly Wynn. Radio-Canada

Nanaimo RCMP continue investigation into suspected drug house
A heavy RCMP presence remains on hand at a home on 9th Street in Nanaimo's south end. Neighbours say a tactical RCMP team entered the home Tuesday with their guns drawn. Nanaimo RCMP have yet to reveal why officers entered the home, but neighbours say it's been a known drug house for a couple of years. They say lots of 'sketchy' people come and go at all hours of the day and night. RCMP Forensic officers have been meticulously combing through the home over the past two days. On Wednesday evening Mounties were seen pulling items – such as bikes, a chainsaw and generator – from the home's basement and loading them into a U-Haul. Nanaimo RCMP say they will issue a news release on Thursday, but spokesperson Cst. Gary O'Brien has hinted the bust is quite significant. CHEK News

Mixed Reactions as Trudeau Nixes Northern Gateway Pipeline but Approves Kinder Morgan Expansion
It was a day of mixed feelings after Prime Minister Justin Trudeau rejected Enbridge's Northern Gateway Pipeline but approved its Line 3 (L3RP) replacement project from Alberta to Wisconsin, as well as the controversial Kinder Morgan pipeline expansion in Vancouver. Indigenous opponents of Northern Gateway are finally breathing a sigh of relief following nearly a decade of protests and litigation from several First Nations and conservation groups on British Columbia's north and central coast. The 1,056-mile-long Northern Gateway pipeline would have carried diluted bitumen from Alberta's tar sands to the deepwater coastal port of Kitimat B.C. (…)However, several First Nations and municipalities near Vancouver have vowed to stop the Kinder Morgan expansion at any cost, which could mean that protests may intensify in the coming months, possibly similar to those taking place in Standing Rock, North Dakota. In early November the Royal Canadian Mounted Police (RCMP) spoke with Kinder Morgan CEO Ian Anderson regarding security of their project. "I'd be naive if I didn't expect that," Anderson told reporters. "Hopefully, it's peaceful. People have the right to express their views publicly and in that regard. It's when it goes beyond that that we'll have to be prepared. We've been in deep conversations with policing authorities, RCMP in the planning for our project—what can we anticipate and what their role needs to be." Indian Country Today Media Network

Perquisitions sur la réserve de Kanesatake liées à du trafic de stupéfiants
La GRC et la Sûreté du Québec mènent ce matin des perquisitions dans deux résidences de la réserve Mohawk de Kanesatake, sur la rive nord du fleuve Saint-Laurent, dans le cadre d'une enquête sur un réseau de trafic de stupéfiants. L'Unité mixte d'enquête sur le crime organisé autochtone de la GRC participe à l'opération. Le corps policier doit faire un bilan des saisies plus tard aujourd'hui. Les personnes visées sont notamment soupçonnées de tremper dans le commerce illégal du cannabis. La Presse

Lake Country crams cruiser
Mounties will once again be inviting the public to cram a police cruiser full of donations in support of the Lake Country Food Bank. The RCMP will again partner with the Lake Country Fire Department for the fifth annual RCMP Cram the Cruiser fundraising event Saturday at the Save-On-Foods in Lake Country between 9 a.m. and 2 p.m. Since its inception, Cram the Cruiser has raised more than 8,843 pounds of donated items, and nearly $11,250 in cash and cheques for the Lake Country Food Bank. Both regular and auxiliary members of the RCMP, in regular uniform or red serge with marked police vehicles, along with RCMP Citizen's On Patrol volunteers will be on location inviting the public to cram the cruiser with non-perishable food donations. Cash donations will also be accepted and all donations will solely benefit the food bank. "The number of those who rely on the support of the Lake Country Food Bank seems to grow each and every year," said Cpl. Jesse O'Donaghey, RCMP spokesperson. "I was shocked to hear that at least 500 individuals, one-fifth of those believed to be seniors, readily depend on this charitable organization for the everyday essentials they need to survive." Vernon Morning Star

Garth Cameron receives RCMP Certificate of Appreciation
When disaster strikes, the families of victims need support. A local hero received an RCMP Certificate of Appreciation at a ceremony held in Courtenay on Nov. 3. Garth Cameron, a 14-year veteran of the West Coast's volunteer Search and Rescue team, was recognized for his actions during a recovery effort to

find the remains of a father and son who died in a plane crash on Vargas Island Dec. 14, 2013. In a letter announcing the award, Island District RCMP Chief Superintendent Ray Bernoties said Cameron was a vital source of leadership during the search, ensuring the remains were handled respectfully and the victim's family members, and volunteer searchers, were taken care of. "His expertise, team building abilities, organization and leadership skills ensured that this difficult task was completed with the respect the families deserved," Bernoties wrote. "His loyal support to the RCMP, the Search and Rescue team and his community bring credit to himself and are in keeping with the highest standards of a Canadian Citizen." Westerly News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

NIL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Family of Muslim teen attacked in Hamilton, Ont. believes assault may be hate crime
Police in Hamilton, Ont., say they are "not ruling anything out" after a Muslim teen was robbed in a weekend attack which his family suggests may have been a hate crime. Hamilton police said Noah Rabbani, a Grade 10 student from Saltfleet Secondary School, was walking near Rymal Road East and Fletcher Road just after midnight on Sunday when two men got out of a vehicle and attacked him. One of the suspects assaulted Rabbani with a baseball bat and both men fled the scene with the victim's backpack. Rabbani, who is a Muslim of Pakistani descent, suffered injuries to his brain, jaw, limbs and spine and remains in the intensive care unit, said his aunt in a Facebook post. 900 CHML

Death of 15-year-old Tina Fontaine drives Manitoba volunteer searchers
The 2014 discovery of 15-year-old Tina Fontaine's body — wrapped in a garbage bag and discarded in the Red River — shook Winnipeg to its core. To this day, it prompts residents of the city's North End neighbourhood, a low-income area with a high crime rate, to try to prevent others from meeting a similar fate. With virtually no public funding, they comb the river, the shoreline and the streets, determined to make a difference. Bad weather doesn't deter them. Neither does the very real risk of danger. CBC News

La communauté Bedeque réclame une enquête publique
Faire la lumière. La communauté autochtone Bedeque, qui a des racines à Mont-Joli, réclame une enquête publique sur les événements de Val-D'Or où une trentaine de femmes autochtones ont dit avoir été victimes de violences et d'agressions sexuelles commises par des policiers. Rappelons que l'enquête menée par le Service de police de la Ville de Montréal (SPVM) ne débouchera finalement sur aucune accusation contre les six policiers qui auraient agressé des femmes autochtones à Val-d'Or. L'Avantage

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Updated - Jennifer Catcheway's mom blasts RCMP at MMIW forum
Bernice Catcheway says she has given up on the RCMP's efforts to find her missing daughter, Jennifer. "We stopped relying on RCMP, on officials. They say 'We're with you, we're standing with you.' Well, I don't see them standing with us," an emotional Catcheway said Wednesday night during a town hall-style public forum on missing and murdered Indigenous women. "I never get a call from the RCMP. I never got a call from who's on her case, Jennifer's case, the detective. Nobody calls me." MMIW families were given the chance Wednesday night to address the RCMP directly at the forum, hosted by CBC's The Current. Catcheway, whose daughter disappeared in 2008 at the age of 18, called for more help and

better communication between RCMP investigators and families in front of the packed house at the University of Winnipeg's Eckhardt Gramatté Hall. CBC News

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Task force on cannabis legalization/regulation completes research; report expected later this month
A task force which has been looking at the legalization of marijuana over the last several months, has announced it has completed the research phase, and will release a report within the next few weeks. The Federal Government is working on legislation to legalize pot by the spring of 2017. Chair of the Task Force on Cannabis Legalization and Regulation, the Honourable Anne McLellan and Dr. Mark Ware, Vice Chair, have released the following statement: "It has been an honour for us, along with the other members of the Task Force, to have had opportunity to engage with Canadians across the country who generously shared their expertise and perspectives on how the government should approach the legalization and regulation of cannabis. We are pleased to announce that the Task Force has completed our work." News Talk 770

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Al-Qaida-led attacks intensify in Mali as Liberals prepare to announce peacekeeping mission
An al-Qaida faction has claimed responsibility for missile strikes aimed at U.N. forces in Mali as the Canadian government is poised to announce details of its peacekeeping deployment to Africa. Photos posted on social media by Al-Qaida in the Islamic Maghreb show two Grad missiles being fired at Timbuktu airport Tuesday, targeting what it called "French forces that invaded the lands of the Muslims." (…) The missiles missed their target, landing outside the airport perimeter, Reuters reported. The Gao bombing was claimed by the AQIM-linked Al Mourabitoun, whose "goal is to spread jihad across North Africa," according to the **Public Safety Canada** website. The Long War Journal reported there had been 228 al-Qaida-linked attacks in the region so far in 2016, many of them in northern Mali. "This represents a significant increase in the al Qaeda-led insurgency in northern Mali since last year, which has also spilled over the borders more frequently than the prior two years." National Post

INTERNATIONAL

Deadly storms add to drought, flood and fires plaguing South
Five people were killed in two states after at least 13 twisters damaged homes, splintered barns and toppled trees in parts of Alabama, Louisiana, Mississippi and Tennessee, the National Weather Service confirmed. At least a dozen more people were injured early Wednesday, adding to a seemingly biblical onslaught of drought, flood and fire plaguing the South. The storms tore through just as firefighters began to get control of wildfires that killed seven and damaged or wiped out more than 700 homes and businesses around the resort town of Gatlinburg, Tennessee. In Alabama, the weather system dumped more than 2 inches of rain in areas that had been parched by months of choking drought. Associated Press (Metro News)

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

RalphGoodale
La consultation sur la sécurité nationale est prolongée jusqu'au 15 déc. J'espère que vous partagerez votre opinion http://Canada.ca/consultation-securite-nationale ...

RalphGoodale
The National Security consultations have been extended to December 15. I hope you share you views at http://Canada.ca/national-security-consultation ...

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Safety_Canada
There's still time to participate in #YourNatISec! Don't miss the chance to contribute! http://ow.ly/oDtv306lmGz

Securite_Canada
Vous pouvez encore participer à la consultation #VotreSecNat! Ne ratez pas la chance de contribuer! http://ow.ly/qdNO306lmXQ

Safety_Canada
Have your say on countering radicalization to violence. Join us LIVE on Periscope @ 7 p.m. EDT tonight https://www.periscope.tv/Safety_Canada

Securite_Canada
Donnez opinion sur lutte c. radicalisation menant à violence. Soyez-y en DIRECT sur Periscope à 19 h HAE ce soir. https://www.periscope.tv/Safety_Canada

Safety_Canada
Dr Amarasingam is a Fellow at George Washington's University's Program on Extremism. Ask him your ?s LIVE tonight http://ow.ly/yYIh306lH5h

Securite_Canada
Amarasingam (Ph. D.) est boursier progr. extrémisme à George Washington University. Posez vos ? EN DIRECT ce soir http://ow.ly/xlVS306lG8Y

NATIONAL SECURITY / SÉCURITÉ NATIONALE

RosieBarton
U.S.-style 'fusion cells' among recommendations for improving Canadian policy on hostages - Politics - #hw

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

VICE
Being deported is a distressing nightmare: http://bit.ly/2gZ8c4J

CTVNewsVI
CBSA discovered shipment of fentanyl bound from China to address in Victoria, alerted Victoria police to initiate investigation

CYBER SECURITY / CYBERSÉCURITÉ

SCMagazine
Carleton University hit with ransomware attack https://t.co/1GcmVIlgQF

SCMagazine
Everyone is worried about internal cybersecurity threats, report https://t.co/wEr484ooa5

LAW ENFORCEMENT / APPLICATION DE LA LOI

rcmpqc
Become a police officer – We are waiting for you in Montréal, Wednesday December 7 at 6:00 p.m. #RCMPcareers http://www.rcmp-grc.gc.ca/even/en/e/981

CORRECTIONAL SERVICES / SERVICES CORRECTIONNELS

ReducingCrime
Happy to see initiatives proposed by @ontMAG follow our #ReasonableBail reco's for repairing our broken bail system! http://bit.ly/1F4omft

Safety_Canada
#DYK how 2 participate in record suspension review? You can online, by email, or even by mail! Learn + here: http://ow.ly/qyOi306Ibex

Securite_Canada
#SVQ vs pouvez participer au prog. de suspension du casier? En ligne, par courriel & par la poste! Savoir + ici: http://ow.ly/xlrh306Ibkf

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

StatCan_eng
Women experiencing violent victimization often rely on emergency shelters: http://ow.ly/A7Za306IyXU #ActionsMatter

Securite_Canada
À suivre : la vie difficile de Tyler, le parcours d'un adolescent fictif vers un mode de vie criminel. Restez branchés! **#TylerStory**

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

CKNW
.@CityofVancouver to quadruple fines for illegal pot shops @EmilyLazatin980 http://bit.ly/2fVRGAA

globalnews
LIVE NOW: Veterans, advocates, share their concerns and perspectives on cannabis as medicine https://t.co/YTnjHJJrav

INTERNATIONAL

CBCAlerts
UN warns repeat of 1994 Rwanda genocide (800K killed) may be underway in South Sudan. Evidence of starvation, gang rapes, villages burned.

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

Today's News / Actualités
December 6, 2016 / le 6 décembre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Le gouvernement Trudeau souligne le 6 décembre sans parler d'armes à feu
Plusieurs gestes de recueillement sont posés en ce jour commémorant le drame de l'Ecole polytechnique de Montréal qui a entraîné 14 jeunes femmes dans la mort, il y a 27 ans. Des cérémonies se déroulent partout au Canada, notamment sur le campus de l'Ecole, où une gerbe de 14 roses blanches a été déposée devant la plaque commémorative. Les drapeaux y resteront en berne jusqu'au crépuscule.
Une diplômée de l'Ecole polytechnique, Heidi Rathjen, militante depuis le drame pour le contrôle des armes à feu au Canada, en a profité de l'anniversaire pour dénoncer l'inaction du gouvernement Trudeau.

(…) En arrivant à la réunion de cabinet, mardi matin, le ministre responsable de ce dossier, Ralph Goodale, n'a pas voulu répondre aux questions des journalistes sur le sujet. À midi, le premier ministre et quelques-uns de ses ministres prévoyaient déposer des roses blanches au cours d'une cérémonie devant le parlement. M. Trudeau et sa ministre de la Condition féminine ont publié, en matinée, des communiqués pour souligner le 6 décembre, communiqués qui ne font aucune allusion au contrôle des armes. Presse Canadienne (98.5FM); Journal de Métro

TOP STORIES / MANCHETTES

Six aboriginals file complaint with human rights tribunal over John Furlong investigation
Six Northern British Columbia First Nations members are accusing the federal government and RCMP of racial and ethnic discrimination for bungling their allegations of abuse against Vancouver corporate director John Furlong. Maurice Joseph, Emma Williams, Dorothy Williams, Richard Perry, Ann Tom and Cathy Woodgate filed a complaint Monday (December 5) with the Canadian Human Rights Tribunal. "Although the government failed to acknowledge, let alone investigate, our concerns regarding alleged abuse by John Furlong, it has favoured Furlong in ways that have silenced and re-traumatized us," said the complaint by the ex-Furlong students. "Neither the **Public Safety Ministry** nor the RCMP provided a service to remedy this situation. (…) On July 13, the Assembly of First Nations resolved at its annual convention to urge the federal government and RCMP to thoroughly and impartially investigate the allegations of abuse and urge the government to meet with anyone affected to hear their concerns about the conduct of the investigations and to discuss acceptable remedies. Business in Vancouver

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Service restored after landline calls, 911 services down across N.L.
Bell Aliant is reporting that service is restored after multiple outages affected landline calls across Newfoundland and Labrador Tuesday, including 911 emergency services. Service was restored around 11:30 a.m. Tuesday, but it is unclear how many users were affected. Bell Aliant has not said what caused the issue. The Royal Newfoundland Constabulary took to Twitter to spread the word and provide alternate contact information for those in need of services during phone outages. CBC News

Winter storm halts some mail delivery in southern Manitoba
The winter storm that's hitting southern Manitoba is affecting roads, flights, schools and even the mail. The severe weather conditions in the area are currently delaying mail delivery, according to Canada Post. "While every effort is being made to deliver the mail, some customers may not receive mail today," stated Canada Post in a tweet Tuesday. Global News

Environment Canada to get $83M in new and upgraded weather radar systems
The federal government has quietly awarded an $83-million contract to outfit Environment Canada with a new national network of weather radar systems. The contract was awarded by Public Works and Government Services in June of this year without an accompanying public announcement. Documents seeking input from industry before the contract was awarded say Environment Canada is embarking on a multi-year project to rejuvenate its network of meteorological radar. "The requirement is to replace approximately 20 of the existing weather radar network and related infrastructure by the spring of 2023," the documents say. The letter explains that Canada has a network of 31 radar systems across the country, one-third of which can be upgraded, but the other two-thirds have to be replaced. CBC News

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Don't repeat past mistakes, Privacy Commissioner warns as government reviews national security framework

The government's initiative to modernize Canada's national security framework should draw from lessons of the post-9-11 world, including commissions of inquiry and Edward Snowden's revelations of mass surveillance, says the federal Privacy Commissioner. The importance of strengthening privacy protections is highlighted in a formal submission to the government's public consultation on Canada's national security framework signed by Commissioner Daniel Therrien and all provincial and territorial privacy commissioners and ombudspersons. Commissioner Therrien was joined by Jean Chartier, President of the Commission d'accès à l'information du Québec and Brian Beamish, Ontario Information and Privacy Commissioner, at a press conference to unveil and discuss the submission Tuesday. "Everyone can agree that the police and national security agencies need adequate tools to protect us, and that these tools need to be adapted to the digital world," says Commissioner Therrien. "But state powers have already been significantly expanded, particularly with Bills C-51 and C-13. At the same time, we have seen too many cases of inappropriate and sometimes illegal conduct by state officials that have impacted on the rights of ordinary citizens not suspected of criminal or terrorist activities. In my view, those serious incidents were caused by deficient legal standards that failed to set appropriate limits on government actions," he says. "These key lessons from history remind us that clear safeguards are needed to protect rights and prevent abuse, that national security agencies must be subject to effective review, and that any new state powers must be justified on the basis of evidence. Government should only propose and Parliament should only approve new state powers if they are demonstrated to be necessary and proportionate – not merely convenient." The importance of considering the impact of surveillance measures on rights is emphasized throughout the submission, which addresses issues such as collection and use of metadata by national security agencies and law enforcement; encryption; information sharing by government and oversight. "In my view, this is not the time to further expand state powers and reduce individual rights. Rather, it is time to enhance both legal standards and oversight to ensure that we do not repeat past mistakes and that we ultimately achieve real balance between security and respect for basic individual rights," says Commissioner Therrien. Office of the Privacy Commissioner of Canada News Release

NATIONAL SECURITY / SÉCURITÉ NATIONALE

NIL

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

NIL

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Facebook and Other Tech Companies Seek to Curb Flow of Terrorist Content
For all the good that has come from the internet, the online world has also served as a powerful device for recruiting terrorists and spreading their propaganda. A coalition of top technology companies is now trying to change that. Facebook, Google, Twitter and Microsoft announced on Monday that they have teamed up to fight the spread of terrorist content over the web by sharing technology and information to reduce the flow of terrorist propaganda across their services. The group plans to create a kind of shared digital database, "fingerprinting" all of the terrorist content that is flagged. By collectively tracking that information, the companies said they could make sure a video posted on Twitter, for instance, did not appear later on Facebook. New York Times (2016-12-05); Softpedia

UNB to beta test Jeopardy computer champ's cybercrime fighting abilities
Just seven months after IBM announced it would begin teaching its Watson computer system to fight cybercrime, the company is graduating Watson to the next level of instruction. Caleb Barlow, vice-president of IBM Security, says 40 organizations will begin beta testing of the cognitive technology. "The learning process is going well. Part of this is getting it out there to several beta customers including the

University of New Brunswick, California State Polytechnic, Sun Life Financial, University of Rochester Medical Centres and others," Barlow said in an interview. Watson -- IBM's question-answering computer system -- was originally designed to compete (and win) on the television quiz show Jeopardy, but the technology has since been used on other problem-solving projects, from clothing design to cancer. CBC News; ZDNet; Infosecurity Magazine; Fortune

Hacker Claims To Push Malicious Firmware Update to 3.2 Million Home Routers
One of the hackers who amassed a new massive army of zombie internet-connected devices that can launch disruptive cyberattacks—even by mistake—now claims to have taken control of 3.2 million home routers, taking advantage of a flaw that allowed anyone to connect to them. On Monday, the cybercriminal, who calls himself BestBuy, claimed to have set up a server that would automatically connect to vulnerable routers and push a malicious firmware update to them. This, he said, would grant him persistent access and the ability to lock out the owners as well as internet providers and device manufacturers. Motherboard

LAW ENFORCEMENT / APPLICATION DE LA LOI

Six aboriginals file complaint with human rights tribunal over John Furlong investigation
Six Northern British Columbia First Nations members are accusing the federal government and RCMP of racial and ethnic discrimination for bungling their allegations of abuse against Vancouver corporate director John Furlong. Maurice Joseph, Emma Williams, Dorothy Williams, Richard Perry, Ann Tom and Cathy Woodgate filed a complaint Monday (December 5) with the Canadian Human Rights Tribunal. "Although the government failed to acknowledge, let alone investigate, our concerns regarding alleged abuse by John Furlong, it has favoured Furlong in ways that have silenced and re-traumatized us," said the complaint by the ex-Furlong students. "Neither the **Public Safety Ministry** nor the RCMP provided a service to remedy this situation. (…) On July 13, the Assembly of First Nations resolved at its annual convention to urge the federal government and RCMP to thoroughly and impartially investigate the allegations of abuse and urge the government to meet with anyone affected to hear their concerns about the conduct of the investigations and to discuss acceptable remedies. Business in Vancouver

Officer attacked with bear spray, suspects considered armed and dangerous
Local RCMP are looking for suspects considered armed and dangerous after an officer was bear sprayed early this morning. Around 4 a.m. Mounties were called to a rural property north east of Grande Prairie to reports of a break and enter. The arriving officer found the vehicle and while trying to speak with the occupants, the officer was sprayed. The suspect vehicle took off through a field and the officer was able to call for help. That vehicle was found by police but another vehicle was stolen from a nearby property. Q99 Live

Woman files complaint against Whistler RCMP over cellphone seizure
A Vancouver woman has filed a formal RCMP complaint, alleging police in Whistler seized her cellphone after she used it to film an arrest. Valerie Connelly said when she refused to give officers the passcode to her phone, she herself was arrested. "There was no conversation — and you can see it in the video that I have — he just walked up and grabbed it out of my hands," said Connelly.
While Mounties have told her she was arrested for obstruction, it's a case that raises concerns with civil rights activists. (…) While Whistler RCMP didn't respond to CBC's request for comment directly, an email from one of the officers to Connelly said her phone was seized as part of an ongoing investigation and that she was detained for obstruction, but released without charges. "E" Division, the provincial body governing RCMP in BC, responded to CBC's request for comment with a statement but wouldn't comment on the specifics of this case. "In general terms, police have the authority to seize cellular phones and other video recording devices from the public, if those devices contain evidence that is not available through other means, and that evidence is at risk of imminent loss or destruction," said Sgt. Annie Linteau. The policy director for the B.C. Civil Liberties Association questioned why officers felt the need to seize Connelly's cellphone under the circumstances as she has described them. "From the outset, there is a concern that there may not have been legal authority for the confiscation," said Micheal Vonn. CBC News

Concerns raised about police conducting checkpoints without flashing lights
Concerns are being raised about RCMP officers conducting checkpoints without engaging their flashing blue and red lights. A recent video taken at nighttime in Waterville, N.S. shows the RCMP pulling over drivers without engaging their flashing red and blue lights, which is against policy. "It's unsafe. Somebody's going to get hurt or killed," says Wayne Bezanson, who recorded the video. "It's about time it got stopped." The officers approached Bezanson while he was filming and asked what he was doing. In the video, Bezanson can be heard asking why the flashing lights aren't on and whether that is against police protocol. The officer tells Bezanson it isn't, but according to the RCMP's official spokesperson, it is against protocol under the RCMP's national policy. "The emergency equipment on the police vehicle needs to be active at all times during the contact with the person who's being stopped," says RCMP Cpl. Jennifer Clarke. CTV News

Canada-wide warrant issued for suspect in B.C. sex offences
A Canada-wide warrant has been issued for a man wanted for alleged sexual offences committed in Prince George in 1993. RCMP are asking the public's help in locating Rupert William Burr, 55, who has been sought by police in B.C. since 1998. The search is being widened by the new warrant. Burr's current whereabouts are unknown and he is believed to be using an alias. The Alberta-born man is believed to have been in the community of Worsley as recently as last year. Metro News

Central man arrested following drug seizure
A 58-year-old Centreville man has been arrested in connection with the seizure of drugs, including cocaine. On Dec. 4, following a three-month investigation, RCMP officers executed a search warrant at a residence in Centreville. Police seized a quantity of cocaine as well as Canadian currency, firearms and prescription narcotics. The search was conducted by officers from the RCMP's Federal Policing Operations West, New-Wes-Valley detachment and Police Dog Services. Gander Beacon

Grounding wire stolen from NL Power's Lethbridge substation
Newfoundland Power says thieves and vandals continue to put the lives of its employees and the public at risk by ignoring warnings about the dangers of illegally entering high voltage substations. Sometime on or before this past Sunday, vandals entered the Lethbridge substation on the Bonavista Peninsula, the company said in a news release Tuesday. A hole was cut in the substation fence, causing damage to electrical equipment. Copper grounding wire that was connected to the high voltage electricity grid was also stolen, compromising the integrity and reliability of the electricity system. (…) Anyone with information is asked to contact the RCMP, RNC or Crime Stoppers. The Labradorian

Teens accused of stealing car, joyriding dangerously though Halifax
Two 16-year-old boys are due in youth court in Halifax today, accused of stealing a car, fleeing police and driving all the way from Bedford to Halifax on a flat tire. According to RCMP, the teens allegedly stole the car from a home on St. Margarets Bay Road in Timberlea on Friday. Officers spotted the stolen vehicle at about 10:30 p.m. Monday night on Prospect Road, near Brookside. The teens tried to evade officers by driving into a parking lot then speeding away, according to RCMP. Police said they didn't chase the vehicle but sent out the description to other officers. The vehicle was then spotted in the Bedford area. At around 2 a.m. this morning police put down a Stop Stick — a device that deflates tires, safely, without a blowout — and were able to flatten one of the tires. CBC News

Lucky to escape unharmed
The Penticton RCMP say a woman that opened an exploding package in a local trailer park last week was lucky to escape mostly uninjured. During a weekly briefing Tuesday, Cpl. Don Wrigglesworth said the package was an unlabelled cardboard box, wrapped in red Christmas paper, containing an explosive device. He said the bomb squad determined the device could have caused serious injury. Investigators have spoken to several people in different residences at the mobile home park on Skaha Lake Road. There have been no other incidents of this type, Wrigglesworth said. Castanet

Cop Shop event in Yarmouth brings RCMP, students together

A group of students from Central School in Yarmouth went for a special outing Friday, thanks to the Cop Shop program. This was the second year for the initiative, which gives students a chance to meet RCMP officers, go to lunch with them and do some Christmas shopping with them. Seven police officers – representing the Yarmouth town and rural detachments – took part in the Dec. 2 event, including staff sergeants Michel Lacroix (town) and Ben Parry (rural). Nine students from Central participated. They were picked up in squad cars by officers, who then drove them to Wendy's, where they had lunch, which was donated by the restaurant. Next it was off to Bulk Barn, where the youngsters were able to get treat bags, courtesy of the store. From there, the officers and students made their way to Dollarama, where the children picked out Christmas gifts. Dollarama donated $25 per student for the event. After returning to Central School, the students and officers teamed up to do some gift-wrapping. Yarmouth County Vanguard (Nova News Now)

All grown up: Nova Scotia RCMP puppy moves away for next phase of police dog training
A RCMP puppy many Nova Scotians watched grow up through social media is moving on to his next adventure. Hamer (pronounced "Hammer"), a one-year-old German Shepherd, was introduced to the public last December at just 10-weeks-old with his imprinter, Const. Richard Bushey. An imprinter is a RCMP officer trained to raise puppies into potential police dogs. Through videos and social media updates, including one in March 2016, Nova Scotians watched Hamer grow in photos and video highlighting his progress. "The goal of puppy training is to develop a confident dog who can work in any setting," Cpl. Glenn Brown, Bushey's imprinting mentor, said in a RCMP release. (…)Now in New Brunswick, Hamer is working with an RCMP dog handler who may become his permanent partner. The release said if the pair seems to mesh, they will be begin the training program at the RCMP Police Dog Service Training Centre in Innisfail, Alberta, in 2017. Metro News

Centralized 911 dispatch centre inches closer towards becoming a reality
As the top cop of the Victoria police, acting chief Del Manak is always looking for ways the department can become more efficient. The department is currently in the midst of an efficiency review focused on front line operations and has ongoing discussions with regional partners on integrating some services. Talks continue with Saanich police on how units can be integrated to fight cyber crime. Computer forensic services have already joined forces. But one thing that Manak has supported for many years and is now inching further towards a reality is the centralized Emergency Response Dispatch Centre, which would bring three dispatch points (for 911 calls and police dispatch) under one roof. It would also be purpose built designed to withstand a major earthquake. Currently, 911 calls for the region are answered among three centres — Victoria police, Saanich police and the Westshore RCMP. The information is then transferred to the appropriate agency for dispatch, but having multiple call takers has caused officials concern. Victoria News

20 police cars packed with food for seniors
Enough food was donated to fill 20 vehicles when a "pack-a-police-car" event was held Saturday at local Save-On Foods.The outcome left Prince George RCMP in an upbeat mood."The generosity of the community was remarkable" Cpl. Craig Douglass said. "We believed this would be a successful event, but had no idea that it would be this successful." Prince George Citizen

Canada-wide warrant issued for mom in girl's disappearance
Niagara police have issued a Canada-wide warrant for a woman they allege abducted her nine-year-old daughter, prompting an Amber Alert over the weekend. Layla Sabry and her mother, Allana Haist, were last seen Thursday around 6 p.m. on King St. in Welland, Niagara Regional Police say. Layla's case continues to be treated as a missing person investigation, but police said Saturday that enough time had elapsed that they concluded the Amber Alert. Police are asking anyone with information regarding the girl or her mother's whereabouts to contact 911 or Crime Stoppers. Canadian Press (Kingston Whig Standard, CJOB)

Leitch vows to 'lock up' illegal pipeline protestors
Conservative leadership candidate Kellie Leitch has turned her right-of-centre brand of populism onto Canada's pipeline protesters, vowing to increase penalties for illegal protests and calling for environmental lobbying to be recognized as a political activity. In a Facebook messaged posted Tuesday,

Leitch outlined a five-point plan in response to the political backlash against oil pipeline construction happening from B.C. to Quebec. She calls for higher penalties against violence and vandalism, "ensuring those who provide support for the aforementioned actions are charged." She wants to create a new joint police force to target environmental protests and to classify environmental lobbying as political activity "to get international money out of the process." She also calling for unspecified changes to regulations to "ensure Canada's ability to compete in the marketplace." (…) The new security "force" that Leitch proposes would be "comprised of specialized components from the RCMP, CSIS, CRA and DFAIT to coordinate investigations, freeze bank accounts, and lay charges to ensure that those who seek to illegally disrupt natural resource development projects are brought to justice." iPolitics

Here Are the Next '20 Standing Rocks' According to Frontline Activists
Anyone with even a passing knowledge of energy politics surely knows what a massive, unexpected victory it was for thousands of Standing Rock campers when the US Army announced its decision to block the Dakota Access pipeline from its planned route. (…) Even before that surprise, Indigenous groups north of the border were already encouraged by what was happening in Standing Rock. Just last month, Kanesatake Grand Chief Serge Simon made it clear that mass civil disobedience is on the table for Indigenous people opposing megaprojects. The Mohawk leader told APTN Canada could see "20 Standing Rocks" if projects go ahead without free, prior and informed consent. (…) Kinder Morgan's recently-approved Trans Mountain expansion, which will transport raw bitumen from Alberta through BC's lower mainland, is the most obviously heated pipeline fight in Canada, and one the major political players are already gesturing toward. "The Standing Rock Sioux won today, and we will win on Kinder Morgan," Green Party Leader Elizabeth May said in an email blast yesterday. Opponents say the project will increase tanker traffic in the area sevenfold and put Canada's climate targets in jeopardy. VICE News

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Montreal mother convicted of attempting to kill daughter granted day parole
After spending less than a year in prison for attempting to kill her daughter, Johra Kaleki has been granted day parole. In February, Kaleki was sentenced to just under three years in prison for attacking her daughter, Bahar Ebrahimi, who was 19 years old at the time. Her daughter went out with friends to a nightclub. When she returned to her Dorval home after midnight, her mother attacked her. The Parole Board of Canada consented to day parole because Kaleki has exhibited good behaviour and has the support of her husband and daughters. However, the board members said they felt she still has some introspection to do and refused her full release. CBC News

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Une centaine de femmes manifestent à Québec
Une centaine de femmes ont encerclé la fontaine de Tourny avec le symbolique ruban blanc à l'occasion du 6 décembre, Journée nationale de commémoration et d'action contre la violence faite aux femmes. Cette journée est également le moment de commémorer le drame survenu en 1989 à l'École polytechnique de Montréal, où 14 jeunes femmes ont été assassinées. Journal de Montréal

Haut taux de violence familiale en Saskatchewan : un problème à causes multiples
Le fait que la Saskatchewan compte une population autochtone importante qui vit dans des conditions particulières et que les communautés rurales, plus isolées, sont nombreuses dans cette province au coeur des Prairies joue un rôle non négligeable.
Les victimes de violence conjugale proviennent de tous les milieux, selon la coordonnatrice de l'Association provinciale des maisons d'hébergement pour femmes de la Saskatchewan (PATHS), Jo-Anne Dusel, mais certaines populations sont toutefois plus à risque, notamment les femmes autochtones. Radio-Canada

B.C. chief apologizes, steps away from missing women portfolio over social media photo

The B.C. regional chief for the Assembly of First Nations has resigned as head of the assembly's missing and murdered women portfolio after posting a picture with sexual undertones on social media. Shane Gottfriedson has told a special meeting of chiefs that the post - a picture of his legs with an emoji in his groin area - was not his finest moment. Gottfriedson says he spoke to AFN National Chief Perry Bellegarde directly about the matter. Canadian Press (Vancouver Sun, Times Colonist); APTN

Police chief apologizes for language used to describe victim in homicide arrest
Winnipeg Police Chief Danny Smyth apologized Tuesday for the language used in recent police statements about the 2014 killing of Angela Marie Poorman. Poorman, a 29-year-old mother of three, was stabbed to death in the North End on Dec. 14, 2014. On Nov. 29, 2016, Winnipeg police announced they had charged an 18-year-old man with second-degree murder in Poorman's death. He could not be named because he was a minor at the time of the homicide. CBC News

Carfentanil responsible for at least 15 deaths as opioid crisis takes new deadly turn
The deadly opioid carfentanil has killed 15 people across Alberta, 14 in the last two months. Alberta's chief medical officer Dr. Karen Grimsrud said the concern is clear within Alberta Health Services, and they must come up with a plan to battle the lethal concoction, which is roughly 100 times more potent than fentanyl. "I am deeply concerned about the increasing number of deaths associated with carfentanil," Grimsrud said in a statement. "It's possible these individuals were not aware they were taking it. Albertans need to know that carfentanil is here ... and that it's an extremely dangerous and deadly opioid. Even the smallest trace can be lethal." Read more: This one intercepted package had the potential to kill every Canadian. In an effort to fight fentanyl-related overdoses, the overdose antidote naloxone was made available at 900 sites across the province, including pharmacies. Calgary Police Service drug unit Staff Sgt. Martin Schiavetta said they spoke at length about the highly toxic drug in July after a one-kilogram seizure of carfentanil. Calgary Sun; Radio-Canada

Elephant sedative carfentanil detected in Waterloo region, drug taskforce warns
Carfentanil has been found in Waterloo region, a drug taskforce is warning. Health Canada confirmed carfentanil was found in green counterfeit pills stamped CDN and 80, which resemble OxyContin pills, the Waterloo Region Integrated Drug Strategy said in an overdose alert sent out Monday. The notice warns carfentanil is an opioid used to sedate large animals, such as elephants, "and is not for human consumption." Carfentanil cannot be detected by sight, smell or taste. CBC News

High number of missing kids 'unacceptable,' says Kenora, Ont. OPP officer
provincial police officer in the northwestern Ontario city of Kenora says more needs to be done to help at-risk kids in his community, in light of the high number reported missing each year. In a city with about 15,000 people, Kenora OPP dealt with close to 900 calls about missing persons last year, said Const. Bob Bernie, the detachment's community mobilization officer. The vast majority of those calls were about kids, he said. "That's a number that's really unacceptable," said Bernie, adding that many of the calls involve children living in group homes, and habitual runaways. "We have a lot of kids in care in Kenora," he said, "and oftentimes they're away from family, they're perhaps not connected to resources in a meaningful way ... and they run away." CBC News

Il y a 27 ans, la tuerie de l'École polytechnique de Montréal
Depuis 27 ans aujourd'hui, le début du mois de décembre est marqué par la commémoration de la tuerie de l'École polytechnique de Montréal où 14 jeunes femmes ont perdu la vie, fauchée par les balles d'un tireur misogyne. Cette année, la mémoire des 14 jeunes femmes sera honorée sobrement sur le campus universitaire. Une gerbe de 14 roses blanches sera déposée devant la plaque commémorative de la tragédie et les drapeaux de l'établissement seront mis en berne de l'aube au crépuscule. Le premier ministre Justin Trudeau déposera également des fleurs sur la Colline du Parlement, à Ottawa, en mémoire des victimes. « Il y a 27 ans, 14 jeunes femmes ont été assassinées à l'École Polytechnique de Montréal seulement parce qu'elles étaient des femmes », a déclaré M. Trudeau par voie de communiqué. « En ce sombre anniversaire, prenons le temps de réfléchir à ce que les Canadiens - femmes, hommes et jeunes - peuvent faire pour mettre fin aux fléaux que sont la misogynie et la violence basée sur le sexe au pays et partout dans le monde. » La Presse Canadienne / Radio-Canada (Huffington Post)

27e anniversaire de la tuerie à la Poly: Trudeau muet sur les armes
En ce 27e anniversaire de la tragédie de l'École polytechnique, le gouvernement de Justin Trudeau dénonce la violence dont sont victimes les femmes, mais ne dit mot de ses intentions pour mieux contrôler les armes à feu. Durant la campagne électorale de 2015, les libéraux ont promis de défaire des mesures prises par les conservateurs de Stephen Harper. La loi C-42, adoptée par les conservateurs, a facilité le transport des armes à autorisation restreinte et des armes prohibées. Depuis l'entrée en vigueur de cette loi, un propriétaire d'arme peut transporter sa possession n'importe où et non pas seulement de son domicile à son centre de tir. La loi a également retiré l'obligation au vendeur d'armes à feu de vérifier le permis de possession d'armes de l'acheteur avant de conclure la transaction. Les libéraux n'ont toujours pas déposé de projet de loi pour modifier C-42. La semaine dernière, le groupe PolySeSouvient, qui milite pour un meilleur contrôle des armes à feu, a manifesté son impatience. La Presse Canadienne (La Presse)

Une centaine de femmes manifestent à Québec
Une centaine de femmes ont encerclé la fontaine de Tourny avec le symbolique ruban blanc à l'occasion du 6 décembre, Journée nationale de commémoration et d'action contre la violence faite aux femmes. Cette journée est également le moment de commémorer le drame survenu en 1989 à l'École polytechnique de Montréal, où 14 jeunes femmes ont été assassinées. Les femmes présentes voulaient appuyer le dépôt d'une pétition dénonçant le harcèlement et les violences vécus par les femmes locataires. Selon le collectif, 1054 femmes et enfants ont été tuées par des hommes au Québec depuis le 6 décembre 1989. Journal de Québec

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Perry Bellegarde wants First Nations to move beyond 'doom and gloom' ahead of Trudeau address to chiefs
While many of Canada's First Nations are gripped by poverty, suicide and a funding crunch, AFN National Chief Perry Bellegarde sounded a positive message Tuesday, calling on Indigenous communities to move beyond the "doom and gloom." (…) Notwithstanding his organization's relative satisfaction with the Trudeau government, Bellegarde chided them for dragging their heels on launching the inquiry into missing and murdered Indigenous women. The prime minister launched the process last year, and has appointed five commissioners, but work has yet to begin. Hundreds of people have been waiting for years for this inquiry to begin. They should not have to wait any longer," he said, adding First Nations people do not want recommendations in two year's time to address the prevalence of violence against Indigenous women. CBC News

Vigil Remembers Women Impacted by Violence
The 27th annual Vigil for Women Against Violence, is set to go at 12 PM at Coulter Parkette in downtown Port Elgin. Pat Sanagan of the Canadian Federation of University Women, organizers of the event, tells Bayshore Broadcasting News, "Every year there are incidents in the news to which we can turn, to remind people that violence against women is not going away." Sanagan suggests this year is worse than ever, citing the Missing and Murdered Indigenous Women (MMIW) inquiry; female RCMP officers who were compensated for sexual harassment in the workplace; and myriad sexual assault cases involving celebrities. She says it's the MMIW stories that have hit home. Bayshore Broadcasting

Honour victims by ending violence against women
An opinion piece states, "In our times, the achievements in civil rights for women have been significant. Some major hurdles have been passed, too: Canada has had a woman prime minister. Women have distinguished themselves from the Supreme Court and the Senate to executive positions in the corporate world. But despite these great gains, women remain the targets of sexist-fueled violence. On Dec. 6, 1989, a deeply troubled young man with a violent attitude towards women unleashed his disturbed sentiments by killing 14 female engineering students at l'École Polytechnique de Montréal. That's why on this day every year, we observe the National Day of Remembrance and Action on Violence Against

Women. In the aftermath of the massacre, we learned that the killer, Marc Lépine, grew up in an environment where abuse against women was common. Too many women are still subjected to this kind of abuse within the privacy of their homes and in the company of their families. While violent crime overall is on the decline in Canada, every year more than 170,000 women are victims of violent crime - 83 per cent of the time men were responsible and 45 per cent of the time the attacker is the woman's intimate partner. Tragically violence against aboriginal women is not in decline. Aboriginal women and girls are 3-4 times more likely to be murdered or sexually assaulted than other women. This national crisis has prompted the government to create its National Inquiry into Missing and Murdered Indigenous Women and Girls." Leader-Post

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Manitoba premier says he is not alone in wanting delay in marijuana bill
Manitoba Premier Brian Pallister wants the federal government to postpone legislation to legalize marijuana. The federal Liberals have promised the law in the spring, but Pallister says he and some other premiers have concerns that there are still many details to work out. Pallister says issues such as the minimum age for users, maximum strength of the pot and proper distribution are still up in the air. The Progressive Conservative premier also says there needs to be a large public awareness campaign about the dangers of driving while high. Pallister says he wants the provinces to have a common set of rules on marijuana. Canadian Press (570 News, Castanet)

Ontario cold to pot at LCBO, poll shows
Selling pot at the liquor store isn't sparking up overwhelming public support, according to stats released in a new poll. The Forum Research survey provided exclusively to the Toronto Sun found that more than a third of Ontarians (36%) think pharmacies are the best place to sell recreational pot, not the LCBO as Premier Kathleen Wynne has suggested. The survey says that specialized marijuana dispensaries rank second with 26% support while selling pot at the LCBO ranked lower with 16% support. "We have polled this issue nationally as well as provincially here in Ontario, and the answers are essentially the same; dispensaries and pharmacies are favoured as the best places to sell marijuana once it is legal, and the LCBO is not seen to be a favoured location," said Forum Research president Lorne Bozinoff. Toronto Sun

Ex-AFN leader teams with grower to bring medical marijuana to First nations
Phil Fontaine, the former national chief of the Assembly of First Nations, has teamed up with one of the first licensed cannabis growers to bring medical marijuana to First Nations. Indigenous Roots is a joint venture between Mr. Fontaine and Cronos Group, which operates the Peace Naturals Project in Ontario and The Zone Produce Ltd. in British Columbia. It would work co-operatively with First Nations to supply people living on and off reserves with the drug. In a news release issued Tuesday morning, the partners say the idea is to allow First Nations to invest, operate, and participate in the economic opportunities related to the emerging cannabis industry. (…) The Liberal government has promised to table legislation to legalize marijuana for recreational use in the spring of 2017, although it remains unclear when the drug will be taken off the prohibited list for the first time since 1923. Globe and Mail

PUBLIC SERVICE / FONCTION PUBLIQUE

Feds overpaid workers $56M
The malfunctioning Phoenix pay system that left thousands of Canada's public servants unpaid has also doled out millions of dollars in overpayments to 13,700 employees since its illfated launch. A letter sent to MPs on the government operations committee says a total of 20,600 public servants had received overpayments of more than $56 million by mid-October. The $5 6 millionin over payments were generated by two pay systems - the old clunky regional pay system and the new Phoenix system, whose first phase went live in February. The old pay system, which was decommissioned after the second phase of Phoenix was rolled out in April, generated $23 million in overpayments. Postmedia (Toronto Sun, A10)

Lack of pay irks workers in payroll snafu
The federal government's Phoenix payroll system continues to be plagued with problems, resulting in thousands of workers not getting paid for months. Roxanne Merrill Young is one of those workers. She is one of 80,000 federal government workers affected by the Phoenix pay problems since last spring. Merrill Young said she works as a seasonal employee at 5th Canadian Division Support Base Gagetown. She said she was part of a team of groundsworkers employed to repair streams and brooks on the base following military training exercises. Merrill Young said she received her first several pays on time. The next two were late, she said, and were sent by courier to her only after she made repeated phone calls asking for what she was owed. Now, she said, she's still waiting for a month's salary. "I have been told I could have to wait 10 to 12 weeks for this money. I think that's ridiculous," she said. And, she said, now the Department of Public Works has no record of employment for her so she is unable to apply for employment insurance. Daily Gleaner, A1

OTHER / AUTRES

Don't offload Syrian refugees on provinces, Senate committee tells feds
The Senate human rights committee is joining a chorus of voices raising concerns about thousands of Syrian refugees about to be shifted on to provincial assistance rolls. Committee chairman Sen. Jim Munson says the federal government has an ongoing responsibility to ensure that language training is provided so that 30,000 Syrians welcomed to Canada in the last year can successfully join the work force and society. Federally sponsored refugees are given a year's worth of supplementary benefits, but that assistance is about to expire and many thousands of the new arrivals still require help — which will fall to provincially funded programs. Canadian Press (Metro News); La Presse canadienne

Dion annonce 8 millions $ d'aide pour le Liban
Le ministre des Affaires étrangères, Stéphane Dion, a annoncé une aide de 8 millions $ pour le Liban, lundi, au cours d'une visite dans ce pays. Selon Affaires mondiales Canada, cette somme servira à aider le Liban à faire face à l'afflux de réfugiés syriens, à favoriser la participation des femmes dans la vie du pays et à soutenir les Forces armées libanaises dans leur lutte contre l'extrémisme. «Le Canada et le Liban entretiennent des liens forts et profonds, et nos deux pays continuent à travailler en étroite collaboration pour parvenir à la paix, la sécurité et la stabilité au Moyen-Orient», a déclaré M. Dion, dans un communiqué. Au cours de sa visite, le ministre Dion a, entre autres, visité deux campements de réfugiés auxquels le Canada collabore en fournissant de l'aide humanitaire. Le Liban accueille plus de 1 million de réfugiés, pour une population d'environ 4,5 millions de personnes. Journal de Montreal (Journal de Québec)

INTERNATIONAL

NATO chief trumpets new 'momentum' with EU military ties
NATO's chief says the alliance and the European Union are moving forward on deepening cooperation, as U.S. President-elect Donald Trump insists European allies start pulling their own military weight. NATO Secretary General Jens Stoltenberg told reporters before chairing talks between NATO foreign ministers Tuesday that "we have a momentum now." He said NATO and the EU would endorse 40 proposals for boosting cooperation on cyber security and hybrid threats, operations at sea and helping neighboring countries better defend themselves. Associated Press (Washington Post, New York Times)

Obama to tout counterterror legacy, even as Trump threatens changes
President Barack Obama plans to provide a final summation of his national security record Tuesday, reaffirming his counterterrorism strategy even as his successor has threatened to reverse course on many of Obama's priorities. During a speech at MacDill Air Force Base, the Florida headquarters of US Central Command and Special Operations Command, Obama plans to again argue for closing the naval prison at Guantanamo Bay and maintaining a ban on torture -- both areas where President-elect Donald Trump says he'll change course. The speech -- Obama's final major national security address -- was billed by the White House Monday as a wrap-up of his national security priorities over his eight years in

office. That tenure has included successes like the end to large-scale troop deployments in Iraq and Afghanistan and the killing of Osama bin Laden, but also new challenges like the rise of ISIS and its threats to Europe and the US homeland. CNN

Other Than ISIS: Half of U.S. Terror Suspects Support ISIS Rival Groups, New Report Details
Almost half of the suspects charged with terrorism offenses in the U.S. since the Syrian civil war began five years ago have not associated themselves with ISIS but with the group's bitter rivals such as al-Qaeda or embraced the broader jihadist ideology, a new study by George Washington University's Program on Extremism has found. While emphasis is often placed on whether ISIS directs or inspires terrorism suspects who attack or are arrested before carrying out attacks, the new study suggests that radicalization to Islamist violence will be a problem in the West far beyond the existence of ISIS or other groups because of an extreme ideology many find alluring. ABC News

We Don't Talk About 'Radicalization' When an Attacker Isn't Muslim. We Should.
Whenever a mass shooting or some other large-scale, incomprehensible attack occurs, the nation collectively holds its breath, waiting to see which set of cultural prejudices can be mobilized to frame the massacre. In the week before the election, when two officers from the Des Moines area were murdered in cold blood, a police spokesman may have gotten ahead of himself when he said that "there are some not-so-positive views of law enforcement that a certain segment of our population holds." What was probably being hinted at here was that the shooter had to be black and all worked up by the Black Lives Matter movement — a presumption immediately squelched once the suspect was identified as Scott Michael Greene, a white local who had enjoyed engaging in racial incitement by waving a Confederate flag at a high-school football game. NY Times

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

Ralph Goodale
Sur la colline avec @JustinTrudeau et le cabinet aujourd'hui, on se souvient des 14 vies précieuses perdues ce jour en 1989.

Ralph Goodale
All Canadians stand together against every form of gender-based violence

Alex Boutilier
As expected, Canada's privacy commissioners questioning the need for expanded police/spy powers in a formal submission to @RalphGoodale.

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

BC Government News
The Extreme Weather Response program enables communities to temporarily increase emergency shelter capacity, http://ow.ly/KPCx306QkiC

Nanaimo SAR
An important reminder that search and rescue is a free service in BC. http://fb.me/4oS0TPSfm

SARPreventionCanada
How much will it #cost if you need @BCSARAssoc ? @SARVAC_ACVRS #SARprevention #itsfree

AdventureSmart
Thx to @1035juicefm for helping us educate about #BCSAR @NelsonSAR2
http://www.mynelsonnow.com/23132/adventuresmart-promotes-three-ts/ … #SARprevention

Coquitlam SAR
#Prussik continues GSAR training learning grid search and other field search techniques. #SAR #SARelf

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Craig Forcese
Cdn privacy commissioners respond to gov's Green Paper consultation on nat'l security law and policy, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/nr-c_161206/ … #c51 #natsec

Althia Raj
Security can't trump privacy, watchdogs warn Trudeau #cdnpoli http://www.huffingtonpost.ca/2016/12/06/security-shouldn-t-trump-privacy-watchdogs-to-tell-trudeau-government_n_13456636.html … via @HuffPostCanada

HuffPost
Security can't trump privacy, watchdogs warn Trudeau http://huff.to/2hcKpdp #cdnpoli

iPolitics
Security shouldn't trump privacy, watchdogs tell Trudeau government http://ipoli.ca/2g63lP0 #cdnpoli

Amanda Connolly
"When data moves across borders...there's a loss of control," Therrien acknowledges when asked on impact of incoming Trump admin

Amanda Connolly
"We remain to be convinced. We do not think they have made their case:" Therrien

Amanda Connolly
"It's not as though there's an absence of tools," Therrien says re: #C51 and C13

Amanda Connolly
"You cannot create a backdoor only for law enforcement," Therrien notes.

Amanda Connolly
"Encryption is a benefit to society at large," Therrien acknowledged. "There is a real dilemma."

Amanda Connolly
Formal submission is signed by all provincial and territorial privacy commissioners

Amanda Connolly
Any new state powers must meet demonstrated need, not just be convenient for law enforcement: Therrien

Amanda Connolly
Privacy Commissioner Daniel Therrien speaking now about his submission to review of national security framework

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Michael Geist
BCCLA: Extra-territorial orders ("Equustek orders") should be available but rarely used. Proposing its own framework.

Michael Geist
Abella: What about cybercrime issues where there is a need for info disclosure? AGofCan: It's a different issue. Also points to MSFT case.

Michael Geist
AGofCan: Court should exercise restraint with judicial order. Has already recognized need to do so with the Internet.

Motherboard
Breaking: Hacker claims to push malicious firmware update to 3.2 million home routers http://bit.ly/2gNlfoX

Wired Magazine
What IBM's Watson has is a particular set of skills. Skills that make it a nightmare for cybercriminals of the world

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

NAACJ
It's been a decade since #AshleySmith died. Can you blame her mother for wanting to see #prisonreform? @CAEFS @CFCN_RCAFD @MOMSGroupOttawa

John Howard Society
Penitentiary tours continue | The Kingston Whig-Standard http://www.thewhig.com/2016/12/05/penitentiary-tours-continue ...

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS
The Globe and Mail
Firefighters' resources stretched thin as overdose rates soar in Vancouver area http://trib.al/pL97V8x From @andreawoo via @GlobeBC

NSPS (CboC)
RT @The_Fuzz74: Firefighters' resources stretched thin as overdose rates soar in Vancouver area /via @globeandmail

Police Montréal
Le SPVM se souvient avec tristesse du tragique événement de la @polymtl. Une pensée pour les victimes et familles. Ne les oublions jamais.

Ottawa Police
The flags at all Ottawa Police buildings will be at half mast today. We all have a role to play in ending the violence. #ActionsMatter

Canadian PM
PM Trudeau marks National Day of Remembrance and Action on Violence Against Women:

Statistics Canada
Measuring #violence against women: Statistical trends. http://ow.ly/kRBD306RIL5 #December6 #ActionsMatter

Kathleen Wynne
14 were killed at l'École Polytechnique simply because they were women. Today we remember them & recommit to ending violence against women.

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

Angela Sterritt
'Stop blaming Indigenous women for being murdered,' critic tells police

APTN National News
AFN BC regional chief issues apology, resigns #MMIW portfolio over Instagram photo: http://aptn.ca/news/2016/12/06/afn-bc-regional-chief-issues-apology-resigns-mmiw-portfolio-over-instagram-photo/ …

Tim Cook
B.C. regional AFN chief apologizes, steps away from missing women portfolio over instagram photo

AFN
Director of Communications for #MMIWG inquiry @Mike_Hutchins0n addresses the #AFNSCA

APTN National News
#mmiw nat'l inquiry spokesperson @Mike_Hutchins0n at #AFNSCA giving an update on inquiry work - "It takes time to do this right"

NWAC
Today we remember; every woman taken from us deserved dignity and respect. Where is our freedom from fear? #MMIW #actionsmatter #dec6

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Chinta Puxley
Manitoba calls on Ottawa to put brakes on legalizing marijuana. More coming from @stevelambertwpg #mbpoli #cdnpoli http://www.metronews.ca/news/winnipeg/2016/12/06/manitoba-premier-says-he-is-not-alone-in-wanting-delay-in-marijuana-bill.html?platform=hootsuite …

PUBLIC SERVICE / FONCTION PUBLIQUE

CBC Nova Scotia
Phoenix payroll woes 'demoralizing,' says federal employee after 10 weeks without pay http://ift.tt/2g4weuX

OTHER / AUTRES

La Presse
Ottawa doit aider à la pleine intégration des réfugiés syriens, dit un comité du Sénat

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

Today's News / Actualités
December 7, 2016 / le 7 décembre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Ralph Goodale plans to "increase gun safety and reduce gun violence"
In a letter to **Public Safety** portfolio employees, **Safety Minister Ralph Goodale** declared that he and **Public Safety Canada** are ***"developing [a] detailed plan needed to deliver on [their] commitments to increase gun safety and reduce gun violence."*** According to the letter, which was made public on **Public Safety Canada's** website, part of this plan is to reconstitute a firearms advisory committee that is supposedly to include experts in law enforcement, public health, agriculture, hunting, and recreation. Of note, however, was also the inclusion of experts from "women's groups" – something that has been

questioned by members the firearms industry who contend that emotion should not be used to undermine facts when determining federal policies and legislation. It is clear that the current government is intent on fulfilling its election platform on the issue of gun control, but exactly how they plan to achieve their goal remains to be seen. The announcement comes on the 27th anniversary of the École Polytechnique massacre where 25-year-old Marc Lépine shot and stabbed 14 women and wounded 14 others before taking his own life at the Montréal engineering school in December of 1989. Canadian Firearms Blog

TOP STORIES / MANCHETTES

'Running out of people:' Documents contradict Sask. RCMP vacancy claims
An internal memo from provincial RCMP suggests vacancy rates are posing a dire problem in Northern Saskatchewan. 650 CKOM obtained paper copies of an email thread dated Nov. 3 discussing the issue within the context of the Northern Sask. youth suicide crisis. A source claims the internal memo was later "retracted in fear of the truth getting out." The first email in the thread was allegedly sent by Supt. Grant St. Germaine, North District commander in Prince Albert, with the subject line: "Current HR Situation – North District – Provost Issues – Relief Request – La Ronge Detachment." "At the current time, the (North) District is operating 15 per cent short of bodies," it reads. (…) The issue of understaffing has plagued Sask. RCMP in recent months following an uptick in rural crime and the recent suicide crisis in the north. "We are running out of people. I hate to say that I can't see the light at the end of the tunnel, but I can't. We are in dire straits." (…) The email thread finishes with a note from Cpl. Devin Pugh with Indian Head detachment, where he asks for members to help – and to keep the memo quiet. "I ask that you do not share the attached email with anyone outside of this office!!"(sic) RCMP have not responded to a request for comment from 650 CKOM. 650 CKOM

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Could increased tanker traffic tank Vancouver's tourism industry?
Representatives of B.C.'s $15 billion tourism industry are apprehensive about the possibility of a devastating oil tanker spill if Kinder Morgan's Trans Mountain pipeline goes through. If constructed, the pipeline expansion project — which would triple the capacity of crude oil coming from Alberta — would increase tanker traffic on B.C.'s South Coast. While Federal Minister of Transport Marc Garneau promises a plan is in place to handle new tankers as well as an extra $200 million for a marine spill response program, Tourism Vancouver CEO Ty Speer is still worried about the impact of a devastating spill. CBC News

Weather to become more inclement as Earth gets warmer: Expert
The nation's top climatologist claims that the Earth is warming up so much that severe weather events involving heavy precipitation are becoming more likely. Environment Canada senior climatologist David Phillips said that Canada should be anticipating more heavy downpours in the near future, citing a recent report by the US Global Change Research Program that observed an increased frequency in downpours in the US (…) Warmer conditions could lead to inclement weather; while one area experiences drought, flooding could occur in another region. Tropical storms become stronger given the warmer temperatures and the number of tornadoes could swell as a result. Phillips argued that there is more than enough evidence to prove that Canada's weather is getting worse due to rising temperatures. Insurance Business.ca

BC Hazmat training today in North Saanich
Don't be alarmed if you see emergency personnel in North Saanich today, as it's most likely members of BCHazmat Management taking part in routine training. Under direction of ECRC and the Canadian Fuels Association, the groups will be conducting "Tanker Truck Rollover Training" at the BC HAZMAT training facility on McDonald Park Road as part of the Land Spill Emergency Preparedness Program. This program was set up to ensure consistent preparedness amongst responders and improve preparations in the event of land-based transportation incidents in the area. Much of the exercise will focus on non-sparking fuel transfers, grounding exercises, bonding practices and aluminum drilling. CHEK

Brace yourself! Intense snowstorm heading for West Coast tomorrow night
Environment Canada has some bad news for West Coast residents weary of the recent snow and cold temperatures: It's likely to get a lot worse before it gets better. That's because an "intense" Pacific storm is expected to batter Metro Vancouver and the rest of the South Coast region Thursday afternoon or evening with "a significant amount of snow (…)"With all the snow in the forecast, Vancouver city officials say they are already making plans with road crews and equipment is on standby. The province says it's also activating its emergency extreme weather shelter program, making an extra 1,000 emergency shelter beds available. CBC News; CTV News

Des gens de Lac-Mégantic à Ottawa pour interpeller Justin Trudeau
Se disant ignorés par les libéraux de Justin Trudeau, des citoyens de Lac-Mégantic se sont déplacés à Ottawa, mercredi, pour réclamer en personne la construction d'une voie ferrée qui contourne le centre de leur municipalité. «Par rapport à M. Trudeau, on a maintes et maintes fois adressé des demandes d'entretiens avec lui, on n'a eu aucun accusé de réception ni aucun signe de vie de la part de son bureau, a déploré en conférence de presse Robert Bellefleur, de la Coaliton citoyenne engagée pour une sécurité ferroviaire de Lac-Mégantic. C'est ce qui explique notre présence aujourd'hui.» La déception de M. Bellefleur est d'autant plus vive que selon lui, Justin Trudeau avait appuyé en campagne électorale le retrait des voies ferrées du centre-ville. Le ministre des Transports, Marc Garneau, dit attendre les résultats des études environnementales avant de trancher dans le dossier. Agence QMI (TVA Nouvelles)

Alberta, Saskatchewan ranchers brace for impact of bovine TB cull and quarantine
Farmers from more than 40 ranches in Alberta and Saskatchewan are wondering what kind of compensation and business lies ahead for them as the Canadian Food Inspection Agency (CFIA) cracks down on a bovine tuberculosis outbreak in Western Canada. In late September, the CFIA discovered a cow with bovine tuberculosis linked to Brad Osadczuk's ranch in Jenner, Alta., and launched an investigation which confirmed five other cases tied to his herd. It placed his entire operation under quarantine. CBC News

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Canadian Conservatives Want More Repression Against Protesters
Canadian conservative leaders appear to be taking cues from the militarized-police response in North Dakota. As Canadian Indigenous leaders draw inspiration from the recent victory at North Dakota, where the pipeline has been halted in search of alternate routes, conservative leaders in the Far North are sharpening their tools of repression. Appearing to take cues from the militarized police response in Morton County, Canadian Conservative leadership candidate Kellie Leitch is vowing to increase police repression, penalties and political push-back against pipeline protesters in that country. (…) Environemtal lobbying is already considered a political activity for tax-exemption purposes, for example, and the repressive anti-terrorism bill C-51, passed last year by the then-conservative government, already targets pipeline protesters using many of the proposed methods. Leitch's misguided attacks come on the heels of Canada's Prime Minister Justin Trudeau's approval of two controversial pipelines that have seen heavy opposition from Indigenous communities for years. Telesur

Surveillance state rolls on
An opinion piece states, "I hope the Federal Court of Canada invites the Canadian Security Intelligence Service (CSIS) to further explain the spying on journalists it may have conducted in the past. While the court may indeed have provided a warrant for such actions – a troubling development by itself – CSIS

also has a record of misleading the court about its intentions, breaching its duty of candour. The most decisive court in the land, the one that should support Senator Claude Carignan's private member's bill establishing stronger protections for journalists and their sources, is the conviction of Canadians. But, unfortunately, too many of us have acquiesced to the emergence of a surveillance state in our parliamentary democracy. Many have reasoned that they have nothing to fear from expansive government surveillance because they have nothing to hide. In the eyes of the surveillance state, however, your opinions about your innocence count for nothing. You won't know whether you have been spied on and you won't know what conclusions have been drawn. You won't know you are a target for "disruptive" actions, permitted by the Anti-Terrorism Act of 2015, the former Bill C-51." Toronto Star

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

NIL

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Evolving technology expected to introduce new cyber threats, broadened attacks: Trend Micro
The coming year is expected to witness evolving technology that introduces new cyber threats and attacks that broaden and differentiate to penetrate new vulnerable surfaces, suggests a report issued Wednesday by Trend Micro Incorporated. The expectation is 2017 "will include an increased breadth and depth of attacks, with malicious threat actors differentiating their tactics to capitalize on the changing technology landscape," Trend Micro, a cyber security solution provider, notes in releasing The Next Tier – 8 Security Predictions for 2017. "People waking up to the threat landscape of 2017 will say it is both familiar and unchartered terrain," the report points out. Canadian Underwriter

Russia Updates Plan to Counter Cyberattacks and Foreign Influence
The Kremlin published a new plan on Tuesday to defend Russia against what it described as stepped-up cyberattacks and "information-psychological" methods by foreign intelligence agencies bent on influencing its population with online information. The plan updates a similar information security doctrine put in place by President Vladimir V. Putin in 2000, early in his first term, that staked out a renewed role for post-Soviet government in monitoring information. The latest iteration of the doctrine comes as American officials have mulled retaliating against Russia for what the Department of Homeland Security said was government-orchestrated hacking before the presidential election, including stealing emails from the Democratic National Committee. New York Times; Bloomberg

LAW ENFORCEMENT / APPLICATION DE LA LOI

'Running out of people:' Documents contradict Sask. RCMP vacancy claims
An internal memo from provincial RCMP suggests vacancy rates are posing a dire problem in Northern Saskatchewan. 650 CKOM obtained paper copies of an email thread dated Nov. 3 discussing the issue within the context of the Northern Sask. youth suicide crisis. A source claims the internal memo was later "retracted in fear of the truth getting out." The first email in the thread was allegedly sent by Supt. Grant St. Germaine, North District commander in Prince Albert, with the subject line: "Current HR Situation – North District – Provost Issues – Relief Request – La Ronge Detachment." "At the current time, the (North) District is operating 15 per cent short of bodies," it reads. (…) The issue of understaffing has plagued Sask. RCMP in recent months following an uptick in rural crime and the recent suicide crisis in the north. "We are running out of people. I hate to say that I can't see the light at the end of the tunnel, but I can't. We are in dire straits." (…) The email thread finishes with a note from Cpl. Devin Pugh with Indian Head detachment, where he asks for members to help – and to keep the memo quiet. "I ask that you do not share the attached email with anyone outside of this office!!"(sic) RCMP have not responded to a request for comment from 650 CKOM. 650 CKOM

Tragic riddle of Canadian Mountie who killed himself in a Manchester hotel on his birthday
A decorated Canadian Mountie with a 'troubling' history of mental health problems killed himself in a Manchester hotel on his birthday during a celebratory trip to the city with his girlfriend. Robert Archibald, 28, served with the Royal Canadian Mounted Police as a federal air marshall, flying armed on planes across the world. A decorated Canadian Mountie with a 'troubling' history of mental health problems killed himself in a Manchester hotel on his birthday during a celebratory trip to the city with his girlfriend. Robert Archibald, 28, served with the Royal Canadian Mounted Police as a federal air marshall, flying armed on planes across the world. (…) He said his brother was also 'very worried' about his job. His partner Ms Lau, an air stewardess who met Mr Archibald in Vancouver, said in a statement that he had been told to take two or three weeks off work because of an old back injury. Manchester Evening News UK

Complaint launched against several Whistler RCMP officers
An official public complaint has been launched against several police officers from the Whistler RCMP. Officer in Charge of Sea to Sky RCMP Inspector Kara Triance, says she's aware that the complaint is in regard to the officers alleged conduct during an interaction with a member of the public where the complainant's cell phone was seized. Triance says that in her preliminary review of the file several components in the public complaint report and the text of the officers' report were unclear and warrants further review. A comprehensive review will be undertaken and the investigation will include interviewing the member of the public that made the complaint, the officers involved, witnesses and any video footage available. Mountain FM

RCMP Charge Calgary Man with Conspiracy to Bribe Thai Officials
The Royal Canadian Mounted Police (RCMP) have recently laid charges against the president of a Canadian commercial aircraft company under the federal *Corruption of Foreign Public Officials Act* (CFPOA), for allegedly conspiring to bribe Thai public officials. It is alleged that this individual conspired to bribe Thai military officials in relation to a proposed deal involving a commercial aircraft from Thailand's national airline. The CFPOA is Canada's primary anti-corruption statute and is focused on combating bribery and corruption of foreign public officials. The scope and reach of the CFPOA is wide-ranging. It applies to the worldwide conduct of Canadian citizens, permanent residents, corporations, and other business organizations. Charges were laid as a result of a lengthy investigation by the RCMP's Federal Serious and Organized Crime Unit, initiated after a tip from the U.S. Federal Bureau of Investigation in 2013. This is the fourth investigation resulting in charges under the CFPOA in Alberta. JD Supra

RCMP in Alberta arrest man who escaped in prisoner transport van
RCMP have arrested a man who escaped from an Alberta Sheriff by stealing a prisoner transport van. Police say a man drove off from the Fort McMurray court house on Monday afternoon in the vehicle. RCMP then received a complaint about a dangerous driver. Mounties say they located the abandoned van in the city and arrested a man who they found nearby. Lyndon Rankin, who is 21, faces escaping lawful custody, dangerous driving and other charges. Canadian Press (Metro News); CBC News

Five people charged, another at large after drugs seized in Grand Rapids and Chemawawin
Five people are facing charges and another is still being sought by police after search warrants were executed in Grand Rapids and Chemawawin Dec. 2-3. RCMP arrested 53-year-old Wilfred Angus Turner, 21-year-old Phyllis Annette Dawn Scott and 28-year-old Jacob Wilfred Ducharme of Grand Rapids after executing a search warrant Dec. 2 and seizing cocaine, pills, marijuana, drug paraphernalia and ammunition. Turner and Scott are charged with possession of cocaine for the purpose of trafficking, while Ducharme is charged with possession of cocaine for the purpose of trafficking and possession of ammunition contrary to a court order. Grand Rapids RCMP are still seeking 35-year-old Kenneth Robert Sanderson of Grand Rapids in connection with the investigation. (…)Grand Rapids and Chemawawin RCMP were assisted by the Integrated Gang Intelligence Unit, the RCMP North District Crime Reduction Enforcement Support Team, the RCMP Emergency Response Team and Police Dog Services in executing the warrants. Thompson Citizen

Police incident in Cloverdale ends but little information released
A police incident in Cloverdale is now over but RCMP is not releasing much information about what happened at this time. Concerned witnesses told Global News Tuesday night there were a large number

of officers at 184 Street and 60 Avenue, starting in the afternoon .Investigators were there until late Tuesday night .The reason is still unclear but many evidence markers could be seen on the ground and police tape had been put up. Despite several requests for information, Surrey RCMP is not commenting on the nature of the investigation. Digital Cameras Planet

Waterville area resident deprived of thousands by fraud
A Waterville area resident is out $4,000 after being scammed recently. Kings District RCMP learned of the loss after a man in his 50s reported what is known as a consignment box scam. According to community policing officer Constab. Kelli Gaudet, the fraud involved a phony diplomat from Ghana and gold, diamonds and cash allegedly worth $30 million. Gaudet stated, "if it sounds too good to be true, it probably is." The RCMP nationally warn Canadians to watch out for the Nigerian/West-African Business letter scam. For years now, a release indicates, businesses, learning institutions, and government departments have been receiving e-mails from senders posing as Nigerian/West-African government or business officials offering to share large sums of money. The police recommend careful research before conducting such transactions. The Commercial Crime Sections of the RCMP within Canada and the Better Business Bureau are available for obtaining further information on this topic along with the Canadian Anti-Fraud Call Centre (CAFC). Kings County News (Annapolis County Spectator)

Drug awareness session held for parents in the Lewisporte area
You could hear a pin drop. Retired RCMP officer Harold Nippard was addressing a crowd of about 60 parents at a drug awareness session at Lewisporte Collegiate on Nov. 28. The parents were of students from Grades 5-12. Collegiate principal Krista Freake explained why they invited parents of younger children — Grade 5 students are 10-11 years old. "Drug use is happening in much lower grades than in the past," she said. "Some parents have little to no information about what drugs are available, what they look like and the side effects they have and we want to start the conversation." Nippard shared the shocking reality of what drugs are available in Lewisporte and surrounding communities. Lewisporte Pilot

Yukon gets a new top mountie
Scott Sheppard replaces longtime Chief Superintendent Peter Clark. Yukon RCMP are welcoming a new commanding officer. Chief Superintendent Scott Sheppard is taking over as M division's top cop. Sheppard is a 27 year veteran of the RCMP and has a variety of experience involving front line community policing in First Nation communities, covert and undercover operations, as well as critical incidents. In a release, Sheppard says he's really looking forward to working with partners to address the needs and expectations of Yukoners. CKRW

Organized crime group in Alberta, B.C. dismantled with 10 arrests, police say
Ten people have been arrested and 111 charges laid in the dismantling of a Calgary-based organized crime group that operated in Alberta and B.C., police say. The charges relate to drugs, firearms, and organized crime, police said in a release. The investigation by ALERT Calgary's organized crime and gang team began in November 2015 and concluded a year later with the arrest of Timothy Varga, 40, from Calgary. ALERT alleges that Varga was the central figure in a criminal network that extended from Alberta to British Columbia and had ties to Manitoba. CBC News

La Sûreté du Québec reste à Lac-Simon, insiste le porte-parole de la SQ
À Lac-Simon, il est « hors de question qu'il y ait un retrait unilatéral de la Sûreté du Québec », affirme le capitaine Guy Lapointe, porte-parole de la Sûreté du Québec. À l'instar du ministre de la Sécurité publique, Martin Coiteux, le capitaine Lapointe dément formellement l'information ayant circulé à l'effet que la SQ ait l'intention de se retirer de Lac-Simon suite à des propos tenus par la chef de la communauté. « Nous croyons toujours que la desserte par la Sûreté du Québec est une solution temporaire et qu'il est souhaitable que le Service de police Lac-Simon retrouve son autonomie. Maintenant, il n'est pas question d'un retrait unilatéral. Ce sont des discussions qui sont en cours à différents niveaux et la Sûreté du Québec ne compte pas se retirer sans avoir la confirmation du chef de police de Lac-Simon qu'ils sont en mesure d'assurer la desserte », a précisé Guy Lapointe sur les ondes de l'émission *Des matins en or*. Radio-Canada; Agence QMI (Journal de Québec, Journal de Montréal)

Broadcast Media / Médias télédiffusés :

The John Gormley Show reported on an internal memo obtained by CKOM that sheds new light on the severity of RCMP staffing shortages in detachments in northern Saskatchewan. (650 CKOM, 8:30 CST)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

New reform committee seeks
A new elders council has been formed to assist in offering advice and council to the attorney General of Ontario as they seek a more culturally responsive justice system in light of the disproportionate incarceration levels of First Nations people. Thirteen indigenous elders from across Canada have been chosen to represent the indigenous worldview and culture as Ontario moves forward in recognizing round pegs do not easily fit in square holes. Not yet one year in office, Trudeau took the brunt of former Harper Conservative government in its failure in providing rehabilitation programs for indigenous offenders, and the few number of incarcerated indigenous men and women who can afford bail, forcing them to serve maximum time in jail or prison. Auditor general Michael Ferguson was highly critical of Correctional Services Canada calling the situation "beyond unacceptable". Two Row Times

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Le Service de police du Grand Sudbury veut se protéger du fentanyl
Le service de police de la ville du Grand Sudbury profite des discussions budgétaires pour demander du financement supplémentaire, destiné à l'achat de naloxone. Il s'agit d'un composé chimique capable d'inverser les effets des opiacés tels que le fentanyl. Le fentanyl peut être absorbé à travers la peau ou encore être inhalé dans l'air, exposant les policiers à un grand risque d'entrer en contact avec le médicament, selon le sergent-détective James Killeen. Comme cette drogue a fait son chemin dans les rues de la municipalité, les policiers veulent s'assurer d'une protection en tout temps. Le fentanyl est 100 fois plus puissant que la morphine. « Le naloxone est un produit périssable et il faut donc prévoir son renouvellement ponctuel, » explique le policier Killeen, qui n'a toutefois pas chiffré sa demande auprès du comité des finances de la ville du Grand Sudbury. Actuellement, Peterborough est la seule ville en Ontario qui fournit du naloxone à ses policiers. Radio-Canada

Sudbury cops say they need fentanyl antidote to save lives
Both authorities and addicts say that fentanyl packs a potent- but deadly - punch. Now the drug has made its way onto Sudbury's streets, and police are making sure they are ready to deal with its effects. Fentanyl can be absorbed through the skin or inhaled in the air, which puts police at greater risk of coming into contact with the drug. The new concern for police is that they can be accidentally exposed, said Detective Sergeant James Killeen of the Greater Sudbury Police Services. But that may be easier said than done. He wants to see naloxone, the the drug's antidote, made available to officers. "Something to be implemented would have to go into our budget. Naloxone is a spray that has an expiry date on it. So that's constantly going to have to get renewed, but it's kind of hard to put a price on saving somebody's life," Killeen said. "Naloxone is going to be basically an instant remedy that they can take. It's a nasal spray they can just spray up their nose and it'll counteract the effects of the fentanyl."Finding someone caught in a fentanyl overdose can be gruesome, Killeen said, and officers also need the training and possible fix to save lives. "It's something that we're just going to have to learn to adapt to and incorporate that as regular equipment for a police officer," he said. Killeen is in the process of writing the proposal to request funding for the naloxone, and any other equipment required to prevent exposure to fentanyl. Currently Peterborough is the only community in Ontario to supply its police officers with naloxone. CBC News

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

'She was Aboriginal. She had an addiction': Sister of MMIW says family had to push police
Bernadette Smith's sister Claudette Osborne went missing in 2008. She was 21-years-old and was last seen near a Winnipeg hotel. According to the Native Women's Association of Canada, in Manitoba there are 40 missing, 120 murdered and five suspicious deaths recorded in the MMIWG (Missing and Murdered Indigenous Women and Girls) database. There are 90 MMIWG recorded in Winnipeg. Two other relatives of Bernadette's have gone missing or have been murdered. Drag the Red, a volunteer-run organization that drags Winnipeg's Red River to search for traces of missing and murdered Indigenous women founded by Bernadette began as a personal mission. CBC News

A search for answers
When Jennifer Catcheway went missing in 2008, her mom, Bernice, was told by the RCMP officer to whom she'd reported it that she should give it a week-her daughter was probably just out on a bender. But Bernice knew the Mountie was wrong: Her loyal, responsible daughter had told her in a phone conversation that she'd be at her Portage la Prairie, Man., home that night to celebrate her 18th birthday. She never arrived. Bernice and Wilfred, Jennifer's father, believe the investigation into their daughter's disappearance was bungled, particularly in the crucial, early stages. Even weeks after Bernice reported her missing, officers had still not taken statements from family members who had been seen with her. "To put it bluntly," Wilfred told the CBC, "it's racism." This spring, hearings are slated to begin in the two-year federal inquiry into missing and murdered Indigenous women and girls (MMIW). They will come more than a year after the Liberals announced the inquiry and nine months after it officially launched (at this point, the inquiry still does not have a working website). But families continue to express their concern over one element that will not be part of the inquiry's agenda: A thorough review of police conduct. (…) The Catcheways are thrilled to finally have a federal ally in the inquiry. But they continue to work on their own, searching marshes, lakes and rivers and have put together a $10,000 reward for information. They've excavated three dumps and taken videotaped statements, hoping they might find out what happened. "We stopped relying on RCMP," Bernice recently told a Winnipeg MMIW forum. "I never got a call from [the officer] on her case." Maclean's

Families and lives of MMIW honoured at McMaster
McMaster University commemorated a plaque for the families of Murdered and Missing Indigenous Women (MMIW) yesterday on campus — a large step forward considering not so long ago indigenous people would lose their status as an Indian for simply attending a post-secondary school. The commemoration ceremony, was held on December 6 on the National Day of Remembrance and Action Against Violence on MMIW and was organized by the Anti-Violence Network and Indigenous Studies Program. The national day of remembrance was established to remember the 14 women murdered on December 6, 1989 in the event also known as the "Montreal Massacre", the five women from the McMaster community who have been murdered and to remember the 1,200 or more indigenous women and girls who have been murdered or unaccounted for. (…)Dr. Robyn Bourgeois gave the keynote address and spoke with an emphasis on how the government has and is currently dealing with indigenous issues that all come back to an apparent lack of effort on the MMIW inquiry. Two Row Times

Sex abuse linked to suicide: grand chief
appears to be a direct correlation between alleged sexual abuse on northern Ontario reserves and a number of recent suicides involving young girls, says Nishnawbe Aski Nation Grand Chief Alvin Fiddler. Fiddler, whose organization represents 49 of Ontario's First Nation communities, says high rates of abuse are also being reported to police in his territory. "The victims of these suicides are young girls, young women," he said in an interview. (…) Officers and nurses also require appropriate tools to gather evidence in the immediate aftermath of an incident because they lack sexual assault forensic evidence kits, he said. Sexual abuse was also a consistent theme raised during the sessions held as the Liberal government looked to design the inquiry into missing and murdered women. Waterloo Region Record

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Marijuana use on rise in Ontario, as is driving under pot's influence, CAMH finds
With Ottawa poised to legalize recreational marijuana next year, researchers are keeping a close eye on use of the so-called demon weed, which has been steadily trending upward over the last couple of decades. In Ontario, for instance, a survey released Wednesday by the Centre for Addiction and Mental Health (CAMH) found that year cannabis use virtually doubled between 1996 and 2015, rising from about 8 per cent to almost 15 per cent of respondents. Significant increases were found among all age groups, but especially among 18- to 29-year-olds, with the proportion of pot smokers jumping from about 18 per cent in 1996 to 38 per cent in 2015. "We also see that the cannabis-using population is aging, as well," said senior scientist Robert Mann, who co-authored the CAMH Monitor report on substance use and mental health status among a representative sample of more than 5,000 Ontario adults. (…) The CAMH Monitor is a collection of survey data that has been published every two years for almost the last four decades, allowing researchers to track long-term trends in the use of alcohol, drugs and tobacco, as well as identifying problematic behaviours related to mental health within the province's population. One finding of particular concern is the proportion of respondents who reported getting behind the wheel after using cannabis. In the last five years, that figure doubled, rising to 3 per cent in 2015 from 1.5 per cent in 2010. Toronto Star

Selling a fairer economy
An opinion piece states, "Few saw the one-two punch thrown by global politics in 2016 coming. Like a set-up jab to the body, Brits voted to exit the European Union. And then, like an even harder follow-up cross to the head, Americans voted Donald Trump into the presidency. The world was left seeing stars. But maybe, if this isn't giving Canada's most famous boxer too much credit as a fight strategist, we might have braced ourselves for the blows if we'd been listening more closely to Justin Trudeau. (…) On other highly controversial files, circling back to that mantra about helping the middle class will be even trickier. Trudeau's vow to legalize and regulate marijuana-the first bold policy initiative he signalled as Liberal leader-is supposed to be fulfilled by legislation in 2017. But marijuana entrepreneurs aren't waiting for a law to be passed, and Trudeau recently expressed frustration at the way storefront pot dispensaries have sprung up in anticipation of the change. Anne McLellan, who was justice minister in the former Liberal government of prime minister Jean Chrétien, headed a task force on marijuana that is slated to deliver its report this week. McLellan was said to favour a restrictive policy, aimed at keeping pot away from young people. But exactly how Trudeau intends to liberalize marijuana policy, while also turning the clock back on the freewheeling weed marketplace that has emerged in recent months, will be a tough test." Maclean's

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Les Occidentaux réclament un « cessez-le-feu immédiat » à Alep
Au moment où l'armée syrienne a repris le contrôle de la vieille ville d'Alep, six pays occidentaux - La France, l'Allemagne, le Canada, les États-Unis, l'Italie et Royaume-Uni - réclament un « cessez-le-feu immédiat » devant la « catastrophe humanitaire » qui sévit dans ce fief de la rébellion syrienne. Appuyés par le secrétaire général de l'ONU, Ban Ki-moon, les six pays occidentaux exhortent la Russie et l'Iran à utiliser leur influence auprès du régime syrien pour l'infléchir en ce sens. « L'urgence absolue est un cessez-le-feu immédiat pour permettre aux Nations unies de livrer de l'aide humanitaire aux populations de l'est d'Alep et de porter secours à ceux qui ont fui », soulignent les six dirigeants dans une déclaration commune. Nous condamnons les actions du régime syrien et de ses partisans étrangers, en particulier la Russie, pour leur obstruction à l'aide humanitaire, et nous condamnons fermement les attaques du

régime syrien qui ont dévasté des installations civiles et médicales ainsi que l'utilisation de barils explosifs et d'armes chimiques. Radio-Canada

Family reunification wait times for immigrants to be cut by half, John McCallum says
Newcomers to Canada will soon have a much shorter wait to reunite with their spouses, partners and children. Immigration, Refugees and Citizenship Minister John McCallum announced today in Brampton, Ont., that the current average two-year processing period will be reduced to 12 months. The new one-year guarantee will apply to applications already in the queue and new applicants. "This will be of direct benefit to the 64,000 spouses we will admit to Canada in the coming year," he said. CBC News

INTERNATIONAL

American and British Spy Agencies Targeted In-Flight Mobile Phone Use
In the trove of documents provided by former National Security Agency contractor Edward Snowden is a treasure. It begins with a riddle: "What do the President of Pakistan, a cigar smuggler, an arms dealer, a counterterrorism target, and a combatting proliferation target have in common? They all used their everyday GSM phone during a flight (…) In a 2012 presentation, Government Communications Headquarters, or GCHQ, the British equivalent of the NSA, in turn disclosed a program called "Southwinds," which was used to gather all the cellular activity, voice communication, data, metadata, and content of calls on board commercial aircraft. The document, designated "top secret strap," one of the highest British classification levels, said the program was still restricted to the regions covered by satellites from British telecommunications provider Inmarsat: Europe, the Middle East, and Africa (…)Le Monde examined information about the surveillance of aircraft and their passengers around the world between 2005 and 2013, including unpublished documents from the Snowden archives; the evidence demonstrates that from an early date, Air France drew particular attention from the United States and the United Kingdom. Air France was targeted as early as 2005, as disclosed in an NSA document setting out the broad outline of a program for "worldwide civilian aircraft tracking. The Intercept; Le Monde

Europe Presses American Tech Companies to Tackle Hate Speech
European officials pushed on Tuesday for American technology giants to do more to tackle online hate speech across the region, adding to the chorus of policy makers worldwide demanding greater action from the likes of Facebook, Google and Twitter. The rebuke came a day after many of those companies announced that they were joining forces to fight the spread of terrorist content on the internet, agreeing to share technology and information to prevent propaganda and other dangerous materials from being disseminated on their services. New York Times

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

Can Firearms Blog
Ralph Goodale plans to "increase gun safety and reduce gun violence" https://canadianfirearmsblog.ca/ralph-goodale-developing-plans-increase-gun-safety/ …

Dale Hunter
Wall had conversation with sask minister Ralph Goodale. They agreed on some things. Disagreed on others. @ctvregina

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Canadian Red Cross

Our CEO @ConradSauve met with Arianna Johnson from @WBFoodBank for an update on the great work the food bank is doing 7 months after #ABfire

CKNW
Our friends at @GlobalNews made the 2016 YouTube? Top 10 Trending list with coverage of Fort McMurray fire. http://bit.ly/2gUdTjt

Saskatoon EMO
The test is today at 10 am. If you haven't already signed up do so at http://Saskatoon.ca/notifynow and find out first hand how it works

Red Cross in Ontario
Do you have these essential #winter supplies in your vehicle? #beready

Postmedia News
Sajjan to announce Airbus C-295 aircraft as winner of fixed wing search and rescue project

Ottawa Citizen
Search and rescue aircraft announcement could take heat off Liberals on fighter jet controversy

BCSARA
@BCSARAssoc groups look forward to these new #BCSAR tools for our partner agencies!

Coquitlam SAR
All #SAR members undergo basic helicopter orientation & hover exit training. #Prussik can fly, but who passes up a helicopter ride! #SARelf

TVA Nouvelles
Des gens de Lac-Mégantic à Ottawa pour interpeller Justin Trudeau http://bit.ly/2hjxPsY

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

Jim Bronskill
Spies should not be allowed to keep innocent people's data, privacy czars say http://www.metronews.ca/news/canada/2016/12/06/security-shouldn-t-trump-privacy-watchdogs-to-tell-trudeau-government.html .... #cdnpoli #hw

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CTV Vancouver
Should the government attempt to regulate B.C.'s birth tourism industry?

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

SC Media
Cybersecurity pros tell Trump to heed commission's recommendations

LAW ENFORCEMENT / APPLICATION DE LA LOI

ICLMG
The #RCMP still won't admit they use #Stingrays even though we've already proven they do https://news.vice.com/story/rcmp-still-wont-admit-that-it-uses-these-high-power-spying-tools-even-though-they-do ... @vicenews #cdnpoli #privacy

CTV News
One week after Jennifer Hillier-Penney was last seen, RCMP in N.L. say her disappearance is considered suspicious http://ow.ly/KFTS306U7HU

Lucas Meyer
The RCMP and Alberta Securities Commission are partnering on enforcement of securities laws #yyc

Dave Gilson
ASC and RCMP launch new joint investigative team to tackle white collar crime in AB. #yyc #cbc

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

VICE Canada
More than a quarter of Ontario's prisoners have mental health issues. That's a huge problem:

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

AFN
Powerful dialogue on #FirstNations child welfare this morning ft. @cblackst of @Caringsociety #AFNSCA

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

CBC News – The Current
"We can't forget these families are grieving and they want answers." @wpgpolice Chief Danny Smyth #TheCurrentMMIW http://www.cbc.ca/1.3883647

CBC – The Current
"Even 10 years ago, some women chiefs were told this is a woman's issue.": @shenorthwilson #TheCurrentMMIW http://www.cbc.ca/1.3883730

CBC – The Current
Red River is Winnipeg's "Highway of Tears." Families speak at #thecurrentMMIW public forum. http://www.cbc.ca/1.3883544

CBC – The Current
"When they did release her picture, it was her mug shot" LISTEN to #thecurrentMMIW special DEC. 7 http://cbc.ca/thecurrent

CRCVC
Police hope 5 people hold clues to help solve 1998 MMIW cold case

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

Globalnews.ca
On the surface, it makes sense to treat stoned driving like drunk driving. But it's complicated

CBC News
Marijuana use on rise, as is driving under drug's influence, Ontario survey finds http://www.cbc.ca/1.3884896

iPolitics
Toronto board of health wants feds to allow pharmacies to sell pot @Kyle_Duggan reports. | AP Photo http://ipoli.ca/2qb9HHV #cdnpoli

OTHER / AUTRES

CBC News
Family reunification wait times for immigrants to be cut by half, John McCallum says http://www.cbc.ca/1.3885129

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

Today's News / Actualités
December 8, 2016 / le 8 décembre 2016
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

NIL

TOP STORIES / MANCHETTES

Montérégie: la GRC saisit 127kg de cocaïne
La Gendarmerie royale du Canada (GRC) rapporte jeudi qu'une saisie de 127 kilogrammes de cocaïne a été faite par ses policiers durant une enquête qui a permis l'arrestation en début de journée de trois

personnes. Ces suspects auraient aussi été impliqués dans du trafic de cannabis et de tabac illégal. Le stratagème auquel ils auraient participé aurait permis d'importer de grandes quantités de cocaïne au Canada qui passaient en transit par Los Angeles et Houston avant d'être destinées au marché de Montréal. Presse canadienne (Journal Métro, La Presse, Radio-Canada) ; CTV News ; Journal de Montréal ; Metro News

Fake job, fake education, fake residency: 15 clients of fraudulent immigration scheme now kicked out of Canada

Fifteen former clients of an imprisoned B.C. immigration consultant have now been deported to China. And the failed appeals by two women who fought to remain in Canada provide a rare glimpse into the illegal tactics used to carry out what has been labelled as the biggest immigration scam in B.C. history. Immigration Appeal Division transcripts obtained by CBC News detail lies and deceptions that include one immigrant pretending to attend university in B.C. while actually obtaining an education outside the country. Another fraudulently claimed to work for a fictitious B.C.-based company while in fact living in China. The two unrelated women have been stripped of their permanent residency status for lying about their eligibility and will be unable to return to Canada for five years — unless they receive permission from immigration officials to come back sooner. They were among 1,200 clients of Xun "Sunny" Wang and his now defunct companies New Can Consultants and Wellong International Investments. Wang is serving seven years in prison for immigration fraud. The Canada Border Services Agency alleges 120 of Wang's former customers obtained permanent residency under false pretences. And more than 200 others may have lied in order to become Canadian citizens. The CBSA says another 500 ex-clients are also under investigation, bringing the total facing possible deportation to more than 800. So far, 44 removal orders have been issued, but some have pending appeals. CBC News

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Airbus chosen to build Canada's new search planes, ending 12-year procurement odyssey

The Canadian military will receive new fixed-wing search and rescue planes in a two-step procurement that will cost taxpayers $4.7 billion over the next two decades. The selection of European defence giant Airbus end a 12-year, frustrating odyssey that spans three governments. Defence Minister Harjit Sajjan, Public Works Minister Judy Foote and the Commander of the Royal Canadian Air Force, Lt.-Gen. Michael Hood, announced the deal at the country's largest military air base in Trenton, Ont., which is also one of the principal search and rescue stations. The first phase — with a pricetag of $2.4 billion — involves the purchase of 16 C-295W aircraft modified for search and rescue missions. A training simulator, to be located in Comox, B.C., and 11 years of in-service support and maintenance will be included. An additional in-service support program will have to be negotiated with Airbus. That cost is estimated at $2.3 billion. CBC News; Reuters (Globe and Mail); Ottawa Citizen; Presse Canadienne (L'actualité); Canadian Press (City News)

Liberal government brings in defence analysts for briefing on how to sell search and rescue aircraft decision

The Department of National Defence is bringing in defence analysts for a special meeting designed to sell the Canadian public on the Liberal's search and rescue aircraft announcement. Canada will purchase 16 Airbus C-295 planes, it was announced today. The meeting between analysts and top government and military procurement officials takes place at 1 p.m. today. The analysts will be given government talking points and information on the aircraft deal and are expected to relay that data during TV, print and radio interviews, sources say. Thirteen individuals will be provided with the information at the meeting. Procurement Minister Judy Foote and Harjit Sajjan announced the search and rescue purchase today at Trenton.

Months into Fort McMurray's wildfire recovery, compassion fatigue could be settling in

The seven-month mark of Fort McMurray's wildfire recovery is a dark time for some of the city's frontline social and aid workers. The hours of sunlight in Canada's oilsands capital are few but there are thousands of residents downloading stories of stress and trauma on crisis support workers. It's enough to

raise worries some support workers could be suffering from compassion fatigue, even within one of the city's crisis agencies. CBC News

Search underway for missing Murray Harbour P.E.I. man
A search for a missing 68-year-old man is underway on Prince Edward Island. Alan Richards of Murray Harbour, P.E.I. was reported missing Wednesday when he failed to show up for work. An air, water, and ground search is underway in the Cape Bear area of Kings County, with Kings District RCMP, PEI Ground Search and Rescue, and the Joint Rescue Coordination Centre taking part. They are also searching on and from the water. CTV News; Guardian; CBC News

Harbour search continues for Jennifer Hillier-Penney, missing for 8 days
A search of the harbour in St. Anthony has moved into its second day, as the probe for clues in the disappearance of Jennifer Hillier-Penney continues. RCMP Cpl. Trevor O'Keefe confirmed the search of the harbour is ongoing Thursday, with the assistance of divers. The overall search has resulted in extra police officers called into the Northern Peninsula community, along with a K-9 unit, helicopters and ground search and rescue. CBC News

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

NIL

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Security hasn't been increased at Toronto-area high school following threat
Security has not been increased at Oakwood Collegiate Institute in the wake of police arresting a 17-year-old boy who allegedly threatened to attack the west-end school on the 27th anniversary of the massacre at École Polytechnique de Montréal on Tuesday. The suspect is alleged to have made the threat in a post on an unspecified blog on Dec. 1. A search warrant was then executed at the suspect's home early Tuesday morning and a number of weapons – including a machete, a hatchet, two swords, four knives and several arrows for a longbow – were seized. (...)TDSB officials say that that the doors to Oakwood Collegiate Institute are locked during the school day, as per board policy. Two Toronto police resource officers are also posted at the school, along with a TDSB hall monitor. As well, there are 26 security cameras at the school. "It's a pretty secure facility," TDSB Spokesperson Shari Schwartz-Maltz said on Thursday. CTV News

Canada spy official doubts intelligence-sharing under Trump: report
The Canadian official who oversees the country's spies says Ottawa may have to rethink how it provides intelligence to the United States, given incoming President Donald Trump's views on torture, a newspaper reported on Thursday. Canada is a member of the so-called Five Eyes intelligence-sharing network, including the United States, Britain, Australia and New Zealand. Michael Doucet, executive director of the Security Intelligence Review Committee (SIRC), said Canada did not want information derived from torture. "They may have a new administration that thinks torture is a good thing," he told a private Toronto audience last week, according to The Globe and Mail, which cited a recording of the remarks. "It's going to be an interesting and challenging time, and we've got to think about what defines us as Canadians." SIRC is a watchdog agency that reviews the activities of the Canadian Security Intelligence Service, or CSIS. During the election campaign, Trump said the United States should use waterboarding and other harsh interrogation techniques when questioning terror suspects. Neither SIRC nor CSIS was immediately available to comment. Reuters

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Fake job, fake education, fake residency: 15 clients of fraudulent immigration scheme now kicked out of Canada
Fifteen former clients of an imprisoned B.C. immigration consultant have now been deported to China. And the failed appeals by two women who fought to remain in Canada provide a rare glimpse into the illegal tactics used to carry out what has been labelled as the biggest immigration scam in B.C. history. Immigration Appeal Division transcripts obtained by CBC News detail lies and deceptions that include one immigrant pretending to attend university in B.C. while actually obtaining an education outside the country. Another fraudulently claimed to work for a fictitious B.C.-based company while in fact living in China. The two unrelated women have been stripped of their permanent residency status for lying about their eligibility and will be unable to return to Canada for five years — unless they receive permission from immigration officials to come back sooner. They were among 1,200 clients of Xun "Sunny" Wang and his now defunct companies New Can Consultants and Wellong International Investments. Wang is serving seven years in prison for immigration fraud. The Canada Border Services Agency alleges 120 of Wang's former customers obtained permanent residency under false pretences. And more than 200 others may have lied in order to become Canadian citizens. The CBSA says another 500 ex-clients are also under investigation, bringing the total facing possible deportation to more than 800. So far, 44 removal orders have been issued, but some have pending appeals. CBC News

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Zeus Variant 'Floki Bot' Targets PoS Data
Researchers have observed an uptick in attacks using the banking malware Floki Bot against U.S., Canadian and Brazilian banks, and insurance firms. Floki Bot, which uses code from the once notorious Zeus banking Trojan, has evolved and unlike its predecessor, is targeting point-of-sale systems via aggressive spear phishing campaigns and the RIG exploit kit. Cisco Talos and Flashpoint security researchers coordinated the release of reports on Floki Bot on Wednesday. Both firms warn the malware is quickly gaining popularity within Dark Web criminal forums. Threat Post; Security Week

Hackers Gamify DDoS Attacks With Collaborative Platform
A Turkish hacking crew is luring participants to join its DDoS platform to compete with peers to earn redeemable points that are exchangeable for hacking tools and click-fraud software. The goal, security researchers say, is to "gamify" DDoS attacks in order to attract a critical mass of hackers working toward a unified goal. The hacking platform is called Surface Defense and is being promoted in Turkish-language Dark Web forums including Turkhackteam and Root Developer, according to Forcepoint Security Labs, the security firm that first uncovered and reported the DDoS platform. Promoters of Surface Defense are actively recruiting Turkish hackers that may be sympathetic to Turkish nationalist beliefs, Forcepoint believes. Targets of the DDoS attacks range from the Kurdistan Workers Party, German Christian Democratic Party and the Armenian National Institute website in Washington D.C., said Carl Leonard, principal security analyst at Forcepoint. Threat Post; Softpedia; Bleeping Computer; ZD Net

Backdoor vulnerabilities discovered in Sony IP cameras
Researchers have discovered backdoors in Sony IPELA Engine IP cameras which could affect as many as 80 models. Cybersecurity firm SEC Consult said on Wednesday that the security flaw allows attackers to remotely execute code, hijack vulnerable cameras, disrupt device functionality, and spy on users. In addition, the backdoor grants attackers the opportunity to add compromised Sony IP cameras to botnets as slave nodes, in the same manner that cyberattackers used the IoT-based Mirai botnet to disrupt online services. ZD Net; Help Net Security; Bleeping Computer

Flash Player Security Flaws Used in Most Exploit Kits, Security Research Shows
Flash Player continues to put computers across the world at risk due to its vulnerabilities and a new research conducted by RecordedFuture shows that cybercriminals are still looking for security flaws in Adobe's solution to compromise computers. A total of 6 of the top 10 vulnerabilities used by exploit kits this year impacted Adobe Flash Player, with just one security flaw being targeted by no less than seven exploits. Softpedia

Google Fixes 74 Android Security Flaws with December Patches
Google has rolled out two security patches for Android devices earlier this month that address a total of 74 vulnerabilities in the operating system, including 11 that are rated as critical. Specifically, Google's December 2016 security patching cycle included two different releases, each of which came with fixes that were aimed at both Google and other Android devices. Softpedia

Report: Mirai 'is just the tip of the iceberg'
Mirai is just the tip of the iceberg according to a new report by the Institute for Critical infrastructure technology. The DDoS malware which has filled security headlines recently is a profound new intervention in the threat landscape, according to the authors Drew Spaniel and James Scott. Mirai, says the report, offers cyber-criminals, hacktivists and APTs, "an asymmetric quantum leap in capability". It's not, as one might expect, because of its sophistication or that it represents some kind of new weapon for which there is no counter defence, but because of its accessibility. Mirai malware offers a "powerful development platform" which can be tailored to even a relatively unsophisticated attacker's needs. The report is stark in its conclusions: "right now, script kiddies and cyber-criminal gangs are already drastically expanding their control over vulnerable IoT devices, which are enslaved to malicious purposes and can be contracted in DDoS-for-Hire services by a virtually unlimited number of actors for use in an infinite variation of layered attack methods." SC Magazine

Automated Phishing Spurs Criminals to New Heights
Cyber-criminals are lowering the cost and increasing the effectiveness of phishing by leveraging compromised servers and turnkey phishing services, which are the key drivers of the overall increase in phishing attacks. According to Imperva's Hacker Intelligence Initiative (HII) Report, the low cost of launching a phishing campaign and the high projected return on investment for cyber-criminals is leading to an epidemic of offensives. Imperva researchers browsed the darknet marketplace to estimate the cost of phishing campaigns and to get a clear picture of the business model. They observed the ease of purchase and low cost of phishing-as-a-service (PhaaS) campaigns. In addition, they saw that hackers were easily able to hijack compromised webservers for their campaign, which further lowered the investment needed. Infosecurity Magazine

Next year, attacks will differentiate to penetrate new vulnerable surfaces
The upcoming year will include an increased breadth and depth of attacks, with malicious threat actors differentiating their tactics to capitalize on the changing technology landscape, according to Trend Micro… The Internet of Things (IoT) and Industrial Internet of Things (IIoT) will play a larger role in targeted attacks in 2017. These attacks will capitalize upon the growing acceptance of connected devices by exploiting vulnerabilities and unsecured systems to disrupt business processes, as we saw with Mirai. The increasing use of mobile devices to monitor control systems in manufacturing and industrial environments will be combined with the significant number of vulnerabilities found in these systems to pose threats to organizations. Business Email Compromise (BEC) and Business Process Compromise (BPC) will continue to grow as a cost-effective and relatively simple form of corporate extortion. Help Net Security

Experts Propose Cybersecurity Strategy for Nuclear Facilities
Institutionalizing cybersecurity, reducing complexity, active defenses and transformative research should be a priority in reducing the risk of damaging cyberattacks at nuclear facilities, according to the Nuclear Threat Initiative (NTI). While the Stuxnet attacks aimed at Iran are the most well-known, nuclear facilities in Germany and South Korea have also been hit by cyberattacks. European Union officials have also raised concerns about the possibility of attacks against Belgium's nuclear plants. Reports published in the past months warned that countries are not prepared to handle attacks targeting their nuclear facilities, and the nuclear industry still underestimates cyber security risk. A report published on Wednesday by the NTI provides a set of recommendations for improving cyber security at nuclear facilities based on a 12-month analysis conducted by an international group of technical and operational experts. Security Week

Judge Releases Avalanche Network Leader, Despite Police Shootout

A judge in the city of Poltava, Ukraine, has released the alleged leader of the Avalanche malware distribution network, despite the fact the crook was involved in a shootout with the local police special forces that came to arrest him. The suspect is a 33-years-old man named Gennady Kapkanov, and according to several Ukrainian news agencies, authorities suspected him of being the leader of an international malware distribution network nicknamed "Avalanche." Bleeping Computer

LAW ENFORCEMENT / APPLICATION DE LA LOI

Montérégie: la GRC saisit 127kg de cocaïne
La Gendarmerie royale du Canada (GRC) rapporte jeudi qu'une saisie de 127 kilogrammes de cocaïne a été faite par ses policiers durant une enquête qui a permis l'arrestation en début de journée de trois personnes. Ces suspects auraient aussi été impliqués dans du trafic de cannabis et de tabac illégal. Le stratagème auquel ils auraient participé aurait permis d'importer de grandes quantités de cocaïne au Canada qui passaient en transit par Los Angeles et Houston avant d'être destinées au marché de Montréal. Presse canadienne (Journal Métro, La Presse, Radio-Canada) ; CTV News ; Journal de Montréal ; Metro News

'Those emails took us by surprise:' Justice ministry reacts to revelations on Sask. RCMP staffing
Officials with Saskatchewan's Ministry of Justice were as shocked as anyone to learn this week that RCMP vacancy rates are as much as five times higher than officially reported in some parts of the province. 650 CKOM obtained a trove of internal RCMP emails on Wednesday. Those emails, dated Nov. 3, showed the commander of the police service's northern district facing 15 per cent of positions sitting empty. Meanwhile, the southern district reported an eight per cent vacancy rate. Both numbers are much higher than the 3.3 per cent vacancy rate reported at an RCMP news conference on Sept. 29. Drew Wilby, executive director of corporate affairs with the Saskatchewan Ministry of Justice, addressed the controversy Thursday on Gormley. "I would say that those emails took us by surprise, yesterday. And obviously that creates some significant concern for the ministry," he said. The province pays 70 per cent of the costs for 924 officer positions under its rural policing contract with RCMP. Wilby said that includes paying for spots that might be vacant for short-term reasons such as illness or injury. Wilby said the province isn't billed for longer-term vacancies, like parental leave. But even so, he said there is an expectation RCMP has enough staff to ensure public safety. 650 CKOM

Sask. premier wants explanation for RCMP vacancy rates
The premier wants answers on the RCMP staffing issues in Saskatchewan. Emails obtained exclusively by our newsroom shows a real issue of unfilled vacancies, particularly in the northern part of the province. Currently there is a 15 per cent vacancy rate in the north and eight per cent in the south. Since it was elected in 2007, Premier Brad Wall's government has increased funding for police, including to the RCMP. Given that reality, Wall is seeking more information. "I think it's reasonable that municipal leaders, urban and rural, know where those officers are, and I would like to know where they are," Wall explained. "If there's great vacancies that aren't being filled or can't be filled, whatever the issue is, we need to know that." Wall contends this speaks to a wider issue that is a concern for all involved. "At the end of the day there is also a fundamental responsibility on the part of the police force that you contract with, in this case the RCMP, to deliver core public safety," Wall argued. 650 CKOM

RCMP officer accused of historic sexual assault in Auburn elects Supreme Court
An RCMP officer accused of committing a sexual assault on a woman in Auburn while he was posted to Bridgetown more than 20 years ago will be in Supreme Court in July for a preliminary inquiry. Const. Charles Kwatei Quartey, 58, of Inuvik, Northwest Territories, was not present in Kentville provincial court Dec. 7, having earlier filed designation of counsel to be represented by lawyer David Bright. Quartey has elected trial by Supreme Court judge alone. The defence is to file notice by Feb. 28, 2017. The matter has been adjourned to July 6, 2017, for a preliminary inquiry. A publication ban protects the identity of the alleged victim. Quartey is charged with committing a sexual assault on a woman in Auburn between Jan. 1 and Dec. 31, 1995. The RCMP's Southwest Nova Major Crime Unit laid the charge against Quartey in July 2016. While dealing with an unrelated matter in July 2015, information came forward to RCMP members that Quartey had sexually assaulted a woman while posted to the Bridgetown Detachment in

1995. The charge relates to Quartey's conduct with a woman he met during the course of his duties as a police officer. It's alleged that he touched the woman in a sexual manner without her consent. Kings County News; 650 CKOM

Canadian Mountie with a 'troubling' history of mental health problems hanged himself on his birthday while on holiday in Manchester

A decorated Canadian Mountie with a 'troubling' history of mental health problems hanged himself on his birthday during a celebratory trip to Manchester. Robert Archibald, 28, served with the Royal Canadian Mounted Police (RCMP) as a federal air marshal, flying armed on planes across the world. An inquest heard his partner, Candice Lau, found him hanged in a their room at the Aurora Hotel in Manchester city centre in July. He was taken to Manchester Royal Infirmary but efforts to revive him failed. The couple had travelled to Manchester for a short trip to celebrate both their birthdays. The inquest in Manchester heard Mr Archibald, who joined the RCMP in 2009 and was honoured with the Queen's Jubilee Medal in 2012, had been 'struggling' with his mental health. Daily Mail

One arrested following threats against Nova Scotia high school

Nova Scotia RCMP say one person is in custody after threats were allegedly made against Millwood High School in Sackville. Police say they were made aware of the threat around 10:30 p.m. Wednesday and worked through the night on the case. Investigators will not release how the threat was received. One person was taken into custody, however no charges have been laid. Police will not say the age, name or gender of the individual arrested. They will also not confirm if they are a student at the school. Information about the incident has been sent home to parents. Extra police will be on scene at the high school today to help ease the minds of both students and staff. RCMP say there is no ongoing threat to either students or staff at Millwood High School at this time. Digital Cameras Planet; Metro News

RCMP officers raid Glebe Smoke Shop

RCMP officers raided a popular smoke shop in the Glebe Thursday morning. Officials from the Canada Revenue Agency were also present at the Glebe Smoke Shop, on Bank Street at Fifth Avenue, starting around 8 a.m. The RCMP didn't say why the raid was occurring Thursday, but officer were seen paying particularly close attention to the store's cash register. CTV News; Ottawa Sun; CBC News

Man charged with murder in 2006 death of Cape Breton WWII veteran

Cape Breton Regional Police say they've charged a 49-year-old man with first-degree murder in the death of a Second World War veteran 10 years ago. Harold James "Buster" Slaunwhite, 82, was found dead by family members in his home on Brook Street in Dominion, Cape Breton, on Sept. 10, 2006. He lived alone. Cape Breton Regional Police and Nova Scotia RCMP have been investigating his death ever since. (…) "Today's charges represent the hard work of dozens of police officers from the Royal Canadian Mounted Police and Cape Breton Regional Police Service," RCMP Insp. Lynn Young said in a news release. CBC News

Penticton RCMP: Explosive device could have resulted in serious injuries

Police are now saying an explosive device which detonated in the hands of a 72-year-old woman on Nov. 30 could have had much more serious consequences. Luckily Dorothy Czerniak suffered only minor burns and singed hair when the device exploded while she was trying to open it the kitchen of her home in Sun Leisure Mobile Home Park. "I can describe it as a cardboard box that was wrapped in red Christmas paper. It was unlabelled, it was examined by the explosives disposal unit and it contained an explosive device that could have caused serious injuries," said Cpl. Don Wrigglesworth of the Penticton RCMP. "The investigation is still ongoing and we've spoken to people in the residences and continue to do so." He added the examination involves not just the finger prints but DNA collection as well examination of the contents. Penticton Western News

RCMP job application leads to sex assault charge on Sask. Mother

If it weren't for an RCMP application, a Saskatchewan woman may not be heading for a second trial on sexual assault charges. Barbara George has admitted to sleeping with a 14-year-old friend of her son when she was 35 — however she maintains she believed he was 16, which is the age of consent. According to court documents, George's 17-year-old son was having a party at the family's apartment,

which the 14-year-old attended. George had stayed in her room for most of the party. (…) A few months later, George applied to become a member of the RCMP and the application asks whether the applicant has ever had sex with someone under the age of 16. George then asked her son about the boy's age for the first time, and her son replied that he was 15 or 15-and-a-half. On the application George replied yes to the question and wrote an explanation, "He was extremely mature. We had a connection. I was very lonely. It happened once. It was so wrong, and I so regret doing so." The RCMP then investigated and laid charges of sexual assault and sexual interference. 980 CJME

RCMP duty gave Hughes the Great White North

When Cpl. Kirk Hughes was young, he wanted to do two things when he got older; serve and explore Canada, particularly the northern regions. Joining the RCMP allowed him to do just that. "I wanted to travel, actually I wanted to go to the north, to serve in the Northwest Territories in one of those territorial communities, and the RCMP is the only agency that does that," said Hughes. "So that was the big motivation to join the RCMP." (…)While he loved working up north, Hughes and his wife have two young children, and there wasn't a lot for the family to do together there. Then about one year ago, a posting came up for a position based in Taber. (…)Besides the noticeable difference in the weather, working alongside another police department is a new experience, as up north there is only the RCMP. Vauxhall Advance

Broadview RCMP charge men after discovering more than $50,000 in counterfeits

Three men have been charged after the Broadview RCMP discovered more than $50,000 of counterfeits. Their vehicle was pulled over on Saturday at about 6:50 a.m. for an excessive speeding infraction. There were three men in the vehicle, one was found to have a warrant for arrest. Officers searched the the vehicle and found a large sum of cash, along with what appeared to be 32 pieces of gold and platinum, with a potential value of between $50,000 to $100,000. Follow up investigation determined the gold and platinum were counterfeit and the occupants were suspects in several suspicious pawn transactions. 620 CKRM

Here's How Much a StingRay Cell Phone Surveillance Tool Costs

Rochester Police Department in New York responded to our Cell Site Simulator Census with a rare look into the pricing and packaging of the cellphone surveillance tech: a completely unredacted quote list of Harris Corporation products. Police departments and federal agencies alike are remarkably secretive about cell site simulator details—important information like pricing, components that are sold with the devices, how the devices are actually operated, has been withheld from the public due to law enforcement fears that this investigative tool will be compromised. With this document though, we can see much more clearly how Harris sells the controversial devices. It seems that the devices are often sold in packages, like the StingRay II (a more powerful, updated version of your typical StingRay) Vehicular System. This comes with equipment for operating a StingRay from a patrol vehicle and three different kinds of Harris' Harpoon signal amplifiers. A laptop, three kinds of software for accessing different types of cellular networks, and an AmberJack cellphone tracker are also included for a grand total of $148,000. Motherboard

Police Release Sketches In 1998 Murder

Project Devote, a task force of the RCMP and the Winnipeg Police, have released some sketches to the public of individuals they hope to identify in relation to the unsolved murder of Tania Marsden. Police said; "Tania Marsden was last seen alive on her 18th birthday – September 9, 1998. She was celebrating with friends at the Gordon Downtowner Motor Hotel, but after leaving her birthday party that night, she was not seen again until her body was found partially submerged in the Assiniboine River." On November 15 of this year, police executed a search warrant at 865 Selkirk Avenue, in relation to Tania's murder. Now, investigators need the public's help in identifying the individuals in the five sketches below as well as information on a vehicle (pictured below), a white mid-1980's four-door sedan. "We believe that identifying the individuals in the sketches could help lead us to Tania's killer," said Sgt. Shawn Pike, a Project Devote Team Commander. "Tania deserves justice. Her family deserves an answer. Please call us with any information." MyToba

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

NIL

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Fentanyl 'scourge' top of the agenda at meeting of Ontario police brass
The 'scourge' of fentanyl was at the top of a heavy agenda for the board of the Ontario Association of Chiefs of Police and police brass from across the province during a two-day meeting in Barrie. "It's unacceptable that 165 people have died in Ontario this past year because of fentanyl overdoses," said O.A.C.P. President and Chief of Ottawa Police Charles Bordeleau. "It is a crisis." Bordeleau cited a recent training session for 450 front line responders and one option on the table is to provide the opiate antidote nalaxone to officers although cost is a consideration. Barrie Police Chief Kimberley Greenwood, host of the O.A.C.P. meeting, says Barrie police have focused on enforcement and rounding up fentanyl dealers and officers are now targeting users. Sudbury.com

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

Broadcast Media / Médias télédiffusés :

CBC News interview Chief Ernie Crey about including Indigenous boys and men into the National Inquiry into Missing and Murdered Indigenous Women. Rough Transcript

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

NIL

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Lawsuit against Canadian Forces alleges discrimination against gays, lesbians
A former member of the Canadian Forces has launched a lawsuit against Ottawa over alleged discrimination based on her sexual orientation. Lawyer John McKiggan says in the statement of claim, which has not been proven in court, that between the 1950s and 1990s the Canadian government engaged in a campaign to identify, harass and purge lesbians and gays from the Armed Forces. The lawsuit, submitted on Tuesday, spans the years 1969 to 1995 and applies to anyone who served in Atlantic Canada. (…) It says after she told investigators about her sexual orientation, Satalic was given the option of staying in the military with no further training or promotions, or a release from service as "Not Advantageously Employable." She accepted the release. CTV News

INTERNATIONAL

NIL

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

Brett_CBC
Minister @RalphGoodale's office responds to today's $1B RCMP overtime story:

Colinfreeze
#%^$&& ! https://twitter.com/Ian_Bron/status/806873349720784900

Ian_Bron
Goodall says the fabricated #RCMP response to access-to-info request was 'unacceptable' https://shar.es/18zZK8 #cdnfoi #cdnpoli https://t.co/7fSU2iNWyM

rideauinstitute
@RalphGoodale Prohibition against #torture must be treated with utmost seriousness by any civilized nation #cdnpoli https://t.co/6rFVicJcd3

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

globeandmail
Airbus says Canada picks C295W planes for search and rescue fleet http://trib.al/3xfXhAH from @GlobeBusiness

Alec_Castonguay
Le Canada achète 16 avions de recherche et de sauvetages http://www.lactualite.com/actualites/le-canada-achete-16-avions-de-recherche-et-de-sauvetages-militaires-dairbus/ … Ce dossier était un total bordel (et chaos) depuis 2004

NATIONAL SECURITY CONSULTATIONS / CONSULTATIONS SUR LA SÉCURITÉ NATIONALE

canadaCJFE
Concerned conservatives confirm that opposition to #C51 crosses party lines and political affiliations. #cdnpoli http://bit.ly/2hkebkl

HuffPostBC
Liberals' digital surveillance proposals are far scarier than Bill C-51, by @danieltencer http://huff.to/2hiBmMe

CPAC_TV
1:30pmET: @MurrayRankin & @MattDube on Bill #C22 + creation of a nat. security & intell. cttee of parliamentarians http://www.cpac.ca/en/direct/cpac3

NATIONAL SECURITY / SÉCURITÉ NATIONALE

alexboutilier
CSIS watchdog's views on Trump's torture comments, offhand suggestion Snowden should be "shot." (via @Colinfreeze) https://t.co/zE81jSO129

alexboutilier
"Do you want my opinion on that? ... I'll give it to you. If Edward Snowden had worked for CSIS, and did what he did, he should be shot."

CBCNews
Identities revealed of 2 Quebec men who joined militants in Syria to fight against the Bashar al-Assad regime http://www.cbc.ca/1.3885740

TheCurrentCBC
"You ate in that cell, you showered in that cell" Canadian Kevin Garratt, detained in China for spying | Full story http://cbc.ca/1.3885918

Colinfreeze
Chilling. Montreal child being likely raised in the so-called Islamic State, and being told to play with guns. Follow @fabricedp https://twitter.com/fabricedp/status/806847011974742016

Colinfreeze
Thanks to @Slorico76 of @theeyeopener for helping w/ @globeandmail story: http://www.theglobeandmail.com/news/politics/trumps-torture-view-may-change-secrets-sharing-with-canada-spy-watchdog-executive/article33263257/ … Her version here: https://theeyeopener.com/2016/12/its-tough-to-keep-canadas-spies-accountable/ ….

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

CanBorder
CBSA officers find suspected cocaine at the Toronto Pearson International Airport. http://news.gc.ca/web/article-en.do?nid=1162419 …

cassidyolivier
Mexican cartels to expand reach in Canada with visa changes, warns CBSA document http://vancouversun.com/news/national/mexican-cartels-to-expand-reach-in-canada-with-visa-changes/ … @kbolan

VassyKapelos
Canada border bill gets passed in US Congress https://t.co/o7K4QuJHRV

avelshi
@pmlagasse @RobSilver also, despite the official rhetoric on how canada doesn't recognise iroquois passport, cbsa definitely waves them in

CYBER SECURITY / CYBERSÉCURITÉ

CityAdrian
Toronto District School board confirm with @CityNews they do not have dedicated cyber security staff monitoring online threats.

LAW ENFORCEMENT / APPLICATION DE LA LOI

motherboard
Here's how much a Stingray cell phone surveillance tool actually costs http://bit.ly/2h0qicc

CTVNews
RCMP seize 127kg of cocaine in Que. drug smuggling investigation http://ctv.news/QuPuJmV

RadioCanadaInfo
La GRC saisit 127 kg de cocaïne en Montérégie http://dlvr.it/Mr789B

620ckrm
Broadview RCMP charge men after discovering more than $50,000 in counterfeits. #sk - http://bit.ly/2hk1E0q

rcmpmb
This is how we police during #mbstorm! Boissevain #rcmpmb used their sleds to patrol, respond to calls & assist motorists stuck in the snow.

CBCTheNational
$1B RCMP overtime bill proof of 'exhausted and depressed' members, retirees say https://t.co/gFRMCJlzkL

TheWhistlerNews

Whistler RCMP under scrutiny after cell phone seizure
http://www.metronews.ca/news/vancouver/2016/12/06/whistler-rcmp-under-scrutiny-after-cell-phone-seizure.html … #whistler #rcmp #bccla #vancouver #rmow #canada #vpd

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

GgNewsCA
New human rights commission strategic plan tackles racial profiling, solitary confinement https://t.co/IvMXuKzDHm

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

nationalpost
Calls for Alberta minister to resign after he didn't give report on girl's tragic death in government care to RCMP http://news.nationalpost.com/news/canada/calls-for-alberta-minister-to-resign-after-he-failed-to-give-report-on-tragic-death-of-girl-in-government-care-to-rcmp …

CBCCanada
'Make Canada great again' flyers raise alarm at McGill University http://ift.tt/2hak3K9

MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS | LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINEES

DouglasTodd
B.C. Chief Ernie Crey @Cheyom1 Janine Cunningham and @JustinTrottier in Ottawa to #expandtheinquiry #MMIW https://twitter.com/equalitycanada/status/806879071963648000

DouglasTodd
Tragic facts on #murder and #gender: 71% slain aboriginals are males #mmiw #expandtheinquiry @equalitycanada @gcindigenous @Cheyom1

equalitycanada
Let's do a better job on behalf of these families. @Cheyom1 #IncludeMen #ExpandtheInquiry @Cheyom1 @GCIndigenous @CBCNews @DouglasTodd

equalitycanada
This is about enhancing the inquiry not about being divisive, says @JustinTrottier on #ExpandtheInquiry to #IncludeMen. @GCIndigenous #MMIW

ONWA
Discrimination is the root cause of **#**MMIW https://t.co/cAYi6mylC2

Megawitch
Seven years without a trace: Families of missing Maniwaki women cling to hope http://ottawacitizen.com/news/politics/seven-years-without-a-trace-families-of-missing-maniwaki-women-cling-to-hope/ … #findmaisyandshannon #mmiw #missing <3 https://t.co/DVp3cAyHO8

AshleyCsanady
The MMIW inquiry is the best thing this govt has done for women, but what else other than a symbolic cabinet and a bill? Serious Q

AngelaSterritt
MISSING Indigenous woman.Carmen Tribiger last seen Nov 26 in Edmonton. 5'10,130 lbs,black hair. Pls call 1-403-304-7196 if you've seen her.

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

ctvottawa

After raiding Glebe Smoke Shop this morning, RCMP and CRA now at Zesty Market on Elgin Street. Photo by @AnnieClaireBO #ottnews

HuffPostCanada
Pot use, driving while high on the rise in Ontario http://huff.to/2gfTGWh

PUBLIC SERVICE / FONCTION PUBLIQUE

OTHER / AUTRE

LP_LaPresse
Une ex-militaire poursuit le gouvernement fédéral pour discrimination

INTERNATIONAL

CTVVancouver
No reports of damage or injuries after 6.5 quake in #California. https://t.co/TTR6hO2irr

CTVNews
BREAKING: Magnitude-8.0 quake off Solomon islands; tsunami watch issued http://ow.ly/Gn3z306Wxpn

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

Lacroix-Menard, Gabriel (PS/SP)

From: PSPMediaCentre/CentredesmediasPSP (PS/SP)
Sent: Thursday, February 19, 2015 2:11 PM
To: Today's News / Actualités (PS/SP)
Subject: Today's News / Actualités (8:00 - 14:00 ET)

Today's News / Actualités
February 19, 2015 / le 19 février, 2015
8:00 - 14:00 ET

This collection contains news items that appeared online between 8:00 a.m. and 2:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 8h00 et 14h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Opposition slams Tories' 'sweeping' terror legislation
New Democrats and Liberals staked competing claims to the political high ground as parliamentary debate on the Conservative government's proposed anti-terror bill kicked off Wednesday. NDP Leader Tom Mulcair cast his party as a bulwark of Canadians' rights and freedoms, vowing to oppose Bill C-51 unless its extraordinary spying and police powers are curtailed and parliamentary oversight created to prevent abuse. Liberal Leader Justin Trudeau proposed more oversight, a mandatory three-year review of the legislation and a narrower definition of risks to national security, yet confirmed his support for the bill nonetheless. (…) But **Public Safety Minister Steven Blaney** dismissed calls for parliamentary oversight as attempts to import "made-in-America" interference into the Canadian system. Justice Minister Peter MacKay said there are enough safeguards in the bill, including: provisions for prior judicial authorization for Charter-breaching actions by CSIS and a requirement for attorney general or a federal prosecutor's consent for applications for special terrorism "peace bonds" or "recognizance with conditions." Toronto Star

Forced to tweet in both languages, ministers lose their impact
An opinion piece states, "Congratulations to my colleagues @HonRobNicholson, @kenneyjason and @PierrePoilievre on their new appointments!" "Enduring love is in the air at Pioneer #ValentinesDay Tea, the couple on my right has been married for 67 years!" These are three tweets you'll receive if you follow the Twitter account of Rona Ambrose, MP for Edmonton-Spruce Grove and federal Minister of Health. But you won't get these tweets in French, and Canada's Official Language Commissioner has a problem with that. Reacting to complaints about the dominance of English-language tweets issued by former foreign affairs minister John Baird and **Public Safety Minister Steven Blaney**, the Commissioner decreed that ministers must tweet equally in French and English when acting in their official capacity. What this means exactly won't be clear until the Commissioner's full report is made public. The key line appears to be "in their official capacity", which leads to the question: Are ministers' Twitter accounts "official" departmental communications, representing the "voice" of the public sector departments these ministers lead? If yes, then of course their tweets need to be bilingual. Legally, this is required under Canada's Official Languages Act. Bilingualism of official government communications is not, and should not, be up for debate here. The Globe and Mail

Forced to tweet in both languages, ministers lose their impact
An opinion piece states, "…Reacting to complaints about the dominance of English-language tweets issued by former foreign affairs minister John Baird and **Public Safety Minister Steven Blaney**, the Commissioner decreed that ministers must tweet equally in French and English when acting in their official capacity. What this means exactly won't be clear until the Commissioner's full report is made public. The key line appears to be "in their official capacity", which leads to the question: Are ministers' Twitter accounts "official" departmental communications, representing the "voice" of the public sector departments these ministers lead? If yes, then of course their tweets need to be bilingual. Legally, this is required under Canada's Official Languages Act. Bilingualism of official government communications is not, and should not, be up for debate here. If ministers' Twitter accounts do not represent the official voice of government departments, but are instead a vehicle for the partisan, personal and professional communications of the MP, then the case is similarly straightforward. While there are many reasons an MP might choose to tweet in both official languages they're not legally obliged to do so. But this is where things get complicated." Globe and Mail

Broadcast media / Médias télédiffusés :

Canada's **Public Safety Minister** will speak this afternoon at CVE summit in Washington. Much of what he'll talk about is bill C-51. (CBC Radio One, 12:06 ET; CBC News, 12:35 ET; RDI, 10:45 ET) CBC News rough transcript

CTV News reports **Public Safety Minister Steven Blaney** will be taking part in the Countering Violent Extremism summit in Washington. According to the polls Canadians support bill C-51. The NDP will not support the legislation. *CBC News* presented a similar report. CTV News rough transcript; CBC News rough transcript

The government is dismissing concerns raised by the NDP over the proposed antiterrorism bill. **Public Safety Minister Steven Blaney** calls the concerns raised by the NDP as nothing more than ideological nonsense. (CJKL-FM, 6:01 ET; CJAD, 6:04 ET; AM 630 CHED Edmonton, 6:04; CFAX 1070 Victoria, 6:35; 680 News, 7 :06 ET; 580 CFRA, 7 :36 ET)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Avis d'ébullition d'eau pour des secteurs de Longueuil, Boucherville et Saint-Bruno
La Ville de Longueuil a émis jeudi un avis d'ébullition d'eau pour les arrondissements de Saint-Hubert et du Vieux-Longueuil et les villes de Boucherville et de Saint-Bruno-de-Montarville. L'avis est en vigueur pour 48 heures. Selon le communiqué de la ville «cette situation résulte de travaux à l'usine de production d'eau potable, située au 1700, rue Bourassa dans l'arrondissement du Vieux-Longueuil». Une baisse de pression affecte actuellement le réseau, mais les autorités prévoient un retour à la normale «sous peu». Huffington Post Québec; CBC News; CTV News

Gogama crude oil spill worries nearby Mattagami First Nation
Mattagami First Nation is sounding the alarm about a CN rail spill near the community. The First Nation said Saturday's derailment involving 29 crude oil tankers occurred on its traditional territory, located 40 kilometres north of the community. Ontario's Regional Chief Stan Beardy is advocating for the community to make sure the site is cleaned, as he's concerned about the spill causing environmental damage. CN and other agencies have been on the scene cleaning up all week. They say the spill is contained, and the rail line is now open to other train traffic. CBC News

NATIONAL SECURITY / SÉCURITÉ NATIONALE

White House summit on ISIL discusses Canadian mom's project
The efforts of a grieving Canadian mother were highlighted at a White House summit this week as an example of how to turn the tide in the online war against ISIL. According to some participants at the three-day summit on countering violent extremism, it's been a lopsided fight. They say the terror group has dominated on the battlefield of modern media. Its gory videos keep surfacing on websites, its online magazines invite youth to the jihadist cause, and its hackers even temporarily seized the social-media accounts of U.S. government and military agencies. One presenter pointed out a rare response to that online onslaught of jihadist propaganda: Christianne Boudreau's participation in a video about the death of her son in Syria. National Post

"Total Information Awareness": The Disastrous Privacy Consequences of Bill C-51
An blog post states, "The House of Commons debate over Bill C-51, the anti-terrorism bill, began yesterday with strong opposition from the NDP, disappointing support from the Liberals, and an effort to politicize seemingly any criticism or analysis from the Conservative government. With the government already serving notice that it will limit debate, the hopes for a non-partisan, in-depth analysis of the anti-terrorism legislation may have already been dashed. This is an incredibly troubling development since the proposed legislation has all the hallmarks of being pulled together quickly with limited analysis. Yet both the Conservatives and Liberals seem content to stick to breezy talking points rather than genuinely work toward a bill that provides Canadians with better safeguards against security threats while also preserving privacy and instituting effective oversight." Michael Geist

Defence minister says more terror attacks possible
Newly appointed defence minister Jason Kenney has used his maiden speech to the country's military establishment to pitch the government's anti-terror bill. He's telling the Conference of Defence Associations Institute that there is a likelihood of more homegrown terror attacks. Kenney, who took over from Rob Nicholson, earlier this month, says the country shouldn't over-react to the threat of the Islamic State-inspired extremism, nor should it under-react. The anti-terrorism bill, which increases the powers of security agencies, notably the Canadian Security Intelligence Service, is being debated by the House of Commons. It is the government's response to last October's attack on Parliament and the murder of two soldiers. Kenney casts the threat of Islamic extremism as a global danger. QMI Agency (The Guardian, Cape Breton Post, The Telegram, iPolitics); iPolitics; Toronto Star; Globe and Mail; iPolitics; Canadian Press (Metro News)

Four former prime ministers call for stronger security oversight
Four former prime ministers are among almost two dozen prominent Canadians calling today for stronger security oversight. The statement published in the Globe and Mail and La Presse newspapers comes as the Conservative government proposes a new mandate for the Canadian Security Intelligence Service. It is signed by Jean Chretien, Paul Martin, Joe Clark, John Turner and 18 others involved in security matters over the years. The Security Intelligence Review Committee currently oversees CSIS, doing several studies each year and tabling a report in Parliament. Critics point out the review committee is just that, a review body, not an oversight agency peering over the spy service's shoulder in real time. The letter notes that detailed recommendations for a new oversight regime, proposed in 2006 by the inquiry into the Maher Arar torture affair, were never implemented. IPolitics (The Chronicle-Herald); Canadian Press (Prince George Citizen); CBC News; CKNW AM 980

Grieving Canadian mother's message heard at White House summit
The efforts of a grieving Canadian mother were highlighted at a White House summit this week as an example of how to turn the tide in the online war against ISIS. According to some participants at the three-day summit on countering violent extremism, it's been a lopsided fight. They say the terror group has dominated on the battlefield of modern media. One presenter pointed out a rare response to that online onslaught of jihadist propaganda: Christianne Boudreau's participation in a video about the death of her son in Syria. The young man from Calgary was one of an estimated 20,000 people from 100 countries who went to fight with ISIS. In a speech earlier Wednesday, President Barack Obama acknowledged the struggle with social media. Canadian Press (CTV News)

A Royal Canadian Mounted Police Report Said Anti-Oil Activists Were National Security Threats
As the Stephen Harper government works to pass the C-51 bill, which would extend anti-terrorism legislation to include anyone who interferes with the "critical infrastructure," "territorial integrity," or "economic and financial stability of Canada," a leaked report from the Royal Canadian Mounted Police (RCMP) Critical Infrastructure Intelligence Team demonstrates how aboriginals and environmentalists are already being targeted by law enforcement for these reasons. The leaked intelligence report from early 2014 discusses a "growing international opposition" to mining operations on Canada's tar sands and focuses on "violent aboriginal extremists," anti-fracking, and anti-pipeline activists, identifying them as threats to national security. In particular, the report is concerned with aboriginal struggles against unwanted fossil fuel developments on lands that were never ceded to the Crown. VICE (2015-02-18)

Broadcast media / Médias télédiffusés :

Broadcast media provided live coverage of U.S. President Barack Obama speaking at the CVE summit. (CBC News, 10:42; CTV News, 10:42 ET) CBC News rough transcript

CTV News reports an Angus Reid poll shows 82% of Canadians support bill C-51 which includes expanding the powers of intelligence agencies and police. Many even believe that the measures don't go far enough. The poll also says a majority of Canadians believe that we need better oversight. (CTV News, 11:35 ET)

La question du jour de *RDI* : Fort appui des Canadiens au projet de loi C-51 contre le terrorisme. Croyez-vous également important d'accroître la surveillance du SCRS? (RDI, 11 :30 ET)

RDI mentionne la lettre de ce matin signé par quatre ex-premier ministre, aussi des ex ministre de la Justice du Canada, Roy Romanow, Bob Rae aussi qui ont été sur le fameux comité de surveillance qui existe actuellement. Ils disent qu'il faut plus de contrôle des agents du SCRS. (RDI, 13 :30 ET)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Canada announces new Windsor-Detroit bridge
Canada was already planning to pay for 95 per cent of a new bridge between Windsor, Ont., and Detroit. Now it's covering the final portion — a United States customs plaza. Transport Minister Lisa Raitt says it won't cost Canadian taxpayers anything because the funds will be recouped through tolls and a public-private partnership. The Canadian government had expressed frustration at having to wait for construction to start on the U.S. side of the estimated $4 billion project. The new infrastructure would be a next-generation replacement for the aging bridge that currently handles one third of all Canada-U.S. trade. The Record.com

MP Not Celebrating Border Agreement
Windsor West MP Brian Masse is not celebrating Wednesday's agreement between Canada and the U.S. over the costing of the new border crossing between Windsor and Detroit.Transport Minister Lisa Raitt told the House of Commons Canada will pay 95% of the cost of building the new bridge and the $250-million cost of building a customs plaza on the U.S. side. Under the public-private partnership, that cost will be recouped through future tolls. Masse, the NDP border critic says that's like charging Windsorites twice, the first time through their taxes. "At first you might think that that's okay, but the reality is tolls are mostly paid by local people crossing the border, so we end up fronting the lion's share of the deal." "Having to front this is not fair," he says. "It's not fair for our economy. It's not fair for tourism. It's not fair for the way we actually interact with our friends and relatives on the American side. We end up becoming an experiment for the government, and I think that's wrong." Blackburn News

Plus de cinq tonnes de tabac de contrebande saisies en deux mois dans la région de Cornwall
Les dernières semaines ont été fructueuses pour le Groupe de travail régional (GTR) de Cornwall et ses partenaires. Depuis le mois de décembre, cinq événements distincts ont mené à la saisie de 5217,7 kg de tabac haché fin et à l'arrestation de trois personnes. Dans un premier cas, le 9 décembre, les policiers ont aperçu une embarcation qui s'approchait à vive allure de la rive ontarienne du fleuve Saint-Laurent, à Bainsville. Ils ont ensuite surpris deux mineurs en train de déposer des sacs à ordures dans une camionnette. Les jeunes suspects ont été arrêtés, l'un sur place et l'autre à son domicile, et ont été libérés sous promesse de comparaître. Les policiers ont également saisi 3329,8 kg de tabac haché fin, qui était caché à l'intérieur de 116 sacs à ordures. Un autre homme a pour sa part été arrêté, le 28 janvier, après que des agents de l'Agence des services frontaliers du Canada (ASFC) l'eurent intercepté en possession d'étuis à cigarettes non déclarés.David Colon Jr, 27 ans, d'Akwesasne, devra répondre à une accusation de possession de tabac non estampillé. Son véhicule a été saisi et il a été remis en liberté en attente de sa comparution, prévue le 10 mars. Radio-Canada

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

IT security overhaul at National Research Council to cost $32.5 million
Fortifying the National Research Council's computer systems in the wake of a high-profile cyber attack last year will cost the federal government $32.5 million. That money, given to the government's super-IT department, will cover costs for a complete overhaul of one of the most complex and sensitive IT infrastructures in the country. Hackers, reportedly from China, infiltrated systems of the NRC, one of the most important research organizations in the Canadian government, in 2014. Ottawa Citizen

Leak threats abound, RCMP's Aubin warns

In the age of cyber security, RCMP's Michel Aubin says that insufficient resources are making insider leaks in the policing community are a significant threat that goes well beyond well intentioned whistle blowers. "I understand that everyone knows about Snowden, Madden, and Delisle... But for the law enforcement community, insider threats are a real issue," Aubin told the Conference Board of Canada Cyber Security conference Thursday morning. "I'm not trying to pick on any agency in particular. Cecere was an RCMP officer in Montreal working in our wire tap room who was leaking information to the mafia." Aubin is the director general of the Criminal Intelligence Service Canada (CISC) and oversees programs that include site, personnel and IT security. The issue for him is that even a small leak would have access to a vast, treasure trove of information. iPolitics

LAW ENFORCEMENT / APPLICATION DE LA LOI

RCMP sees 'anti-petroleum' movement as a threat

In response to the news about an RCMP document obtained by Greenpeace Canada, Council of Canadians chairperson Maude Barlow has tweeted: "Dissent is a right!" She and many others are worried because the Globe and Mail reports, "The RCMP has labelled the 'anti-petroleum' movement as a growing and violent threat to Canada's security, raising fears among environmentalists that they face increased surveillance, and possibly worse, under the Harper government's new terrorism legislation." In highly charged language that reflects the government's hostility toward environmental activists, an RCMP intelligence assessment warns that foreign-funded groups are bent on blocking oil sands expansion and pipeline construction, and that the extremists in the movement are willing to resort to violence. ...The report extolls the value of the oil and gas sector to the Canadian economy, and adds that many environmentalists 'claim' that climate change is the most serious global environmental threat, and 'claim' it is a direct consequence of human activity and is 'reportedly' linked to the use of fossil fuels." Rabble.ca

RCMP charges SNC-Lavalin with fraud and corruption linked to Libyan projects

Canadian police laid charges against Montreal-based SNC-Lavalin on Thursday for corruption and fraud in connection with an investigation into dealings with Libya. The RCMP National Division announced on Thursday that three divisions, SNC-Lavalin Group Inc., SNC-Lavalin Construction Inc. and SNC Lavalin International Inc. are all charged with fraud and corruption. SNC shares fell more than 6% in early trading after the charges were laid. SNC-Lavalin said in a statement Thursday and on Twitter that it will contest the charges and enter not-guilty pleas. "The charges stem from the same alleged activities of former employees from over three years ago in Libya, which are publicly known, and that the company has cooperated on with authorities since then," said Robert Card, the company's chief executive, in the statement. We will contest the charges in the interest of our current employees and their families, clients, investors, partners. The RCMP allege that between Aug. 16, 2001, and Sept. 20, 2011, the three entities bribed a Libyan official or officials with $47,689,868 Canadian to "use their positions to influence any acts or decisions of the Great Socialist People's Libyan Arab Jamahiriya." SNC-Lavalin CEO says projects won through corruption have been commercial flops Former SNC-Lavalin executive Riadh Ben Aissa pleads guilty to corruption charges. During the same period, the RCMP allege that all three entities defrauded "by means of deceit, falsehood or other fraudulent means" the Great Socialist People's Libyan Arab Jamahiriya with regards to a manmade river project in Libya, for a value of $129,832,830 Canadian. "Corruption of foreign officials undermines good governance and sustainable economic development. Financial Post (Montreal Gazette)

Epic Team-up: Hickory police & Canadian Mounties

The Royal Canadian Mounted Police, better known as Mounties, reached out to the Hickory Police Department recently for a little help solving a crime that police say got its start north of the border before making its way to Hickory. It all started in Squamish, British Columbia, in Canada, which is about 180 miles north of Seattle and about 3,000 miles northwest of Hickory, when a check from a Canadian business was reported stolen. The payee and the amount were allegedly altered before someone cashed it for $38,375 at a Hickory branch of Capitol One Bank, according to a Hickory police incident report. Hickory Record

Muir Lake School 'locked down' as police search for suspect

RCMP in Stony Plain put Muir Lake School under lockdown Thursday morning while they searched for a suspect in connection with a stolen vehicle. Police were called out to the area, west of Edmonton, around 6 a.m. after receiving reports that four people were trying to steal a vehicle. When they arrived on scene, the four suspects were spotted trying to free a truck that was stuck in a driveway. Two men were arrested on scene, while a third was tracked down with a police dog shortly afterwards. The fourth suspect's location remains unknown. While RCMP continued to search for the fourth suspect, exterior doors at Muir Lake School were locked as a precaution. Inside the school, students and staff were allowed to move freely. CBC.ca

Broadcast media / Médias télédiffusés :

A high-profile engineer firm SNC-Lavalin is accused of fraud and corruption. The RCMP alleges that they paid nearly $47.7 million to public officials in Libya directly or indirectly in order to obtain a business advantage. They say a subsidiary are also accused of defrauding Libyan organizations more than $100 million. SNC-Lavalin plans to plead not guilty. (CTV News, 10:11 ET; CBC News, 13:30 ET; RDI, 12:30 ET)

Nova scotia RCMP to the rescue. Again. Earlier this week, we told you about officers rescuing a baby seal. Well, look at this repeat performance Tuesday night. In both cases, the seals were on the road, not a safe place, especially at night. But here are two of Pictou County's finest urging this pup back into the water. A little fun slide there as he heads back. All in a day's work. (CBC News, 9:12 ET)

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

Man under arrest after two years on the run
A man from Gibbons is now behind bars after evading arrest for more than two years. 38-year-old Ron Sparling has been flying under police radar since he walked away from an Edmonton halfway house. Several warrants were issued for his arrest in both Edmonton and Stony Plain/Spruce Grove, including being unlawfully at large. It was Wednesday afternoon that Morinville Mounties, with the help of St. Albert's Police Dog Section and "K" Division officers arrested Sparling at a Bon Accord gas station. He now faces an additional charge of resisting arrest. He'll stay in police custody until at least March 4, 2015. That's when he's due in Stony Plain court. 630 CHED

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Human Trafficking Is Part of the Story of Missing and Murdered Aboriginal Women
An opinion piece states, "The distraught woman paced the streets, clearly in search of someone. She broke down in tears when police approached. "I'm looking for my daughter. She's being pimped out by a boy who's in a gang, and I need to find her." In no time, a sting was set up. The trafficker was arrested and the girl restored to her family on a First Nations Reserve in northern Alberta. She was one of the lucky ones. Many more victims end up on Canada's too-long list of missing and murdered women. Aboriginal women and girls are at higher risk of becoming victims of human trafficking in Canada than non-aboriginals, according to Canada's National Action Plan to Combat Human Trafficking. This selling and abusing of people -- a modern-day form of slavery -- is one of the pieces that make up the complex puzzle of Canada's more than 1,100 missing and murdered aboriginal women. And another reason we must take action. The story of the girl and her mother -- their names have been omitted for privacy -- was one of many heard by Canadian researchers, Yvonne Boyer and Peggy Kampouris, when they conducted a study for **Public Safety Canada** on the trafficking of aboriginal women and girls. We spoke with Kampouris about why First Nation women are at greater risk, and the challenges of addressing this appalling trend. Kampouris told us underlying issues, like higher rates of extreme poverty, substance addiction, family violence and sexual abuse, make aboriginal women more vulnerable to exploitation." Huffington Post

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

Feds table supplementary estimates, seeking approval for $138.1-million for incremental costs of Iraq mission
The federal government is asking Parliament to approve a total of $138.1-million for the incremental costs so far of Canada's air strike mission in Iraq and participation in NATO efforts against Russian support for separatists in Ukraine-but its Treasury Board submission to the Commons and Senate does not break down the price tag for each mission or itemize details. The request for the new spending authorities contained in supplementary estimates Treasury Board President Tony Clement (Parry Sound-Muskoka, Ont.) tabled Thursday morning does not include the full cost for each mission, listing instead the cost that Canadian Forces are incurring over and above the salaries and normal operating costs that would have gone toward the roughly 600 personnel, six CF-18 fighter bombers and other aircraft deployed to the fight against Islamic State militants in Iraq. The Hill Times

Obama calls on world to focus on roots of ISIS, al Qaeda extremism
President Barack Obama called for a global effort to combat violent extremism and urged countries around the world to address the root causes that fuel groups like ISIS and al Qaeda during a speech Thursday before hundreds of foreign officials gathered for a summit on countering violent extremism. As he recalled recent terror attacks around the world,

Obama urged countries to "break the cycles of conflict, especially sectarian conflict" and called on governments to "address the grievances that terrorists exploit," both political and economic. CNN

INTERNATIONAL

NIL

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

connect2canada
.@MinStevenBlaney represents Canada at the #CVESummit in Washington, DC today bit.ly/1AT5iRz pic.twitter.com/gBnWcoOr17
@Safety_Canada

Kristie__Smith
Today is a pretty big day in news. Don't forget, Pub. Safety Min Steven Blaney is in Washington for #CVESummit promoting #C51 #cdnpoli

MCCongress
MCC & Canadians overwhelmingly support new Terror Laws. bit.ly/1BqjYJf @pmharper @MinChrisA @MinStevenBlaney

MCCongress
All Canadians should view this and support, that is what Canada wants angusreid.org/c51/ @pmharper @MinChrisA @MinStevenBlaney

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

CBCAlerts
Boil water advisory issued in #Longueuil, #Quebec due to work being done in treatment plant. Advisory to be in effect for 48 hours.

NATIONAL SECURITY / SÉCURITÉ NATIONALE

JusticeCanadaEN
RT @Safety_Canada Read about our plan for protecting Canadians from the global terrorist threat: canada.ca/antiterrorism#antiterrorism

globepolitics
More jihadist attacks likely, Kenney says, defending anti-terror bill http://bit.ly/1CNkeQc #cdnpoli

ipoliticsca
Kenney tells conference fears of terror bill overreach are 'exaggerated' | iPolitics http://www.ipolitics.ca/2015/02/19/kenney-tells-conference-fears-of-terror-bill-overreach-are-exaggerated/ ...

VICE
In Canada, if you're an anti-oil activist, the police think you're a national security threat bit.ly/1AmqVYD

JULIEVANDUSEN
Julian Fantino says c51 is not about taking away people's rights says there's enough oversight -it strikes a balance #cdnpoli #hw

JULIEVANDUSEN
Ndp Randall Garrison says it's incredible govt bringing in time allocation on c51-will restrict privacy and rights #cdnpoli #hhw

TondaMacC
#NDP @r_garrison demands if govt is going to allow full debate on #C51 in committee despite invoking time allocation at 2nd reading.

TondaMacC
#CPC House leader PVL says "full debate" is desirable at committee, that committees are masters of their own process. @WayneEaster scoffs.

TondaMacC
.@LindaDuncanMP: PVL absurdly limits time for #C51 debate then scolds MPs for failing to debate substance during debate on time limit.

TondaMacC
Surprise. The motion to limit 2nd reading debate on #C51 carries.

withfilesfrom
Jason Kenney: anti-terror bill #C51 "doesn't give new power to police or intelligence agencies but rather to judges"

stphnmaher
Two big times of, um, contention in that Kenney quote. 1. Bill does give CSIS new powers to act without warrants, profs say.

stphnmaher
2. System of oversight was greatly diminished by this government when it shut down CSIS inspector general in 2012.

mgeist
"Total Information Awareness": The Disastrous Privacy Consequences of #BillC51 http://www.michaelgeist.ca/2015/02/total-information-awareness-disastrous-privacy-consequences-bill-c-51/ ...

mgeist
The Disastrous Privacy Consequences of Canada's Anti-Terrorism Bill: info sharing provisions http://bit.ly/1vKozyA #BillC51

mgeist
1 Anti-terror bill info sharing rules raised immediate alarm bells for Cdn Privacy Commish. Why? http://bit.ly/1vKozyA #BillC51

mgeist
2. Massive expansion of info sharing across gov for reasons that have nothing to do w/terrorism http://bit.ly/1vKozyA #BillC51

mgeist
3. Sharing across 17 gov depts & open door to disclosure "to any person, for any purpose" http://bit.ly/1vKozyA #BillC51

mgeist
4. Woeful oversight - Privacy Act has not been updated since it was enacted in 1983! http://bit.ly/1vKozyA #BillC51

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

GetCyberSafe 10:04am via Hootsuite
Your business may be small, but cybercriminals see it as a big target.
getcybersafe.gc.ca/cnt/prtct-yrsl…

cyber_securite
Votre PME est peut-être petite mais pour les cybercriminels, elle est une cible de taille. http://www.pensezcybersecurite.gc.ca/cnt/prtct-yrslf/prtct-smlbsn/index-fra.aspx …

LAW ENFORCEMENT / APPLICATION DE LA LOI

CBCAlerts
#RCMP charge #SNCLavalin with corruption, fraud. Charges relate to company's dealings in #Libya between 2001 -- 2011. #cdnpoli

StewartBellNP
SNC-Lavalin paid $48-million in bribes to Gaddafi regime between 2001-2011, RCMP says. rcmp-grc.gc.ca/ottawa/ne-no/p...

QMInews
#BREAKING: SNC-Lavalin has been charged with bribery and fraud involving the company's operations in Libya, the RCMP says.

CdnPress
RCMP lays fraud, corruption charges against SNC-Lavalin, subsidiaries: is.gd/2S7YSq

financialpost
SNC-Lavalin shares drop nearly 7% after RCMP lays fraud and corruption charges natpo.st/1vK2VdL

VancouverSun

RCMP charges SNC-Lavalin with corruption, fraud http://ow.ly/2USBfc

nationalpost
Accused killer on the loose and believed to be armed after abduction, murder in Saskatchewan natpo.st/17hndoZ

CBCManitoba
BREAKING: Jonas Budd, suspect in shooting and abduction, located by RCMP http://cbc.ca/1.2963111 #cbcmb #skcbc

edmontonjournal
RCMP locate homicide, abduction suspect; home surrounded in northern Saskatchewan edmjr.nl/19DxfCg

globalnews
Police in standoff with Jonas Budd in Sturgeon Landing, Sask. http://glbn.ca/JkXH1

InfoNewsKam
RCMP investigate third bomb threat at a Salmon Arm school. goo.gl/zM3imJ

ipoliticsca
Leak threats abound, RCMP's Aubin warns | iPolitics http://bit.ly/1Ead2iY #cdnpoli

INTERNATIONAL

StateDept
President Obama at #CVESummit: We must remain unwavering in our fight against terrorist organizations. http://snpy.tv/1LhpQWV

Blogs

"Total Information Awareness": The Disastrous Privacy Consequences of Bill C-51
The House of Commons debate over Bill C-51, the anti-terrorism bill, began yesterday with strong opposition from the NDP, disappointing support from the Liberals, and an effort to politicize seemingly any criticism or analysis from the Conservative government. With the government already serving notice that it will limit debate, the hopes for a non-partisan, in-depth analysis of the anti-terrorism legislation may have already been dashed. This is an incredibly troubling development since the proposed legislation has all the hallmarks of being pulled together quickly with limited analysis. Yet both the Conservatives and Liberals seem content to stick to breezy talking points rather than genuinely work toward a bill that provides Canadians with better safeguards against security threats while also preserving privacy and instituting effective oversight. The only detailed review to date has come from Professors Kent Roach and Craig Forcese. Their ongoing work – three lengthy background papers so far (Advocating or Promoting Terrorism, new CSIS powers, expanded information sharing) – provides by far the most exhaustive analysis of the bill and is a must-read for anyone concerned with the issue. Indeed, once you have read their work, it becomes readily apparent that all should be concerned with this legislation. Much of the focus to date has been on the lack of oversight and the expansive new powers granted to CSIS. However, the privacy implications of Bill C-51's information sharing provisions also cry out for study and reform. MichaelGeist.ca

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

Lacroix-Menard, Gabriel (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Monday, July 11, 2016 8:07 PM
To: Today's News / Actualités (PS/SP)
Subject: Today's News / Actualités (14:00 - 20:00 ET)
Attachments: TN A - 2016-07-11 - 8pm.docx

Today's News / Actualités
July 11, 2016 / le 11 juillet 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Immigration detainees on hunger strike; want meeting with public safety minister
A group advocating for full immigration status for all migrants says more than 50 immigration detainees began refusing food Monday in two Ontario centres. The End Immigration Detention Network says the detainees are protesting prison conditions that include increasing lockdowns and the use of solitary confinement, and are calling for an end to indefinite detentions in maximum security prisons. The immigration detainees are asking for a meeting with **Public Safety Minister Ralph Goodale** to discuss their concerns. **A spokesman for Goodale** says **the minister** is working on issues related to

detention and hopes to put forward proposals later this year... The End Immigration Detention Network says immigration detainees previously went on a hunger strike that began on April 21, and met with officials from Canada Border Services Agency. But the group says CBSA has not followed through on promises it made and the detainees have begun the new hunger strike — this time calling for a meeting with elected officials."We would like to meet with MPs," said Toby Clark, who has been in immigration detention since August 2014...Sharmeen Khan of End Immigration Detention Network said detainees are often on long lockdowns during the summer — sometimes kept in their cells for days in a row, unable to speak with their families, or get legal support. "**Goodale** must meet with the detainees, and commit to upholding international norms and basic human rights by ending immigration detention," Khan said... **Goodale spokesman Scott Bardsley said** Monday in an email that CBSA is required to consider all reasonable alternatives before detaining someone. ***"Under Canadian law, detention is only allowed when: identity is not certain, there is a flight risk or a danger for the public," Bardsley said. Goodale*** has met with the United Nations High Commissioner for Refugees, the BC Civil Liberties Association, the Canadian Association of Refugee Lawyers and others to discuss detention issues, **he said**. ***"Our goal is to ensure our Canadian approach is world-class, including our methods of enforcement, with effective transparency and accountability."*** Canadian Press (Coast Reporter, The Record)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Funnel clouds formed as warnings ended not capable of causing much damage: Environment Canada
Environment Canada says many of the funnel clouds seen on Sunday in the Saskatoon area were only capable of producing landspout tornadoes, which are not capable of doing much damage. Technically the clouds could have formed tornadoes but they would be in the form of landsprout tornadoes, according to Natalie Hasell, warning preparedness meteorologist with Environment Canada. CBC News

Saskatoon residents warned of heavy rainfall rolling in
City crews are cleaning catch basins and priming pumps in anticipation of heavy rain expected to settle in the next 24 hours. Jeff Jorgenson, with the City of Saskatoon, said that workers and systems are in good shape as the clouds darken. Environment Canada has issued a rainfall warning for Saskatoon, forecasting between 60 and 100 millimetres by Wednesday. CBC News; News Talk 650

UPDATE: Nova Scotia Power launches new outage map
Nova Scotia Power has launched an online map that delivers near-live power outage reports on mobile devices. The outage map, which launched on Sunday, will automatically be updated every 15 minutes and can be viewed directly from your smartphone or tablet. Chronicle Herald

Toronto may join growing number of US cities with 911 texting
A city council vote this week could set Toronto on the path to becoming the first jurisdiction in Canada where all residents can send text messages to 911 operators instead of calling them. Coun. Norm Kelly is calling on the city to request that the Toronto Police Services Board consider adopting emergency texting. Many parts of Canada, including Toronto and 500 other Ontario communities, offer 911 texting for people with hearing or speech impairments. Text service for people with special needs also exists in Manitoba, New Brunswick, Nova Scotia, most of Quebec, and parts of Alberta and British Columbia. But emergency texting for people without hearing or speech impairment is not available anywhere in Canada. Canadian Press (Global News)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

NIL

BORDER SECURITY / SÉCURITÉ FRONATLIÈRE

Sask. CBSA officers seize alcohol, drugs and weapons in June
The Canadian Border Service Agency (CBSA) seized 147 litres of undeclared alcohol, as well as drugs and guns in some June border seizures in Saskatchewan. On June 16 CBSA officers in Saskatoon were examining international commercial shipments in a warehouse when they discovered 147 litres of alcohol inside a container. In addition they also seized wood, meat and medicine that weren't declared, the CBSA said. Global News

Prohibited Weapon, Undervalued Boat Among June Border Seizures at Prince Rupert
A prohibited gun found hidden in various parts of a vehicle and an undervalued boat were the two most notable seizures made by Canada Border Services Agents in Prince Rupert last month. The CBSA says both seizures were made at the

Alaska Marine Highway ferry terminal. On June 14th, someone trying to bring in a 27-foot boat was forced to pay over $30,000 US, after officers determined it had been undervalued by nearly $24,000 US. CFTK TV

Canadian Men Accused of Trying to Smuggle Cocaine, Ecstasy Across Border
Three Canadian men have been accused of trying to smuggle more than a $1 million worth of cocaine and ecstasy through the remote Yaak River region of Lincoln County. Kristopher Glenn Pfeifer and Preston Frederick Lahmer were charged in U.S. District Court in Missoula with felony conspiracy to possess controlled substances with intent to distribute and possession with intent to distribute a schedule one controlled substance. Matthew Desmond Browne was charged with one count of felony conspiracy to possess controlled substance with intent to distribute and one count of felony possession with intent to distribute cocaine. Flathead Beacon

Marble Restaurants Ltd. of Edmonton receives significant sentence under Immigration and Refugee Protection Act
MARBLE Restaurants Ltd. in Edmonton on June 28 pled guilty to employing a foreign national without authorization and failure to follow terms of a Labour Market Impact Assessment (LMIA), and was sentenced under the Immigration and Refugee Protection Act (IRPA). The Canada Border Services Agency said that between February 2014 and April 2015, Marble Restaurants Director Shamez Jivraj employed a woman as a housekeeper and part-time caregiver in his home, despite having received authorization to only employ her as a food counter attendant at the restaurant. Jivraj did not adhere to hours or occupational role set out in the LMIA, but continued to pay the woman as an employee of Marble Restaurants Ltd. Voice Online

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Companies must directly notify people affected by privacy breaches: watchdog
Companies that lose personal customer data should be required to directly notify affected people — with limited exceptions — about the nature and date of the lapse along with steps taken to reduce the harm, says the federal privacy watchdog. The Trudeau government plans to introduce breach-notification regulations in coming months to improve transparency and help consumers. Several large businesses have been stung by hackers in recent years, causing embarrassment for proprietors and potential headaches for customers whose personal and financial details are suddenly circulating in cyberspace. Canadian Press (Metro)

NATO sites downed as measures approved opposing Russian aggression
Three days after the North Atlantic Treaty Organization's Allied Transformation Command websites were knocked offline, the alliance has yet to release official comments over the cause of the outage that felled two military command websites. The outages occurred during a NATO summit held in Warsaw last week, raising suspicions that Russian hackers could have attacked the websites in response to the summit's initiatives opposing Russian military aggression. “This is a suspicious timing for a technical failure,” a senior NATO official said, according to a Wall Street Journal report. “If this is a cyberattack, it would be no surprise.” On Friday, NATO approved measures to place US, UK, Germany and Canada-led battalions along member nations' borders with Russia. The battalions are expected to be placed in Estonia, Latvia, Lithuania and Poland by early next year. The intergovernmental alliance also on Friday approved language that defines cyberspace as a domain of war. SC Magazine

Hidden voice commands in YouTube vids can hack mobile devices
Hidden voice commands embedded in a YouTube video can trigger mobile devices to download malware and alter configuration settings, according to ZDNet. A team made up of researchers from the University of California, Berkeley, and Georgetown University, have created a technique capable of compromising a mobile device via voice commands embedded into a YouTube video. The signal is imperceptible to viewers, but is able to trigger commands within a nearby device, whether a laptop, computer, smart TV, smartphone or tablet. On Apple systems, Siri receives the message and on Android systems, Google Now interprets the signal. In attempting to warn of the risks inherent in increasingly ubiquitous voice interfaces, the researchers note how "an attacker uses the speech recognition system as an opaque oracle." The incursion could enable attackers to issue instructions to any nearby mobile device to initiate a download of malware or adjust configuration settings, which could then lead to a compromise of the device and the possibility of surveillance. SC Magazine

LAW ENFORCEMENT / APPLICATION DE LA LOI

Bob Paulson tells Mounties taking off-duty community assignments not an 'expectation'
The commissioner of the RCMP has told his officers they are not expected to take part in community events while off duty if they don't want to, after CBC revealed Mounties across the country were declining "red serge duty" in a protest over

working conditions. Bob Paulson made the comments in an email to staff dated July 8 and obtained by CBC News. "Many of our members choose to represent their RCMP profession in the community activity they engage in while off duty," Paulson said in the email, which does not mention the CBC story. "That is outstanding and frankly represents the professionalism and privilege many of us feel as employees of the force. But there is no rule or expectation that everyone do so." Last week, the CBC learned that some Mounties were no longer volunteering to appear in parades, fairs and festivals wearing their ceremonial red uniforms and Stetson hats in protest over unsustainable understaffing and overall morale issues within the force, among other irritants. CBC News

Axe woman tased, beaned
Police in the Kootenays arrested an axe-wielding woman without injury to her or the attending officers. Castlegar RCMP arrested the violent and distraught woman in Robson Saturday morning. "Reports had been received that the woman was damaging a home with an axe," said Cpl Dan Moskaluk. The call came in at after 11 a.m. July 9. "Upon police arrival, Castlegar RCMP officers found the woman outside of the residence, where it is alleged that the woman, who while armed with an axe, repeatedly made threatening gestures and approaches towards the RCMP officers," said Moskaluk. Castanet.net

Tensions avec les policiers de Montréal?
Alors que les tensions sont vives aux États-Unis entre les policiers et les membres de la communauté noire, le maire de Montréal ne croit pas que ce soit le cas ici. Pourtant, des experts disent le contraire. Certains policiers du Service de police de la Ville de Montréal (SPVM) croient surtout qu'il est important de distinguer le profilage racial du profilage criminel. Pourtant les intervenants rencontrés par TVA Nouvelles disent le contraire, mais surtout qu'il y a toujours du travail à faire. TVA Nouvelles

Rural Manitoba police constable among few wearing body cameras
Chief Const. Darwin Drader is the lone officer for the Rural Municipality of Cornwallis' police department in western Manitoba. But with the simple click of a switch, he's now got a second set of eyes when he's on calls. Drader has started using a small body-worn camera while on the job in the Rural municipality, located on the outskirts of Brandon and about 200 km west of Winnipeg. It's believed he's the only police officer in the province currently doing so... The RCMP also said officers in Manitoba aren't wearing cameras. It's not known if there are plans to implement their use but they have been tested out at a small number of detachments across the country. CBC News

UPDATE: Man to be tried for murder, interfering with body of Nova Scotia police officer
A man accused of killing an off-duty Nova Scotia police officer and disposing of her body near a Halifax bridge will be committed to stand trial. Christopher Calvin Garner, 28, was in court Monday for a preliminary hearing on charges that he committed second-degree murder and interfered with a dead body in the death of Truro officer Catherine Campbell last September... A sworn affidavit from an RCMP officer obtained prior to the hearing says Garnier allegedly told police he punched and strangled Campbell at an apartment in the city. Chronicle Herald

RCMP unveils memorial plaque for slain West Shore Mountie
West Shore RCMP have unveiled a new memorial for fallen Const. Sarah Beckett, who died in the line of duty earlier this year. The granite stone plaque was installed Monday in a memorial garden commemorating Beckett at the West Shore detachment in Langford. CTV News

Viral footage of violent Calgary police arrest shows officer worn cameras critical to public trust
An opinion piece states "Where there's no trust, there must be cameras. That's not to say the Calgary Police Service did anything wrong on Friday night, in an arrest that's since because fodder for every armchair cop critic, thanks to an amateur video showing 21-seconds of the violent detainment on 17 Ave. S.W., outside a pub. But that's not to say the three-on-one arrest was right, either -- and from a layman's perspective, without context, it does look like very harsh treatment for the person being busted, with one cop dishing out several punches to the man's face, and pulling his hair while he is pinned to the ground..." Calgary Sun

Collingwood man charged after police seize LSD, magic mushrooms, cocaine
Magic mushrooms, LSD and cocaine were some of the drugs seized by police from a Collingwood home last week. Members of the Organized Crime Enforcement Bureau, Central Drug Enforcement Unit, Community Drug Action Team (CDAT) and Collingwood OPP seized 70 grams of cocaine, 85 grams of marijuana, a small amount of LSD, magic mushrooms as well as cash, prohibited knives and brass knuckles from a Second Street home July 7. Simcoe.com

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

'Institutional resistance' to treating inmates with mental health issues, Senator Bob Runciman says

There is a 100-bed unit at The Royal mental health centre in Brockville, Ont., that is dedicated to federal male inmates, and in 14 years, there has never been a suicide and no one has ever escaped. "They've had a tremendously successful track record of reducing reoffending rates and turning lives around," Senator Bob Runciman told CBC Radio's The Morning Edition host Craig Norris Monday. Despite this success, Runciman said, there is still resistance in the correctional system to treating people with mental health issues by placing them in a secure facility like the one in Brockville. That needs to change, he said. Especially after it appears a female offender being held at the Grand Valley Institution in Kitchener, Terry Baker, took her own life last week... There was a pilot project where Correctional Service Canada had one bed in the Brockville facility, but those at The Royal said it wasn't enough, they needed at least 10 beds, according to Runciman. That didn't happen and the pilot project failed, Runciman said. CBC News

Rapist to call Kelowna home
A notorious Calgary rapist is moving to Kelowna at the end of this week. Known as the Falconridge Rapist, the Parole Board of Canada confirms reports that Andrew Aurie Jefferson is set to be released from a federal corrections institute on Friday, with plans to take up residence in Kelowna. Jefferson, 31, gained notoriety nearly a decade ago after terrorizing women at knifepoint during a series of armed street attacks. He was convicted in 2008 of the 2006 violent rape of two women in Calgary. After spending time in prison for the assaults, Jefferson was supposed to be released in Kelowna in 2011, but chose Mission as his new home instead. Two years later, he was put back behind bars after a violent 2013 carjacking in Langley. Friday will mark his second statutory release from the federal system, mandated by law when offenders complete two-thirds of their sentence. Just like his release in 2011, the Parole Board states that Jefferson is considered a high risk to reoffend sexually. He will be required to follow strict rules upon his release including a residency condition requiring him to live in a halfway house or other facility chosen by the Correctional Service of Canada. Castanet.net

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Five hospitalized after drug overdoses at Coquitlam house
Emergency crews were at a Coquitlam house Sunday night to deal with multiple overdoses. Just before 11 p.m., police were called to the home in the 800-block of MacIntosh Street to assist ambulance and fire crews already on the scene, according to Coquitlam RCMP Const. Pamela Newman. Vancouver Sun

Fentanyl sentencing same as other drugs, unless Parliament acts: B.C. judge
A judge in Kelowna declined to consider the presence of fentanyl an aggravating factor in handing down a sentence for trafficking the highly potent and potentially deadly synthetic opioid, saying it's up to Canadian lawmakers to dictate how the drug should be handled by the courts. Matthew Hickson was handed a 28-month prison sentence on Monday after pleading guilty to two counts of possession of a controlled substance for the purpose of trafficking — one for cocaine, the other for fentanyl. Canadian Press (Trail Times)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

'People just don't disappear:' Family asks for help to find woman missing a year
The daughter of a woman who disappeared a year ago is asking anyone with information to come forward and give the family closure. Thelma Krull, 57, went for a walk in her Winnipeg neighbourhood last July 11 and hasn't been seen since. "A whole year has passed and we still have no idea what happened or why," her daughter, Lisa Besser, said at a police news conference Monday. "It's extremely hard not knowing — not knowing if she's coming home again or never again, not knowing if she'll be at another birthday party, Christmas, family event." Someone out there has to know something, Besser said. Canadian Press (Metro News)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

NIL

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

NIL

INTERNATIONAL

Banerjee: Bangladesh must halt the creep of terrorism
An opinion piece states "In the eve of the closure of the holy month of Ramadan before Eid al-Fitr, Islamic militants stepped up attacks in Afghanistan, struck Istanbul, Baghdad, Dhaka and its outskirts and Saudi Arabia. The attack in Dhaka, the capital of Bangladesh, on July 1, and the second attack in a Eid prayer ground outside the Dhaka city limits, on July 7, are particularly deeply shocking as the world has witnessed the slide of a state with a secular constitution, albeit with Muslim majority, down the dangerous slope of violence and terror that are gripping the world. Bangladesh emerged as a nation directly out of a movement of liberation from an Islamic republic – Pakistan. The independence movement was based on Bengali cultural identity and rights of self-determination. The nation's original constitution embraced secularism, social justice, pluralism and diversity, despite 90 per cent of the population following Islam. One may argue that these foundational principles were not well protected by governments in power at different periods of time in Bangladesh's history, since 1971. But Bangladeshi Muslims had certainly made their mark as moderate followers of Islam; and despite dysfunctional politics, Bangladesh has served as a role model for low-income countries in the new millennium." Ottawa Citizen

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

RalphGoodale
Heureux de voir cette nouvelle entente finalisée entre le Canada et l'Ukraine, tel que promis http://bit.ly/29KlJq0 #cdnpoli

RalphGoodale
Glad to see this new trade deal finalized between Canada and Ukraine, as promised http://bit.ly/29JRUqQ #cdnpoli

No One Is Illegal
BREAKING: Immigration detainees in two prisons are refusing food until they meet with Minister Ralph Goodale....
http://fb.me/7Zhbblrei

No One Is Illegal
BREAKING! - 50 Detainees refusing food demanding justice. Tell @RalphGoodale to meet detainees #CdnPoli #CdnImm

globalnewsto
Immigration detainees on hunger strike, request meeting with public safety minister glbn.ca/xdA9MD

natnewswatch
Immigration detainees on hunger strike nationalnewswatch.com/2016/07/11/imm…

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

TheTorontoSun
Fort McMurray firefighters' "lives are going to be shortened" because of wildfire battle. ow.ly/lXW13028VQF pic.twitter.com/iGJV7fJbKa

CBCSask
Funnel clouds formed as warnings ended not capable of causing much damage: Environment Canada cbc.ca/news/canada/sa…

chintapuxley
Flash floods plaguing Saskatchewan communities with more heavy rain forecasted. Story by CP's @JGrahamCP

globalnews
Toronto may join growing number of US cities with 911 texting if @norm gets his way https://t.co/4XDehlttm2

RadioCanadaInfo
Le sol de Fort McMurray n'est pas dangereux pour les humains, selon des tests effectués en juin bit.ly/29zttQf

chronicleherald
Nova Scotia Power launches new outage map herald.ca/nLp pic.twitter.com/vutfvsQN4t

NATIONAL SECURITY / SÉCURITÉ NATIONALE

bccla
Canadian government expects another #Snowden-level leak, documents say @TorontoStar: https://www.thestar.com/ #cdnpoli #privacy #surveillance

BORDER SECURITY / SÉCURITÉ FRONATLIÈRE

GlobalRegina
#Sask CBSA officers seize alcohol, drugs and weapons in June glbn.ca/vhwmha

GlobalSaskatoon
#Sask CBSA officers seize alcohol, drugs and weapons in June glbn.ca/GPrHJR

Stewart Bell
Former Iraqi diplomat ordered deported from Canada http://natpo.st/29JZoKd @nationalpost

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

SCMagazine
Hidden voice commands in #YouTube vids can hack mobile devices https://t.co/lusY6DjzAi

LAW ENFORCEMENT / APPLICATION DE LA LOI

CBCPpolitics
Bob Paulson tells Mounties taking off-duty community assignments not an 'expectation' cbc.ca/news/politics/… #cdnpoli #hw

TVA Nouvelles
Tensions avec les policiers de Montréal? http://bit.ly/29lLOdt

CastanetNews
Axe woman tased, beaned (Kootenays) bit.ly/29E4Yz5

CBCManitoba
RT @RileyLaychuk: Rural Manitoba police constable among few wearing body cameras cbc.ca/1.3671410 #cbcmb #bdnmb

chronicleherald
UPDATE: Man to be tried for murder, interfering with body of Nova Scotia police officer herald.ca/nux pic.twitter.com/Gmaf0Uf70r

CTVNewsVI
Granite plaque commemorating Const. Sarah Beckett unveiled in @WestshoreRCMP garden vancouverisland.ctvnews.ca/rcmp-unveils-m…

calgarysun
Platt: Viral video of arrest shows why body cameras are critical for public trust ow.ly/BJUY3028hPT #yyc pic.twitter.com/8sanoZ0xHb

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

CBCKW891
'Institutional resistance' to treating inmates with mental health issues, Senator Bob Runc… ift.tt/29KJiQu pic.twitter.com/YcjiI03Leb

CastanetNews
Rapist to call Kelowna home #Kelowna bit.ly/29DUS17

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

VancouverSun
Five hospitalized after drug overdoses at Coquitlam house - Emergency crews were at a Coquitlam house Sunday ni... https://t.co/JXXopLymb2

John Howard Society
Opioid antidote now free at Ontario pharmacies. Implementation for those leaving jail not yet clear http://www.thespec.com/

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

chronicleherald
Winnipeg police call for help in case of woman who disappeared a year ago herald.ca/nLA#.

OTHER / AUTRES

TheTorontoSun
Concordia professor being held in Iranian jail now reportedly facing charges. http://ow.ly/MqYP3028S0s

INTERNATIONAL

lesoir
Fusillade dans un tribunal au #Michigan : au moins deux blessés et trois morts http://bit.ly/29KQtYQ

TheTorontoSun
2 bailiffs and gunman dead in shooting at western Michigan courthouse. http://ow.ly/WkuD3028S9k

WSJ
Investigators believe the Dallas shooter legally purchased weapons online or at a gun show https://t.co/ED1AMijGR6

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

Today's News / Actualités
July 11, 2016 / le 11 juillet 2016
14:00 - 20:00 ET

This collection contains news items that appeared online between 2:00 p.m. and 8:00 p.m., Eastern Time.
Ce recueil contient des actualités qui ont paru sur Internet entre 14h00 et 20h00, heure de l'Est.

Today's News can also be accessed through Newsdesk / Les Actualités peut également être accédée via InfoMédia

MINISTER / MINISTRE

Immigration detainees on hunger strike; want meeting with public safety minister
A group advocating for full immigration status for all migrants says more than 50 immigration detainees began refusing food Monday in two Ontario centres. The End Immigration Detention Network says the detainees are protesting prison conditions that include increasing lockdowns and the use of solitary confinement, and are calling for an end to indefinite detentions in maximum security prisons. The immigration detainees are asking for a meeting with **Public Safety Minister Ralph Goodale** to discuss their concerns. **A spokesman for Goodale** says **the minister** is working on issues related to detention and hopes to put forward proposals later this year... The End Immigration Detention Network says immigration detainees previously went on a hunger strike that began on April 21, and met with officials from Canada Border Services Agency. But the group says CBSA has not followed through on promises it made and the detainees have begun the new hunger strike — this time calling for a meeting with elected

officials."We would like to meet with MPs," said Toby Clark, who has been in immigration detention since August 2014…Sharmeen Khan of End Immigration Detention Network said detainees are often on long lockdowns during the summer — sometimes kept in their cells for days in a row, unable to speak with their families, or get legal support. "**Goodale** must meet with the detainees, and commit to upholding international norms and basic human rights by ending immigration detention," Khan said… **Goodale spokesman Scott Bardsley said** Monday in an email that CBSA is required to consider all reasonable alternatives before detaining someone. ***"Under Canadian law, detention is only allowed when: identity is not certain, there is a flight risk or a danger for the public," Bardsley said. Goodale*** has met with the United Nations High Commissioner for Refugees, the BC Civil Liberties Association, the Canadian Association of Refugee Lawyers and others to discuss detention issues, **he said**. ***"Our goal is to ensure our Canadian approach is world-class, including our methods of enforcement, with effective transparency and accountability."*** Canadian Press (Coast Reporter, The Record)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Funnel clouds formed as warnings ended not capable of causing much damage: Environment Canada
Environment Canada says many of the funnel clouds seen on Sunday in the Saskatoon area were only capable of producing landspout tornadoes, which are not capable of doing much damage. Technically the clouds could have formed tornadoes but they would be in the form of landsprout tornadoes, according to Natalie Hasell, warning preparedness meteorologist with Environment Canada. CBC News

Saskatoon residents warned of heavy rainfall rolling in
City crews are cleaning catch basins and priming pumps in anticipation of heavy rain expected to settle in the next 24 hours. Jeff Jorgenson, with the City of Saskatoon, said that workers and systems are in good shape as the clouds darken. Environment Canada has issued a rainfall warning for Saskatoon, forecasting between 60 and 100 millimetres by Wednesday. CBC News; News Talk 650

UPDATE: Nova Scotia Power launches new outage map
Nova Scotia Power has launched an online map that delivers near-live power outage reports on mobile devices. The outage map, which launched on Sunday, will automatically be updated every 15 minutes and can be viewed directly from your smartphone or tablet. Chronicle Herald

Toronto may join growing number of US cities with 911 texting
A city council vote this week could set Toronto on the path to becoming the first jurisdiction in Canada where all residents can send text messages to 911 operators instead of calling them. Coun. Norm Kelly is calling on the city to request that the Toronto Police Services Board consider adopting emergency texting. Many parts of Canada, including Toronto and 500 other Ontario communities, offer 911 texting for people with hearing or speech impairments. Text service for people with special needs also exists in Manitoba, New Brunswick, Nova Scotia, most of Quebec, and parts of Alberta and British Columbia. But emergency texting for people without hearing or speech impairment is not available anywhere in Canada. Canadian Press (Global News)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

NIL

BORDER SECURITY / SÉCURITÉ FRONATLIÈRE

Sask. CBSA officers seize alcohol, drugs and weapons in June
The Canadian Border Service Agency (CBSA) seized 147 litres of undeclared alcohol, as well as drugs and guns in some June border seizures in Saskatchewan. On June 16 CBSA officers in Saskatoon were examining international commercial shipments in a warehouse when they discovered 147 litres of alcohol

inside a container. In addition they also seized wood, meat and medicine that weren't declared, the CBSA said. Global News

Prohibited Weapon, Undervalued Boat Among June Border Seizures at Prince Rupert
A prohibited gun found hidden in various parts of a vehicle and an undervalued boat were the two most notable seizures made by Canada Border Services Agents in Prince Rupert last month. The CBSA says both seizures were made at the Alaska Marine Highway ferry terminal. On June 14th, someone trying to bring in a 27-foot boat was forced to pay over $30,000 US, after officers determined it had been undervalued by nearly $24,000 US. CFTK TV

Canadian Men Accused of Trying to Smuggle Cocaine, Ecstasy Across Border
Three Canadian men have been accused of trying to smuggle more than a $1 million worth of cocaine and ecstasy through the remote Yaak River region of Lincoln County. Kristopher Glenn Pfeifer and Preston Frederick Lahmer were charged in U.S. District Court in Missoula with felony conspiracy to possess controlled substances with intent to distribute and possession with intent to distribute a schedule one controlled substance. Matthew Desmond Browne was charged with one count of felony conspiracy to possess controlled substance with intent to distribute and one count of felony possession with intent to distribute cocaine. Flathead Beacon

Marble Restaurants Ltd. of Edmonton receives significant sentence under Immigration and Refugee Protection Act
MARBLE Restaurants Ltd. in Edmonton on June 28 pled guilty to employing a foreign national without authorization and failure to follow terms of a Labour Market Impact Assessment (LMIA), and was sentenced under the Immigration and Refugee Protection Act (IRPA). The Canada Border Services Agency said that between February 2014 and April 2015, Marble Restaurants Director Shamez Jivraj employed a woman as a housekeeper and part-time caregiver in his home, despite having received authorization to only employ her as a food counter attendant at the restaurant. Jivraj did not adhere to hours or occupational role set out in the LMIA, but continued to pay the woman as an employee of Marble Restaurants Ltd. Voice Online

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

Companies must directly notify people affected by privacy breaches: watchdog
Companies that lose personal customer data should be required to directly notify affected people — with limited exceptions — about the nature and date of the lapse along with steps taken to reduce the harm, says the federal privacy watchdog. The Trudeau government plans to introduce breach-notification regulations in coming months to improve transparency and help consumers. Several large businesses have been stung by hackers in recent years, causing embarrassment for proprietors and potential headaches for customers whose personal and financial details are suddenly circulating in cyberspace. Canadian Press (Metro)

NATO sites downed as measures approved opposing Russian aggression
Three days after the North Atlantic Treaty Organization's Allied Transformation Command websites were knocked offline, the alliance has yet to release official comments over the cause of the outage that felled two military command websites. The outages occurred during a NATO summit held in Warsaw last week, raising suspicions that Russian hackers could have attacked the websites in response to the summit's initiatives opposing Russian military aggression. "This is a suspicious timing for a technical failure," a senior NATO official said, according to a Wall Street Journal report. "If this is a cyberattack, it would be no surprise." On Friday, NATO approved measures to place US, UK, Germany and Canada-led battalions along member nations' borders with Russia. The battalions are expected to be placed in Estonia, Latvia, Lithuania and Poland by early next year. The intergovernmental alliance also on Friday approved language that defines cyberspace as a domain of war. SC Magazine

Hidden voice commands in YouTube vids can hack mobile devices
Hidden voice commands embedded in a YouTube video can trigger mobile devices to download malware and alter configuration settings, according to ZDNet. A team made up of researchers from the University of California, Berkeley, and Georgetown University, have created a technique capable of compromising a mobile device via voice commands embedded into a YouTube video. The signal is imperceptible to viewers, but is able to trigger commands within a nearby device, whether a laptop, computer, smart TV, smartphone or tablet. On Apple systems, Siri receives the message and on Android systems, Google Now interprets the signal. In attempting to warn of the risks inherent in increasingly ubiquitous voice interfaces, the researchers note how "an attacker uses the speech recognition system as an opaque oracle." The incursion could enable attackers to issue instructions to any nearby mobile device to initiate a download of malware or adjust configuration settings, which could then lead to a compromise of the device and the possibility of surveillance. SC Magazine

LAW ENFORCEMENT / APPLICATION DE LA LOI

Bob Paulson tells Mounties taking off-duty community assignments not an 'expectation'
The commissioner of the RCMP has told his officers they are not expected to take part in community events while off duty if they don't want to, after CBC revealed Mounties across the country were declining "red serge duty" in a protest over working conditions. Bob Paulson made the comments in an email to staff dated July 8 and obtained by CBC News. "Many of our members choose to represent their RCMP profession in the community activity they engage in while off duty," Paulson said in the email, which does not mention the CBC story. "That is outstanding and frankly represents the professionalism and privilege many of us feel as employees of the force. But there is no rule or expectation that everyone do so." Last week, the CBC learned that some Mounties were no longer volunteering to appear in parades, fairs and festivals wearing their ceremonial red uniforms and Stetson hats in protest over unsustainable understaffing and overall morale issues within the force, among other irritants. CBC News

Axe woman tased, beaned
Police in the Kootenays arrested an axe-wielding woman without injury to her or the attending officers. Castlegar RCMP arrested the violent and distraught woman in Robson Saturday morning. “Reports had been received that the woman was damaging a home with an axe,” said Cpl Dan Moskaluk. The call came in at after 11 a.m. July 9. “Upon police arrival, Castlegar RCMP officers found the woman outside of the residence, where it is alleged that the woman, who while armed with an axe, repeatedly made threatening gestures and approaches towards the RCMP officers,” said Moskaluk. Castanet.net

Tensions avec les policiers de Montréal?
Alors que les tensions sont vives aux États-Unis entre les policiers et les membres de la communauté noire, le maire de Montréal ne croit pas que ce soit le cas ici. Pourtant, des experts disent le contraire. Certains policiers du Service de police de la Ville de Montréal (SPVM) croient surtout qu'il est important de distinguer le profilage racial du profilage criminel. Pourtant les intervenants rencontrés par TVA Nouvelles disent le contraire, mais surtout qu'il y a toujours du travail à faire. TVA Nouvelles

Rural Manitoba police constable among few wearing body cameras
Chief Const. Darwin Drader is the lone officer for the Rural Municipality of Cornwallis' police department in western Manitoba. But with the simple click of a switch, he's now got a second set of eyes when he's on calls. Drader has started using a small body-worn camera while on the job in the Rural municipality, located on the outskirts of Brandon and about 200 km west of Winnipeg. It's believed he's the only police officer in the province currently doing so…The RCMP also said officers in Manitoba aren't wearing cameras. It's not known if there are plans to implement their use but they have been tested out at a small number of detachments across the country. CBC News

UPDATE: Man to be tried for murder, interfering with body of Nova Scotia police officer
A man accused of killing an off-duty Nova Scotia police officer and disposing of her body near a Halifax bridge will be committed to stand trial. Christopher Calvin Garner, 28, was in court Monday for a preliminary hearing on charges that he committed second-degree murder and interfered with a dead body

in the death of Truro officer Catherine Campbell last September... A sworn affidavit from an RCMP officer obtained prior to the hearing says Garnier allegedly told police he punched and strangled Campbell at an apartment in the city. Chronicle Herald

RCMP unveils memorial plaque for slain West Shore Mountie
West Shore RCMP have unveiled a new memorial for fallen Const. Sarah Beckett, who died in the line of duty earlier this year. The granite stone plaque was installed Monday in a memorial garden commemorating Beckett at the West Shore detachment in Langford. CTV News

Viral footage of violent Calgary police arrest shows officer worn cameras critical to public trust
An opinion piece states "Where there's no trust, there must be cameras. That's not to say the Calgary Police Service did anything wrong on Friday night, in an arrest that's since because fodder for every armchair cop critic, thanks to an amateur video showing 21-seconds of the violent detainment on 17 Ave. S.W., outside a pub. But that's not to say the three-on-one arrest was right, either -- and from a layman's perspective, without context, it does look like very harsh treatment for the person being busted, with one cop dishing out several punches to the man's face, and pulling his hair while he is pinned to the ground..." Calgary Sun

Collingwood man charged after police seize LSD, magic mushrooms, cocaine
Magic mushrooms, LSD and cocaine were some of the drugs seized by police from a Collingwood home last week. Members of the Organized Crime Enforcement Bureau, Central Drug Enforcement Unit, Community Drug Action Team (CDAT) and Collingwood OPP seized 70 grams of cocaine, 85 grams of marijuana, a small amount of LSD, magic mushrooms as well as cash, prohibited knives and brass knuckles from a Second Street home July 7. Simcoe.com

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

'Institutional resistance' to treating inmates with mental health issues, Senator Bob Runciman says
There is a 100-bed unit at The Royal mental health centre in Brockville, Ont., that is dedicated to federal male inmates, and in 14 years, there has never been a suicide and no one has ever escaped. "They've had a tremendously successful track record of reducing reoffending rates and turning lives around," Senator Bob Runciman told CBC Radio's The Morning Edition host Craig Norris Monday. Despite this success, Runciman said, there is still resistance in the correctional system to treating people with mental health issues by placing them in a secure facility like the one in Brockville. That needs to change, he said. Especially after it appears a female offender being held at the Grand Valley Institution in Kitchener, Terry Baker, took her own life last week... There was a pilot project where Correctional Service Canada had one bed in the Brockville facility, but those at The Royal said it wasn't enough, they needed at least 10 beds, according to Runciman. That didn't happen and the pilot project failed, Runciman said. CBC News

Rapist to call Kelowna home
A notorious Calgary rapist is moving to Kelowna at the end of this week. Known as the Falconridge Rapist, the Parole Board of Canada confirms reports that Andrew Aurie Jefferson is set to be released from a federal corrections institute on Friday, with plans to take up residence in Kelowna. Jefferson, 31, gained notoriety nearly a decade ago after terrorizing women at knifepoint during a series of armed street attacks. He was convicted in 2008 of the 2006 violent rape of two women in Calgary. After spending time in prison for the assaults, Jefferson was supposed to be released in Kelowna in 2011, but chose Mission as his new home instead. Two years later, he was put back behind bars after a violent 2013 carjacking in Langley. Friday will mark his second statutory release from the federal system, mandated by law when offenders complete two-thirds of their sentence. Just like his release in 2011, the Parole Board states that Jefferson is considered a high risk to reoffend sexually. He will be required to follow strict rules upon his release including a residency condition requiring him to live in a halfway house or other facility chosen by the Correctional Service of Canada. Castanet.net

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Five hospitalized after drug overdoses at Coquitlam house
Emergency crews were at a Coquitlam house Sunday night to deal with multiple overdoses. Just before 11 p.m., police were called to the home in the 800-block of MacIntosh Street to assist ambulance and fire crews already on the scene, according to Coquitlam RCMP Const. Pamela Newman. Vancouver Sun

Fentanyl sentencing same as other drugs, unless Parliament acts: B.C. judge
A judge in Kelowna declined to consider the presence of fentanyl an aggravating factor in handing down a sentence for trafficking the highly potent and potentially deadly synthetic opioid, saying it's up to Canadian lawmakers to dictate how the drug should be handled by the courts. Matthew Hickson was handed a 28-month prison sentence on Monday after pleading guilty to two counts of possession of a controlled substance for the purpose of trafficking — one for cocaine, the other for fentanyl. Canadian Press (Trail Times)

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

'People just don't disappear:' Family asks for help to find woman missing a year
The daughter of a woman who disappeared a year ago is asking anyone with information to come forward and give the family closure. Thelma Krull, 57, went for a walk in her Winnipeg neighbourhood last July 11 and hasn't been seen since. "A whole year has passed and we still have no idea what happened or why," her daughter, Lisa Besser, said at a police news conference Monday. "It's extremely hard not knowing — not knowing if she's coming home again or never again, not knowing if she'll be at another birthday party, Christmas, family event." Someone out there has to know something, Besser said. Canadian Press (Metro News)

REGULATION OF MARIJUANA / RÉGLEMENTATION DE LA MARIJUANA

NIL

PUBLIC SERVICE / FONCTION PUBLIQUE

NIL

OTHER / AUTRES

NIL

INTERNATIONAL

Banerjee: Bangladesh must halt the creep of terrorism
An opinion piece states "In the eve of the closure of the holy month of Ramadan before Eid al-Fitr, Islamic militants stepped up attacks in Afghanistan, struck Istanbul, Baghdad, Dhaka and its outskirts and Saudi Arabia. The attack in Dhaka, the capital of Bangladesh, on July 1, and the second attack in a Eid prayer ground outside the Dhaka city limits, on July 7, are particularly deeply shocking as the world has witnessed the slide of a state with a secular constitution, albeit with Muslim majority, down the dangerous slope of violence and terror that are gripping the world. Bangladesh emerged as a nation directly out of a

movement of liberation from an Islamic republic – Pakistan. The independence movement was based on Bengali cultural identity and rights of self-determination. The nation's original constitution embraced secularism, social justice, pluralism and diversity, despite 90 per cent of the population following Islam. One may argue that these foundational principles were not well protected by governments in power at different periods of time in Bangladesh's history, since 1971. But Bangladeshi Muslims had certainly made their mark as moderate followers of Islam; and despite dysfunctional politics, Bangladesh has served as a role model for low-income countries in the new millennium." Ottawa Citizen

SOCIAL MEDIA / MÉDIAS SOCIAUX

Twitter

MINISTER / MINISTRE

RalphGoodale
Heureux de voir cette nouvelle entente finalisée entre le Canada et l'Ukraine, tel que promis http://bit.ly/29KlJq0 #cdnpoli

RalphGoodale
Glad to see this new trade deal finalized between Canada and Ukraine, as promised http://bit.ly/29JRUqQ #cdnpoli

No One Is Illegal
BREAKING: Immigration detainees in two prisons are refusing food until they meet with Minister Ralph Goodale.... http://fb.me/7Zhbblrei

No One Is Illegal
BREAKING! - 50 Detainees refusing food demanding justice. Tell @RalphGoodale to meet detainees #CdnPoli #CdnImm

globalnewsto
Immigration detainees on hunger strike, request meeting with public safety minister glbn.ca/xdA9MD

natnewswatch
Immigration detainees on hunger strike nationalnewswatch.com/2016/07/11/imm…

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

TheTorontoSun
Fort McMurray firefighters' "lives are going to be shortened" because of wildfire battle. ow.ly/lXW13028VQF pic.twitter.com/iGJV7fJbKa

CBCSask
Funnel clouds formed as warnings ended not capable of causing much damage: Environment Canada cbc.ca/news/canada/sa…

chintapuxley
Flash floods plaguing Saskatchewan communities with more heavy rain forecasted. Story by CP's @JGrahamCP

globalnews
Toronto may join growing number of US cities with 911 texting if @norm gets his way https://t.co/4XDehlttm2

RadioCanadaInfo
Le sol de Fort McMurray n'est pas dangereux pour les humains, selon des tests effectués en juin bit.ly/29zttQf

chronicleherald
Nova Scotia Power launches new outage map herald.ca/nLp pic.twitter.com/vutfvsQN4t

NATIONAL SECURITY / SÉCURITÉ NATIONALE

bccla
Canadian government expects another #Snowden-level leak, documents say @TorontoStar: https://www.thestar.com/ #cdnpoli #privacy #surveillance

BORDER SECURITY / SÉCURITÉ FRONATLIÈRE

GlobalRegina
#Sask CBSA officers seize alcohol, drugs and weapons in June glbn.ca/vhwmha

GlobalSaskatoon
#Sask CBSA officers seize alcohol, drugs and weapons in June glbn.ca/GPrHJR

Stewart Bell
Former Iraqi diplomat ordered deported from Canada http://natpo.st/29JZoKd @nationalpost

CYBER SECURITY / SÉCURITÉ CYBERNÉTIQUE

SCMagazine
Hidden voice commands in #YouTube vids can hack mobile devices https://t.co/IusY6DjzAi

LAW ENFORCEMENT / APPLICATION DE LA LOI

CBCPolitics
Bob Paulson tells Mounties taking off-duty community assignments not an 'expectation' cbc.ca/news/politics/… #cdnpoli #hw

TVA Nouvelles
Tensions avec les policiers de Montréal? http://bit.ly/29lLOdt

CastanetNews
Axe woman tased, beaned (Kootenays) bit.ly/29E4Yz5

CBCManitoba
RT @RileyLaychuk: Rural Manitoba police constable among few wearing body cameras cbc.ca/1.3671410 #cbcmb #bdnmb

chronicleherald
UPDATE: Man to be tried for murder, interfering with body of Nova Scotia police officer herald.ca/nux pic.twitter.com/Gmaf0Uf70r

CTVNewsVI
Granite plaque commemorating Const. Sarah Beckett unveiled in @WestshoreRCMP garden vancouverisland.ctvnews.ca/rcmp-unveils-m…

calgarysun
Platt: Viral video of arrest shows why body cameras are critical for public trust ow.ly/BJUY3028hPT #yyc pic.twitter.com/8sanoZ0xHb

CORRECTIONAL SERVICES / SERVICE CORRECTIONNEL

CBCKW891
'Institutional resistance' to treating inmates with mental health issues, Senator Bob Runc… ift.tt/29KJiQu pic.twitter.com/YcjiI03Leb

CastanetNews
Rapist to call Kelowna home #Kelowna bit.ly/29DUS17

COMMUNITY SAFETY & PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

VancouverSun
Five hospitalized after drug overdoses at Coquitlam house - Emergency crews were at a Coquitlam house Sunday ni... https://t.co/JXXopLymb2

John Howard Society
Opioid antidote now free at Ontario pharmacies. Implementation for those leaving jail not yet clear http://www.thespec.com/

NATIONAL INQUIRY INTO MISSING AND MURDERED INDIGENOUS WOMEN AND GIRLS / ENQUÊTE NATIONALE SUR LES FEMMES ET LES FILLES AUTOCHTONES DISPARUES ET ASSASSINÉES

chronicleherald
Winnipeg police call for help in case of woman who disappeared a year ago herald.ca/nLA#.

OTHER / AUTRES

TheTorontoSun
Concordia professor being held in Iranian jail now reportedly facing charges. http://ow.ly/MqYP3028S0s

INTERNATIONAL

lesoir
Fusillade dans un tribunal au #Michigan : au moins deux blessés et trois morts http://bit.ly/29KQtYQ

TheTorontoSun
2 bailiffs and gunman dead in shooting at western Michigan courthouse. http://ow.ly/WkuD3028S9k

WSJ
Investigators believe the Dallas shooter legally purchased weapons online or at a gun show https://t.co/ED1AMijGR6

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

Lacroix-Menard, Gabriel (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Wednesday, April 01, 2015 11:02 PM
To: Today's News / Actualités (PS/SP)
Subject: Toronto Star: Canada's spy review bodies struggling to keep tabs on agencies (Minister quoted)

Canada's spy review bodies struggling to keep tabs on agencies
Toronto Star
Alex Boutilier
April 1 2015

The review bodies for both of Canada's intelligence agencies are raising concerns about their ability to keep track of the country's spies.

The warnings come as the Conservatives continue to insist that Canada does not require increased oversight into the Canadian Security Intelligence Service or the Communications Security Establishment.

The Security Intelligence Review Committee (SIRC), which reviews CSIS actions, said continued vacancies on the five-person board, the inability to investigate CSIS operations with other agencies, and delays in CSIS providing required information are "key risks" to the committee's mandate.

Meanwhile, the Office of the Communications Security Establishment Commissioner warned that the growth of the massive electronic spying agency, coupled with fiscal restraint at the commissioner's office, is a "constant concern."

The two review bodies combined boast about 30 full-time employees and an annual budget of roughly $5 million, according to government documents. The agencies they review are expected to spend more than $1 billion this year, and CSE alone has more than 2,000 employees.

The concerns were raised in both agencies' plans and priorities reports, which outline the expected actions and spending of government departments and agencies for the year.

They come as Parliament continues to debate Bill C-51, which would give CSIS a much wider mandate to investigate and "disrupt" threats to Canada's national security.

Many critics who testified about the bill, and a good number of witnesses who support it, have argued there should be some measure of parliamentary oversight into the actions intelligence services take on Canadians' behalf.

But **Public Safety Minister Steven Blaney**, responding to questions in the House of Commons Wednesday, said Canada's review system is the ***"envy of the world."***

***"We will continue to support them,"* Blaney** said of the review bodies.

Blaney has argued that SIRC provides adequate review of CSIS activities, and that additional oversight would simply be ***"needless red tape."***

In its report, however, the SIRC admitted it can review only a "small number" of the spy agency's actions each year.

"Currently, SIRC reviews still lack the ability to 'follow the thread' of a CSIS investigation if it involves another government department or agency," the SIRC wrote.

"SIRC's effectiveness is dependent on (CSIS's) timely provision of information. In those cases where there are delays in receiving information, SIRC is at risk of being unable to complete its reviews and investigations in a timely manner."

Both SIRC and the CSE commissioner reported their review capacity depends on co-operation with the agencies they look into — while both are separate and independent from the agencies, both say they require a close working relationship. The CSE commissioner's report went so far as to say the success of their reviews is "fundamentally reliant on the relationship between the office and CSE."

Both review bodies also say they need to work together. SIRC's mandate is to review CSIS operations, but not CSIS's co-operation with CSE. Without seeing how the different agencies interact — including with the RCMP, which has civilian review, and Military Intelligence, which has no civilian review — the CSE commissioner said it's difficult to see the whole picture.

"Information sharing among intelligence agencies at the national and international level requires at minimum some co-operation among the various review and oversight bodies," the report notes.

CSIS's operations have been well known since the intelligence branch of the RCMP was separated from the law enforcement mandate. The operations of CSE, on the other hand, have attracted widespread attention only through the leaks of whistleblower Edward Snowden.

Working from those disclosures, The Intercept and CBC revealed CSE has developed a suite of cyberwarfare tools, and had a goal to become more aggressive in their use by 2015.

Other documents leaked by Snowden suggest CSE has engaged in mass Internet surveillance of file-sharing sites, and collects massive amounts of Internet traffic through 200 "Internet backbone" sites worldwide through a program called EONBLUE.

Bill Galbraith, the executive director of the CSE commissioner's office, said he could not discuss whether the office is looking into those disclosures.

"The reviews that we are conducting cover a range of signals intelligence activities, IT security activities, and there is a major review of metadata underway," Galbraith said in an interview.

Deborah Grey, the former Conservative MP and current acting chair of the SIRC, could not be reached for comment on Wednesday.

How the review bodies measure up:

18 – The number of full-time equivalent positions at the SIRC

11.5 – The number of full-time equivalent position at the CSE commissioner's office

$5 million – Roughly how much both offices have to spend this year

$537 million – Amount CSIS expects to spend in 2015-2016 alone.

2,175 – Number of employees at CSE

Link

Lacroix-Menard, Gabriel (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Sunday, May 22, 2016 7:12 AM
To: Today's News / Actualités (PS/SP)
Subject: Toronto Star: Is CSIS concealing security breaches? (Department mentioned)

Is CSIS concealing security breaches?
Alex Boutilier
Toronto Star
2016-05-22, 03:27 ET

A federal watchdog is looking into claims that Canada's spy agency had only one serious privacy violation in 2015, the Star has learned.

The Canadian Security Intelligence Service reported its one privacy breach last year only after the spy agency was urged to by an independent review body.

Privacy commissioner Daniel Therrien said he'll contact CSIS to ensure they're following government-wide rules to report all serious breaches to his office.

"It is certainly something to investigate with CSIS," Therrien said in an interview Friday.

"I will follow up with CSIS to inquire as to whether they think they're bound by (the reporting requirement), (and) whether truly there was only one incident to be reported."

Documents recently tabled in Parliament revealed federal departments and agencies logged 5,853 privacy and data breaches in 2015. Taken together, the breaches involved 45,892 individual Canadians.

CSIS did not disclose its one reported incident in the parliamentary documents, citing national security concerns, but confirmed it when contacted by the Star.

In 2014, the federal government created a new rule that all "material" privacy breaches - those that could cause serious damage to Canadians, or affect a large number of individuals - must be reported to Therrien's office and the Treasury Board.

Material privacy breaches can range from the relatively minor - misdirected mail or electronic files mistakenly accessed - to serious incidents, such as stolen hard drives or improper snooping.

But the parliamentary documents reveal that in 2015, only 304 breaches were disclosed to the commissioner - 5.2 per cent of the total.

CSIS was asked to report one incident by the Security Intelligence Review Committee, an independent body that looks into the agency's operations.

The agency had been accessing taxpayer information at the Canada Revenue Agency without a warrant - a practice that CSIS itself reported to the SIRC and asked them to investigate. It's not clear how many people were affected by the breach.

In a statement, CSIS said it was bound by the policy to disclose material breaches. But when asked if the agency proactively reports breaches, or only does so at the SIRC's direction, a spokesperson said only that the agency respects Canadian law and ministerial directive.

"The (SIRC) reports to Parliament on the operations of CSIS," spokeswoman Roxanne Ouellette wrote in a statement.

"SIRC ensures that powers given to CSIS are used legally and appropriately, in order to protect Canadians' rights and freedoms.

In response to an official request to detail the number of privacy and information breaches from NDP MP Alexandre Boulerice, CSIS said they have "robust" protections in place for private information.

"CSIS maintains robust policies and procedures in regards to its collection activities and in its information management polices and procedures," the agency wrote.

"For reasons of national security, CSIS does not disclose information related to data, information, or privacy breaches."

The agency declined to provide a global number of breaches in 2015, as requested.

Other departments on the national security file, such as **Public Safety (two breaches)**, the Canadian Border Services Agency (35), and the RCMP (52) were more forthcoming.

RCMP Const. Annie Delisle said the force reviews potential privacy breaches before reporting them to both the privacy commissioner and Treasury Board.

"While the RCMP would not disclose specific details of a privacy breach that could compromise national security, or ongoing operations and investigations, it is still obligated to report that a breach has occurred," Delisle wrote in a statement.

Therrien said some national security agencies seem to be concerned that reporting to his office as well as their own review bodies would create duplication.

He said he is open to discussing how the privacy office could work with review bodies like the SIRC to provide efficient and effective oversight on privacy files.

"We're only two or three years after the Snowden revelations," Therrien said, referring to U.S. whistleblower Edward Snowden.

"I don't think it's the time now to reduce the jurisdiction of review bodies. ... I think it is more time to facilitate the sharing of information between oversight bodies so that we can do our job as efficiently as possible."

In a recent submission to a parliamentary committee, Therrien recommended that the duty to report privacy breaches to his office be enshrined in law.

Sent to: !INTERNAL & RCMP Breaking News & CBSA Breaking News

Lacroix-Menard, Gabriel (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Sunday, September 25, 2016 8:43 PM
To: Today's News / Actualités (PS/SP)
Subject: Toronto Star: National electronic intelligence agency executive calls for 'rational debate' on encryption (Department mentioned)

National electronic intelligence agency executive calls for 'rational debate' on encryption
Toronto Star
Alex Boutilier
September 25, 2016

Canadians are being encouraged to ask more questions about the security of their electronic devices from an unlikely source: an executive at the country's electronic intelligence agency.

Scott Jones, the deputy director of IT security at the Communications Security Establishment, said Canadians need to start taking a greater interest in how their electronic devices protect personal information.

"We should be asking when we go and buy the stuff we have at home, OK, tell me how it's being protected," Jones said in an interview.

"If it's my cellphone, does it have encryption if I lose it? Can somebody just read the data off of it or not? We need to start asking questions like that … We need to start helping each other, and helping citizens, helping businesses, helping the government when we're buying these products they need to be secure by default."

It may surprise some to hear an employee at CSE counselling Canadians to protect their private information. The agency, which has largely operated in secret since its creation at the end of the Second World War, was thrust into the spotlight after U.S. whistleblower Edward Snowden's disclosures.

CSE is part of the Five Eyes alliance, which includes security agencies in the United States, the United Kingdom, Australia and New Zealand. Snowden's disclosures drew back the curtain on mass surveillance programs used by those countries, including programs that scooped up their own citizens' communications.

Jones' comments also come as law enforcement agencies in the U.S. and Canada are forcefully arguing for limiting citizens' ability to secure their information through encryption programs — calling for so-called "backdoors" that would let authorities decode the data.

When this is pointed out, Jones agreed the encryption debate is a difficult one to resolve.

"I don't take it personally, because I think it's a really important question," Jones said.

"(We need) a rational debate over the tools that law enforcement needs to do its job, right? I trust law enforcement to keep me safe, but I also trust the legal system to protect my privacy as well, and to find a balance. But we haven't been able to have those conversations in this country (yet)."

While police and intelligence agencies argue about whether citizens should have access to strong encryption, the federal government, on the other hand, is trying to improve its own electronic defences.

Known as "Part B" of CSE's mandate, cyber-defence operations require the agency to work with a host of other federal departments to try and protect government information — including Canadians' personal information.

For serious cyberattacks, the response could include the RCMP, CSIS, **Public Safety**, Shared Services Canada, even Global Affairs and the Privy Council Office.

"Cyber is not a singular dimensional problem, it's not just a technical issue or the computer system, it's also about the objective of the compromise or what the threat actor was trying to obtain," Jones said.

"You can't have the master of cyber in a single department, because to do that you'd have to create the department of everything."

The Liberal government is in the middle of a wide-ranging review of Canada's approach to cyber security, and Jones expects the encryption debate to figure into that larger discussion.

The government has also pledged to review Ottawa's overall national security regime, beginning with increased oversight from a parliamentary committee, and to roll back some of the powers granted to intelligence agencies through the Conservatives' controversial terrorism law, Bill C-51.

Sent to: !INTERNAL; !INTERNAL 2; CBSA Breaking News; RCMP Breaking News

Lacroix-Menard, Gabriel (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Monday, March 28, 2016 4:34 PM
To: Today's News / Actualités (PS/SP)
Subject: Transcript: CBC-R1 - The Current - Tolerance for collateral damage too low: ex-CIA Director General Hayden - 2016-03-28 - 09h04 ET

Follow Up Flag: Follow up
Flag Status: Completed

SOURCE:
CBC – R1

PROGRAM:
THE CURRENT

DATE:
MARCH 28, 2016

TIME:
09:04 ET

LENGTH:
23:40 MIN

SUBJECT:
TOLERANCE FOR COLLATERAL DAMAGE TOO LOW: EX-CIA DIRECTOR GENERAL HAYDEN

[CLIP] – DONALD TRUMP (Republican Presidential Candidate Frontrunner): *I said, they're chopping off our heads in the Middle East. They want to kill us. They want to kill us. They want to kill our country. They want to knock out our cities. And don't tell me it doesn't work. Torture works, okay folks? Torture… you know I have these guys, "torture doesn't work." Believe me, it works, okay? And waterboarding is your minor form. Some people say it's not actually torture. Let's assume it is. But they ask me the question: what do you think of waterboarding? Absolutely fine. But we should go much stronger than waterboarding. That's the way I feel.*

LYNCH: That of course is Republican frontrunner Donald Trump, absolutely convinced that torture is the way to go in the fight against terrorism. He's also said it's a pretty good idea to target the families of terrorists, despite that being a war crime under international law. While Trump's ideas may be winning him some support, it's causing unease among people whose job it is to actually hunt down terrorist fighters.

One of them is Michael Hayden. He was the director of the National Security Agency from 1999 until 2005, and the director of the Central Intelligence Agency from 2006 until 2009. He's the only person ever to hold both positions. He's now the author of a new book, Playing to the Edge: American Intelligence in the Age of Terror, and Michael Hayden joins me from Washington, D.C.

Hello.

GENERAL MICHAEL HAYDEN (Ex-NSA and CIA Director and Author): Hi Laura.

LYNCH: General, what do you think of what Donald Trump said? Morality and war crimes aside, does torture work?

GENERAL HAYDEN: Wow, where to begin? How to unpack all that you just played. Look, let me give you the gut feeling of what Mr. Trump is saying, and how people like me feel about this.

Number one: he seems to be doing this out of enthusiasm. Whatever we did, and again, honest men can argue about it, we did not do out of enthusiasm, we did out of duty and occasionally out of regret. He says we ought to do this because they deserve it. We never did anything to these people because they deserved it. We're not the arm of American justice, this is American intelligence. This was never backward-looking, this was forward-looking. And again, people can disagree with what we did, and…

LYNCH: And people do…

GENERAL HAYDEN: Yes.

LYNCH: But you do say in the book – you point to examples of where you say it was effective…

GENERAL HAYDEN: Right.

LYNCH: … in gathering information.

GENERAL HAYDEN: Right. But again, just back to motivation and distinguishing what happened, to what he's claiming he would do, this was forward-looking, and it was about safety, and then finally… finally what we did was rare. We did it on three, and only three people, and the last time in 2003. He appears that he wants to do it routinely.

LYNCH: Okay, so that comment and his comment about going after the families, what do you think of that? Do you think that that's an appropriate role for America's military or intelligence agencies?

GENERAL HAYDEN: Well, two broad thoughts. With regard to waterboarding, I have said in other fora and I'll repeat for your audience, Laura, if a future president wants to waterboard somebody, he'd better bring his own bucket because the agency I'd led will not do it. Not because they disagreed with what they'd done in the past, but they frankly feel betrayed by the society they served because of what's happening… happened to them afterwards.

And with regard to targeting the innocent, violating the Geneva Convention and going after women and children because they happen to be related to terrorists, that's such a fundamental violation of the laws of armed conflict, that my expectation would be that if that order ever popped up in the American command and control system, the first American in uniform, man or woman, would simply turn to whomever had given the order to him or her and simply say, this just isn't going to happen.

LYNCH: You would defy an order of the Commander-in-Chief?

GENERAL HAYDEN: I… I… I fully expect an order so black and white as that one, I can't picture the American Armed Forces carrying it out.

Now, Laura, to be perfectly honest, you know, innocents die in combat. It's called collateral damage, and there is a moral judgement to be made with regard to the eternal principle of war with regard to distinction and proportionality. How many of the innocent might die, and is that target really necessary? That happens all the time, and frankly, I think right now our threshold for collateral damage under President Obama in Syria is too low. In the end, more innocent people will die because you have not disabled an enemy that does intentionally target the innocent.

LYNCH: And there are some who would certainly dispute that argument with you who say that the civilians dying in the name of killing those who are labelled as terrorists is simply not acceptable. But when you hear Donald Trump speak about fighting terrorism and maintaining security at home, and the words obviously concern you, but does it worry you that he might be a threat to national security?

GENERAL HAYDEN: Well, one hopes that whenever anyone becomes president, what the permanent government – you know, the folks I left behind at these agencies – try to impose on the President-Elect is their world view. I have a line in the book, Laura, and I applied it to the 2008 election, and it would have applied no matter who won – Senator Obama or Senator McCain – and it's simply this: our job is to point out to the newly-elected president, that national security looks different from the Oval Office than it does from a hotel room in Iowa.

LYNCH: I guess you're hoping that'll be true if Mr. Trump becomes president.

GENERAL HAYDEN: That's right.

LYNCH: I want to ask you about the recent attacks in Paris and Brussels. I'm wondering, what did these attacks tell you about the state of intelligence-gathering these days?

GENERAL HAYDEN: Yeah, sadly these attacks were not a surprise. They were somewhere between expected and inevitable, knowing what it was we knew and knowing what it was we didn't know about the ISIS network in Europe. These were fairly mature attacks. Multiple targets. High-end targets sequentially done, synchronized. This wasn't cooked up in somebody's basement the night before, and it's clear that the attacks for their success depended upon a network that could get the weapons, could get them hidden, could get the detonators, could get everyone to the targets on time, and so on.

And so, I fear the extent of this network is broader than we know, and it remains there as a clear and present danger to safety. I should add, Laura, in Europe.

LYNCH: But did intelligence fail?

GENERAL HAYDEN: Well, I mean the attack took place, and so, yeah, when you look back as to what happened, both intelligence – and in this case law enforcement because we are talking about domestic activities in these countries – appears to have been well short of need.

LYNCH: Let me go back to a very dark day in American history – one that was certainly dark for you and many other Americans. You were the head of the National Security Agency the day the planes flew into the World Trade Centre and the Pentagon and in the field in Pennsylvania. What were your main concerns in the minutes and hours after that attack?

GENERAL HAYDEN: Yeah, the first concern I had was to protect my workforce, not because that was a moral imperative—not just because it was a moral imperative—but it was an operational imperative. The nation would be badly damaged if we lost the talent that is represented by the NSA workforce. So the first thing I did was to evacuate all non-essential personnel, and then I took the essential personnel, Laura, and to the best of our ability got them out of the highrise headquarters building and put them into an older three-storey operations building that goes back to the near-founding of the agency. Get them out of the highrises, get them into the low building, let the non-essential folks go home. And then the other thing we started to do, Laura, was to build in plans, not just to protect America, but to protect ourselves.

LYNCH: And I want to get to that, but I need to ask you in light of what we were just discussing with Brussels and Paris, this was an intelligence failure, was it not?

GENERAL HAYDEN: What, 9/11?

LYNCH: Yeah.

GENERAL HAYDEN: Yeah. We freely admit that it was a failure, but, you know, if you let me step back, and this is not meant to be in the defense of the community of which I was a part, but to describe more broadly the issues we all face, I agree mistakes were made. My agency made some, CIA, FBI in the run-up to this. But given the overall condition of the country, Laura, given the state of law enforcement, the state of law, the way we had decided to protect ourselves against what we viewed to be the threat, if this 9/11 had been stopped, another 9/11 would have happened.

The reason we're safer after 9/11 than we were before, is not just that our intelligence got better, but that we as a nation decided to go on a war footing, and that totality is what has made us safer.

LYNCH: You write about a meeting that took place shortly after that involving intelligence services of Britain, Australia, New Zealand, the U.S and Canada, and you were told by Britain at that time that there needed to be a discussion about balancing security with freedom, and I'm wondering how the U.S responded to that advice.

GENERAL HAYDEN: Oh, no! We welcomed that. We all knew that... we all share that Anglo-Saxon democratic tradition. I mean, we've got shades of differences between and among us, you know, parliamentary governments, presidential governments, and so on, but we all go back to the same trunk of the tree, to the same roots. And in that meeting, Eliza Manningham-Buller, who then was Deputy MI5 -- later became the head -- she summarized it quite well. She said: our societies are all accustomed to do what it is we have to do to those who are guilty. Our challenge in the intelligence services is to devise what it is we must do to find and ferret out those who are not yet guilty. That's a real challenge.

LYNCH: Okay, and so your response to this is, the president asked you to find out what you can do, you write about a top secret program you launched called Stellarwind that's attracted a lot of controversy over the years. What was Stellarwind?

GENERAL HAYDEN: Yeah, Stellarwind, if you just step back for a second, Laura, talking about how we were as a society before 9/11, we, in the United States had decided the best way to get both freedom and security, liberty and privacy, was to create divisions until we kind of shoved all the foreign stuff to one side, all the domestic stuff to another, shoved all the intelligence activity to one side, all the law enforcement stuff to the other side, and we kept those separate as the best compromise to buy both security and liberty, safety and privacy. Those 19 hijackers drove down that seam between those characteristics that I just described.

So the challenge we had was how then do we... do we tighten up, in a world in which we kept foreign and domestic intelligence and law enforcement information isolated from one another... And the challenge – we responded to the challenge in many ways, but one of them was the Stellarwind program, which was designed to detect terrorist communications that should have been at the highest importance to the United States, terrorist communications one end of which was in this country, right?

LYNCH: And yet, you seem somewhat aware of the fact that you were, as you say "clinging to the edge" because you write in your book about taking a walk with your wife at Fort Meade and telling her you were about to do something controversial.

GENERAL HAYDEN: Right.

LYNCH: And you write, and I'm going to quote here: "I was comfortable with doing it because it was right, but at some point there was going to be high political and reputational risk, and I couldn't rule out legal risk either."
Why did you think that?

GENERAL HAYDEN: Because... a subsequent president might decide that what this president had authorized was, in one way or another, illegal or unconstitutional. Now, as it turned out, Laura, the next president – President Obama – not only did not do that, he actually doubled-down on the program and actually expanded it. On the other hand, some of the things that CIA had been doing, which are not the subject of that chapter, the incoming president decided, quite arbitrarily in my view, that what the agency had been ordered to do actually constituted felonies. And there were investigations of CIA officers.

So, you know, eyes wide open, reputational risk was going to be there, political risk certainly, and could not rule out legal risk -- I still thought it was, not just the right thing to do but the legal thing to do. My lawyers told me that our president, under his Article 2 authorities, did indeed have the power to—in this case—ignore the FISA Statute and go ahead and authorize us to gather metadata.

LYNCH: Now your words there that I read in that quote, someone like Edward Snowden might make the same case. He knew leaking the documents carried a legal risk, but he thought it was the "right thing" to do for the country, so what's the difference?

GENERAL HAYDEN: Well, the difference is that I stayed in this country and was willing to... willing to go under anything the American political or legal system would have me do. I did not go to a third country and remain there. You know, I don't view what I did to be civil disobedience, since I was doing it under the authority of the president with the approval of the Attorney General. Mr. Snowden has indeed conducted what he believed to be civil disobedience, and if you read the American classic on civil disobedience, Henry David Thoreau's piece, he says that civil disobedience takes its moral meaning from the willingness to suffer the consequences of your action legally. Mr. Snowden does not appear to be willing to do that.

LYNCH: And you disagree with what he did, obviously.

GENERAL HAYDEN: Yes.

LYNCH: Now I just recently though... the former Chief of Staff to Colin Powell, Colonel Lawrence Wilkerson said Snowden has done a service. He called him, and I'm going to use the words that he used: courageous, logical, impressive, he refrained from releasing anything truly dangerous, he was circumspect, altruistic motives, more helpful than dangerous...
What do you think of Colonel Wilkerson's assessment?

GENERAL HAYDEN: That's fundamentally an idiotic statement because Snowden stole more than a quarter of a million documents. He was largely unaware of the content of the documents. He freely admits that he didn't curate the documents, and so I mean, you know, I would just raise the question: what's the civil liberty's quotient of telling the world that the National Security Agency is intercepting the unclassified emails of the Syrian Armed Forces? Actually, about 1 or 2% of what the man released had to do with American privacy. The other 98% had to do with how America collects foreign intelligence, and one has to wonder, why did he shove all that other stuff out the door if his question was about American privacy?

LYNCH: I want to play you a clip now from February the 5th 2003, and this is Colin Powell, then the Secretary of State, making his case for war against Iraq before the UN Security Council:

[CLIP] – COLIN POWELL (Secretary of State-2003): *Let me begin by playing a tape for you. What you're about to hear is a conversation that my government monitored that takes place on November 26th of last year, on the day before United Nations teams resumed inspections in Iraq. The conversation involves two senior officers, a colonel and a brigadier-general from Iraq's elite military unit, the Republican Guard (plays conversation).*

LYNCH: Now, in your book you write that Colin Powell used NSA intercepts to build the case that Saddam Hussein had weapons of mass destruction and you… and of course we know that case was wrong…

GENERAL HAYDEN: Right

LYNCH: As the head of the NSA at the time, how convinced were you, really, that Saddam Hussein had weapons of mass destruction?

GENERAL HAYDEN: I was convinced enough to vote "yes" in the ultimate meeting we had on the National Intelligence Estimate. The rhythm, Laura, in our… in our intelligence organization is that the director of Central Intelligence, George Tenet, brings in the head of the three-letter agencies, we discuss the conclusions, the key judgements of the NIE, and I bid… voted in favour of each of the conclusions. I was wrong.

I did have a private conversation that I mention in the book, with Condi Rice, saying, Condi, I've got a room full of evidence this guy's doing this, I got to tell you though, Condi, all my evidence is circumstantial. Now before you jump on that, Laura, I tell another story in the book where President Obama is talking to Mike Morell, one of the good guys at the CIA that worked with me and was a senior. And the President was asking him, Michael, you guys seem all over the map in terms of whether Osama bin Laden is in that compound in Abbottabad or not. What are the people in the agency really saying? And the answer Michael gave was, well, Mr. President, anybody who touched the Iraq NIE is saying it's 50/50. Those folks who… who studied only Osama bin Laden and Al-Qaeda are giving it 90/10. And the president said, ah… so I understand. And then Michael interrupted him, because Michael had a very good relationship with the president, and Michael said, Mr. President, I gotta tell you, all the evidence that Osama bin Laden is in that compound is indeed circumstantial…

LYNCH: But you raise the question, is circumstantial good enough to take a nation to war—a war that's led to the destabilization of Iraq and…

GENERAL HAYDEN: Oh! Well…

LYNCH: … and the rise of extremist groups like ISIS?

GENERAL HAYDEN: Well, look… look… George… George Tenet makes the point that that NIE was the public justification for war, it was not the casus belli. But Laura, the purpose of intelligence is not the same purpose of evidence in a court of law where you're supposed to get things beyond all reasonable doubt. The purpose of intelligence is to enable action even in the face of lingering doubt.

I was asked by an American, actually a venture-capitalist, on a scale of zero to ten, how would you rate… right… rate CIA analysis? And the first thing I said was, we don't do 8, 9, or 10. If we can get it to 8, 9, or 10, they aren't asking us the question, they're chucking it down to the Department of Commerce or the Interior or somebody. We get a lot right, we… and that I freely admit, we got this one wrong.

LYNCH: Let's wind up our conversation then by taking it back onto your territory, the United States…

GENERAL HAYDEN: I should say…

LYNCH: Republicans often accuse President Obama of being weak when it comes to targeting of Islamic extremists – you've spoken of him already of his efforts to double-down on some of the programs you have – what do you think of that charge against him?

GENERAL HAYDEN: So, a couple of macro judgements, alright? And this may surprise your Canadian listeners, but in my heart of hearts, and I actually mention it in the book, Laura, in terms of fighting terrorism, there are bigger changes between President Bush's first and second administrations than there were between the Bush and the Obama administration. When you talk about recalibrating our fight, there was more done to do things differently between 43.1 and 43.2, than there was between 43 and 44.

LYNCH: And these are the numbers of the presidents?

GENERAL HAYDEN: Yes.

LYNCH: Just in case the listeners...

GENERAL HAYDEN: Sorry (laughs)...

LYNCH: That's okay.

GENERAL HAYDEN: Yeah. And so... so the first thing is the remarkable continuity between two incredibly different presidents which actually has disturbed some folks abroad who thought this was all about George Bush. Actually, it appears that a whole lot of it was all about America. Not Texas, not George Bush. So that's one.
That said, I got my complaints. And I do think what we're doing against ISIS in Iraq, in Syria, my line Laura has been: under-resourced and over-regulated. I would have used more firepower. I would have put more American forces. I would have pushed them more forward into the battle space — no one is calling for American manoeuvre brigades back there — but right now, Americans can't go below the brigade level even advising the Iraqi army.

And then, finally, to come back to a point we've discussed two or three times, I do think our tolerance for collateral damage is far too low. I do think, to successfully conduct a necessary and just war, we do have to accept the fact that from time to time, despite our best efforts, people we're not mad at might be hurt.

LYNCH: And that might be a difficult sell for the public, again. But I've got to ask you this, do you... you still have security clearance, do you not?

GENERAL HAYDEN: I do.

LYNCH: So, tell me, when you take a look at the world today, what do you think is the biggest national security threat facing the next president?

GENERAL HAYDEN: I... I...

LYNCH: You can tell me secrets. Go ahead.

GENERAL HAYDEN: Yeah, sure. I... I... look, I look at it three ways. And so, Laura, if you imagine I've got a graph between us. I've got an X axis and a Y axis, and the vertical axis is how bad is it, and the horizontal axis is how immediate is it... in the lower left-hand corner, I put "terrorism and cyber-attacks." In other words, they're very immediate. We have a TSA agent make a bad decision here, something bad could happen tonight.

LYNCH: You mean the airport screening...

GENERAL HAYDEN: Right, right. But as the president is correct in pointing out, that's not an existential threat to the United States. It's bad, but it doesn't threaten our existence.

Now you run the timeline on a little bit, Laura, three, four, five years, and here I bump into another problem: this is a group of states that I've taken to labelling "ambitious, brittle, and nuclear," And here I include the North Koreans, the Iranians, the Pakistanis, and maybe even the Russians. That's actually more serious. If that goes bad, it's a lot worse, but it's not going to happen overnight. We've got some time—three, four, or five years.

And then I go further out on my timeline to about the ten year point, and way up there, something that is really important is the long-term relationship of the United States and the People's Republic of China. And here I'm not talking about China

as a threat like I might view North Korea or terrorism, I'm just talking about the reality of Chinese emergence. If that is not handled well, Laura, the rest of this probably doesn't matter. You know, this is the whole historical tale of the emerging power and the status quo power. Far too many times in human history, the way we get from the old to the new equilibrium, to accommodate the emerging power, is a process that popularly goes by the name "global war." We don't want that one.

LYNCH: What about global warming?

GENERAL HAYDEN: Well, I... well you asked me my list. I've given you my list.

(Laughter)

LYNCH: Okay. General Hayden, I thank you very much for your time.

GENERAL HAYDEN: Okay Laura, thank you.

LYNCH: Bye-bye.

GENERAL HAYDEN: Bye.

LYNCH: Michael Hayden was the director of the National Security Agency from 1999 until 2005, and the director of the Central Intelligence Agency from 2006 until 2009. His new book is called: Playing to the Edge: American Intelligence in the Age of Terror, and he was in Washington, D.C.

Questions? Please contact us at PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.
Questions? Veuillez communiquer avec nous au PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Sent to: !INTERNAL

Lacroix-Menard, Gabriel (PS/SP)

From: PSPMediaCentre / CentredesmediasPSP (PS/SP)
Sent: Thursday, January 28, 2016 4:20 PM
To: Today's News / Actualités (PS/SP)
Subject: Transcript: CSE senior officials provide a not-for-attribution technical briefing on the 2014-2015 CSE Commissioner's annual report - 2016-01-28, 11:00 ET

DATE/DATE:
January 28, 2016, 11:00 a.m. ET

LOCATION/ENDROIT:
National Press Theatre, Ottawa, ON

PRINCIPAL(S)/PRINCIPAUX:
Senior Official from the Communications Security Establishment

SUBJECT/SUJET:
A senior official from the Communications Security Establishment (CSE) provides a not-for-attribution technical briefing about the 2014-2015 CSE Commissioner's annual report.

CSE Official 1: Good day, everyone, Mesdames et Messieurs. My name is [name withheld] and I'm the [title withheld] for the Communications Security Establishment. Today a CSE departmental official will provide a background briefing on the CSE Commissioner's 2014-2015 annual report. Following the briefing, we'll be able to answer some questions, so until 11:15. With this in mind, the briefing will be done predominantly in English, but we're able to answer questions in both official languages.

Aujourd'hui, un représentant officiel de la CST présentera quelques éléments contextuels portant sur le Rapport annuel du commissaire de CST pour l'exercice 2014-2015.
As already indicated in the media advisory, this briefing is provided on background only, and is not for attribution.

We ask that all quotes be attributed to a CSE official. Cameras are not permitted, nor is there any recording for broadcast purposes.

Tel que indiqué dans l'avis aux médias, la présente séance d'information ne fournira que les renseignements généraux et ne sera pas offert à des fins d'attribution. Toutes citations devraient être attribuées à un représentant officiel de CST. Il est interdit d'utiliser des caméras ou de enregistrer afin de diffusion. Today's briefing will be provided by [name withheld], the [title withheld] at CSE. With that, I pass it (off microphone).

CSE Official 2: Thank you, [name withheld]. Bonjour. Good morning. So as [name withheld] pointed out, my name is [name withheld]. I am the [title withheld] for the Communications Security Establishment, and I'm here this morning to provide a background briefing about certain aspects of CSE's Commissioner's annual report for 2014-2015. I'll make an initial statement, and then I'll try to answer as many questions as possible, keeping in mind, as I'm sure you can appreciate, that there are some questions I will not be able to answer for operational reasons. As you all know, I am bound to secrecy on national security matters by the Security of Information Act. And as [name withheld] just pointed out, the briefing is not for attribution, and you can identify me as a senior CSE official.

So this morning the Minister of National Defence tabled the CSE Commissioner's annual report for 2014-2015. The CSE Commissioner is a fully independent review body with dedicated resources and expert staff authorized to review CSE's activities. He and his staff have full access to CSE's facilities, information holdings, and employees at all stages of their review activities.

Le commissaire du CST, l'honorable Jean-Pierre Plouffe, présente des rapports classifiés au ministre de la Défense nationale tout au long de l'année. Il lui remet ensuite un Rapport annuel non classifié qu'il dépose également à la Chambre des communes, comme il l'a fait ce matin.

The annual report for 2014-2015 summarizes nine classified reports, including: a review of metadata activities related to CSE's Foreign Signals Intelligence Program; a review of CSE's information technology security activities conducted under ministerial authorizations; a review of the Canadian Armed Forces' Cyber Support Detachments; a review of CSE's assistance to CSIS under Part C of CSE's mandate and Section 16 of the CSIS Act; and three annual reports – an annual review of disclosures of Canadian identity information; an annual review of CSE's Privacy Incidents File and Minor Procedural Errors Record; and finally, an annual review of Foreign Signals Intelligence Ministerial Authorizations. That particular review included two separate spot check reviews of intercepted private communications. So that brought the total number of reviews this year in the 2014-2015 annual report to nine.

Dans son Rapport annuel, le commissaire du CST a aussi formulé huit recommandations qui visent à favoriser le respect de la loi et à renforcer les mécanismes de protection de la vie privée. Le CST et le ministre ont tous deux accepté ces huit recommandations, et j'aimerais souligner que toutes les activités du CST ayant fait l'objet d'un examen en 2014-2015, à l'exception d'un examen portant sur les métadonnées, ont été déclarées conformes aux lois en vigueur.

So in terms of that one exception, you will have seen from the Minister's statement and the Commissioner's statement, both released this morning, that the Commissioner has completed his assessment of the metadata activities that raised legal questions. The Commissioner has made a determination and found CSE to be non-compliant with the law, in particular Sections 273-6-4 and 273-6-6 of the National Defence Act, and, as a result, Section 8 of the Privacy Act.

The Minister of National Defence has reviewed the Commissioner's annual report and the finding of non-compliance, and has accepted his recommendations on this matter. Namely the two recommendations from the report were: that CSE seek an updated ministerial directive that provides clear guidance related to the collection, use, and disclosure of metadata in a foreign signals intelligence context; and, that CSE use its existing centralized records system to record decisions and actions taken regarding new and updated collection systems, as well as decisions and actions taken regarding minimization of metadata. I'll get into definitions in a moment. It is therefore on this metadata review and the Commissioner's subsequent finding of non-compliance that I intend to focus the remainder of this briefing.

So what happened? As the Commissioner points out in his report, his office has been reviewing CSE's collection and use of metadata for quite some time. In fact, almost every review by the CSE Commissioner touches on CSE's metadata activities as they are core – a core component of both our Foreign Signals Intelligence and Cyber Defence programs. An early, more focused review on metadata occurred in 2006, and following that, subsequent reviews of metadata over the years have led to a number of recommendations that CSE has accepted and implemented. Planning by the Commissioner for a broader review of CSE's collection, use, and sharing of metadata is highlighted in his report and began around 2012, with a first report of that broader review focusing on CSE's use of metadata in a foreign signals intelligence context.

At the early stages of this review, CSE discovered on its own that certain types of metadata containing information with a Canadian privacy interest were not being minimized properly before being shared with CSE's Five Eyes partners in the United States, the United Kingdom, Australia, and New Zealand. After making this discovery, CSE proactively suspended the sharing of this metadata with its partners. The Chief of CSE informed the Commissioner as well as the Minister of National Defence about the matter. The Chief of CSE assured the Commissioner and the Minister that the suspension will remain in effect until systems are in place to effectively protect the privacy of Canadians related to that specific metadata.

So as I mentioned, I think it's important to pause here to explain a couple of very important terms. First of all, metadata. We have prepared a fact sheet that we've posted on our website today that describes what metadata is, why CSE collects it, how we use it, and how we share it. Metadata is critical to understanding the communications environments in which CSE operates. As you have heard many times, metadata is the context but not the content of a communication. Context, not content. We have defined it as information used to identify, describe, manage, or route a telecommunication or any part of a telecommunication, as well as the means by which it is transmitted.

Metadata plays a vital role in all of CSE's signals intelligence activities. CSE would not be able to conduct any signals intelligence operations without the context and lead information that metadata provides. Metadata helps us understand the networks we're targeting. Without understanding the environment in which we operate, we are blind. We use metadata to discover and track foreign targets. Without targets, we're essentially deaf. And we use it to understand anomalies in network behaviour and identify cyber threats. Without knowing these threats, we're at risk.

I'll also note that the use of metadata is pervasive. For example, telecommunications companies must use metadata to route communications from the originor (ph) to the recipient, or to manage high volumes of Internet activity. Anti-virus companies use metadata to study patterns of network activity, to reveal the efforts of hackers and other actors who want to breach network security defences, and the anti-virus companies then turn their analysis into measures that can improve

the security of the networks they defend. And indeed, advertising companies use metadata to understand the viewing patterns of Internet users and insert information of potential interest into your browsing activities.

So metadata is used for many purposes for a variety of reasons, but as far as CSE's metadata is concerned, we have a legal mandate to collect, use, and share it, albeit within certain limitations. As the Commissioner clearly states in his report, the National Defence Act mandates CSE to acquire and use information, including metadata, to understand the global information infrastructure, to provide intelligence on foreign entities located outside of Canada, or to protect computer networks and systems of importance to the Government of Canada. A ministerial directive on metadata provides additional guidance and places limits on CSE's metadata activities. In fact, both the National Defence Act and the ministerial directive also require CSE to have in place measures and – measures to protect the privacy of Canadians in conducting these activities.

So we have also on our website a fact sheet that highlights how CSE protects the privacy of Canadians. In our end-to-end activities, we apply various measures to help protect the privacy of Canadians. We have developed and – very detailed operational policies and procedures that establish specific measures to protect the privacy of Canadians and persons in Canada in the use and retention of intercepted communications. There is always a clear focus on the prohibition against directing any of our activities at Canadians or at anyone in Canada, highlighted in our policies and procedures. Our focus is also on networks most likely to have foreign targets. We avoid other networks. Only trained, tested operational and policy personnel have access to any of our data. We have time limits on the retention of data. We apply caveats on reports regarding the use of information. And of course all of CSE's activities, including collection and use of metadata, are reviewed by the CSE Commissioner.

As for the term minimization, it describes the process by which information that could be used to identify a Canadian is rendered unidentifiable before it is shared with allies.

So back to the issue. CSE discovered on its own that certain metadata was not being properly minimized prior to being shared with our Five Eyes partners due to technical deficiencies. What do we mean by technical deficiencies? It's important to underscore the complexity and the dynamic, changing nature of our operating environment. CSE must constantly adjust systems to reflect the ongoing evolution of technology. In this case, a system upgrade, which we do to address the dynamic technological environment I just described, led to the discovery of a deficiency in our automated systems responsible for some of our minimization activities related to some subsets of metadata. As a result, some metadata with a potential Canadian privacy interest was shared with our Five Eyes sig—partners.

So you're probably going to be asking the most important question, which is what was the impact of this unintended sharing with our partners. The unminimized metadata had a privacy interest, but it did not contain specific names or identities. Additional and indeed sometimes significant analysis would have been required before any unintentionally shared data could be associated with a specific Canadian. In light of this, and given the fact that the other measures in the suite of privacy protections I mentioned earlier remained effective, the privacy impact of the technical deficiency in this case was assessed as low. The protection of the privacy of Canadians is CSE's legally mandated responsibility, and it is one of our most important principles. It guides our mission to contribute to the security of our country and our citizens, and it is a principle all our employees appreciate and understand as being fundamental to a democratic society.

I do want to reiterate, as I prepare to answer your questions, that I'm limited in what I can say, in particular regarding information about CSE's signals intelligence activities. I have to be careful not to disclose national security related information that could point to our targets, our capabilities, our trade craft, our partnerships, etcetera. I'm about to be done. One last thing, and then I'll open it up to questions.

At a time when the threats from foreign signals – or rather, foreign states – terrorists, and cyber criminals are increasing, it is more important than ever to protect our national interests, our critical infrastructure, and our people. CSE has been at work protecting Canada and Canadians for over 70 years. We help to ensure the nation's prosperity, security, and stability. And we do this with a full understanding and appreciation of the necessity of privacy of Canadians and for Canadians. The principles of lawfulness and privacy are engrained in everything CSE does: in our systems, our processes, our policies, and, most importantly, our people. It is for that reason we advised the Commissioner's office of the technical deficiencies we discovered in our systems, and it's for that reason that I am here today. So thank you, and I'll now turn things over to [name withheld], who can moderate questions.

CSE Official 1: Thank you, [name withheld]. So we're going to open the floor to questions. We'll be – like I said, we'll be able to address your questions until 11:30. To give everyone a chance to participate, please limit yourself to one question and one follow-up. If you still have questions after 11:30, please, our media relations folks will be happy to take your calls. So we'll start just at the back there with the – just in front of you (off microphone).

Question: Could you give a sense of how you came to have this Canadian information? You mentioned that you're prohibited from directing your activities towards Canadians, so how is it that you found yourself with Canadian metadata in the first place?

CSE Official 2: So you're quite right, we are prohibited from targeting any of our activities at Canadians, or anyone in Canada for that matter. But as you can appreciate, we do have a legal mandate to collect information from the global information infrastructure for purposes of foreign signals intelligence in this case, or to defend systems of importance to the Government of Canada. As I think is apparent in the actual report, on our website in terms of how we describe our activities, we have collection systems. Those collection systems collect information from the global information infrastructure, and that global information infrastructure doesn't have a place that says here is somewhere where Canadians don't go. Obviously, when you're collecting metadata to try and understand what communications are transpiring in order to get ultimately to a foreign target, you need to be able to collect information. And so we collect metadata, and in that metadata it stands to reason that incidentally you're going to be collecting metadata related to Canadians.

Question: That sounds like (off microphone) interception, like mass interception.

CSE Official 2: I'm not going to get into the details of our capabilities, but certainly we have collection systems, and those collection systems vary.

Question: Can you give us a sense of how many people this may have affected in terms of how many individual Canadians may have had parts of their personal information or metadata shared with allies?

CSE Official 2: So the complexity of the systems – the complexity of our systems, the dynamic nature of the global information infrastructure means that everything is constantly changing. And we don't just have one system; we have several systems. So it becomes very difficult to answer your question specifically. We do regular upgrades. A regular upgrade of our system identified that certain fields of metadata were not being minimized. We assessed that those certain fields did have a Canadian privacy interest. But the metadata that was shared does not contain enough information on its own or contextual details to identify individuals associated with the metadata. So you can't – we never drilled down to does this point the finger at one particular Canadian. So as a result, there wasn't – there was no drilling down to have to identify that there was a Canadian.

The complexity of it makes it impossible to be able to tell you the actual volume. There are retention periods, there are various systems that do different things. And so as a result, I think the important thing is – is that the privacy impact was assessed at low, we identified that there was a problem with the minimization function, we stopped that sharing of that specific metadata until such time as we're able to fix it.

CSE Official 1: Okay, we'll move on. And if I can ask you to identify yourself as well, please.

Question: Daniel Thibeault, Radio-Canada. Est-ce que – sans rentrer dans le détail exactement des informations qui ont été transmises, sans – je comprends que c'était pas pour permettre l'identification d'un individu en particulier, mais c'était un lieu géographique, c'était un fournisseur de services internet? Qu'est-ce qui – qu'est-ce qui vous a accrochés? Qu'est-ce qui semblait être un problème de divulgation?

CSE Official 2: Je vais répondre en anglais. J'espère que les – vous avez une interprétation simultanée. Donc je suis plus confortable avec les termes en anglais, alors si vous me permettez, je vais répondre en anglais.

The – it's impossible to get in that detail metadata. Metadata, as I tried to describe, and as indeed we have a fact sheet that will walk you through it, there are all sorts of subfields of metadata. And the National Defence Act requires us to have measures in place to protect the privacy of Canadians. Indeed, the ministerial directive states you have to – it elaborates a little bit further on what kinds of measures we have to have in place, including the measure of minimizing.

So internally, we constantly have to look at metadata, because it's always evolving. We have to look at metadata and we have to say, as we're collecting it, we have to evaluate which fields we believe have a Canadian privacy interest. And if we believe that it – we do an assessment, and if we believe that it does, we then have to make sure that we have systems that will minimize that if we want to share that. So again, I don't have any specific for you in terms of in this particular case. There were examples of some subsets of metadata that we noticed had been altered when we did a systems upgrade, and our minimization system wasn't addressing it, and therefore we had to stop.

Question: Existe-il des garanties que cette information-là qui était transmise aux partenaires des Five Eyes n'a pas été ensuite transmis à d'autres agences à l'extérieur du groupe de Five Eyes?

CSE Official 2: In terms of guarantees, we have – obviously this has been a topic, I think, of debate for several years now in terms of the information sharing. We have a Five Eyes partnership. It's existed for over 70 years. We have policies, processes, procedures in place. We benefit from the information sharing that we have. I think I highlighted the fact that we have a whole series of privacy measures in place to make sure that, just because this one measure failed, that we don't have other measures in place to make sure that, if there was a potential impact on the privacy of any Canadian, that we would have other measures in place that would have caught it and made sure that we would have protected it.

So what I mean by that is, if we are to share it, only certain people that are cleared are actually available to access the information. Our allies, as are we, are bound by the fact that they cannot target Canadians. So they would not be going and looking into a pool of information that we would have shared to look for a specific Canadian. They would have had to do significant analytics. And even if they would have gotten to the end of those analytics and found a Canadian, and they – at the end of the day, in the cryptologic agency world, that turns out to a end product report. In the end product report, they would have had to have minimized the identity of the Canadian, if they even ever got to that point, and they would have had to have told us about it.

And in terms of guarantees, there are never any guarantees, but certainly in our relationship we constantly are talking to each other and we're flagging these things for each other. I also believe that, in his report, the Commissioner cites the fact that he did go down to one of our partners, for example the NSA, he met with the Inspector General that reviews NSA and got assurances that indeed they follow policies and procedures that meet our requirements.

CSE Official 1: Thank you. And just behind you, and I'll come to you right after.

Question: Philippe-Vincent Foisy de Cogeco. Juste comprendre en termes de temps combien de temps on a donné de l'information qui pouvait être avec des privacy interest? À quel moment vous l'avez remarqué et ça va être suspendu pendant combien de temps ce partage-là?

CSE Official 2: Encore, c'est très – j'ai pas envie de – c'est très compliqué. Le monde dans lequel on opère est très, très compliqué. On a – on a – il y a beaucoup de systèmes. Je sais, je sais.

I mean, just to give you an idea of, you know, metadata, what we're – what we do with metadata, we thwart tens of millions of cy—of malicious cyber attempts every day – every day, tens of millions. To give you an idea of how complex the various systems, so when one of our systems, when we're upgrading it and we discover that there's an issue – so in this particular case, we discovered it towards the end of 2013. Okay? To give you – to give you a sense of timing. It was the end of 2013. Notified the Commissioner, notified the Minister. The Commissioner was – actually, his office was undergoing a review, and so we started doing a bunch of analytics to unders—for them to understand and explain, etcetera.

In terms of trying to go back in time to say, well, how long has this error been occurred, I think that's where the recommendation came out from the Commissioner in terms of improving our records keeping practices. Because he wasn't satisfied that we were actually able to keep track. The fact of the matter is we are. We have some – we have very good records keeping practices. But in this particular case, because of the complexity, we needed to be able to discover exactly why the problem occurred, how it occurred, and how to make sure that if we continue and turn the sharing back on, that the privacy measures of minimization are in place.

How long is it going to be until we actually share information again? We haven't resumed sharing. We've told the Commissioner, we've told the Minister that – and we're keeping both apprised of our efforts in this particular complex matter, and we won't resume sharing until it's done. I can't give you a timeframe, unfortunately.

Question: Juste pour comprendre, donc d'abord vous pouvez pas garantir que l'info qui a été partagée à nos alliés n'a pas été repartagée par la suite? Et j'ai pas compris, la collecte de données d'info canadienne, comment vous faites pour avoir les infos sur les Canadiens?

CSE Official 2: Donc je vais répondre à votre première question, puis ensuite je pense que je veux avoir une clarification sur votre deuxième. Première question, question de garantie, oui, ils ne prennent pas notre information – there's a principle that anything that we share, the originator has control over that information. If they want to re-disseminate that information, they would have to check with us. So that's where I was getting in terms of my answer in terms of privacy measures in place. So it's not like we would give them something and then off they go with it and we never know what they do with it. We still collaborate. There's an exchange of information, there's an exchange of understanding in terms of analytics around that information, and ultimately when it leads to end product reporting, we share those, we see those, and there are other measures in place to protect the privacy of a Canadian. So that's the first question.

In terms of your second question --

Question: The first one. The first question, I mean. I didn't quite get simp—if you could simplify the way we --

CSE Official 2: We collect?

Question: -- collect Canadian information. It's too complicated, what you said before.

CSE Official 2: So simply put, I'm not going to – I can't get into the capabilities of how we do – how we do that. I mean --

Question: Legally.

CSE Official 2: Legally?

Question: (Off microphone)

CSE Official 2: The National Defence Act legally mandates us. We're allowed to collect foreign signals intelligence on the global information infrastructure, provided that we're doing so for intelligence – foreign intelligence purposes, so that they meet with the foreign intelligence priorities of the government.

Question: I'd like to ask you, if I may, about the extent to which your protestations that no specific names or identities were revealed is essentially meaningless. It's not a perfect analogy, but for the sake of argument, a policeman has your license plate, he doesn't know your identity but he can find it and prosecute you for running the light. The only reason you collect metadata is so that you can do that. If you give numbers, an IP address, which accessed this site so many times at what frequency on what date, whatever, you haven't revealed a specific name or identity. But the receiving agency in Five Eyes is perfectly capable of doing that. So the whole pretence that you didn't reveal identities is hollow, it seems to me, and I'd like you to comment on that.

Secondly, why do you think – they know what you're saying about oh, well, they have to let us know if they pursue that, if they drill down to the next level and establish the identity. Why the hell would they tell you if they know that it's going to create a problem for you? They're a cooperating agency. They're in the intelligence business. They're not going to create problems by revealing to you, you know, that they are doing what they should not be doing --

CSE Official 2: Right.

Question: -- in Canada, which they're not doing in Canada anyway.

CSE Official 2: Right.

Question: Okay?

CSE Official 2: Okay. So I'll answer your first question, then it'll blend into your second question. Sharing subsets of metadata, you're quite right, I mean, if I – a subset of metadata could be a phone number, could be an IP address, and that could be shared. It would go into a pool of metadata that, if you can imagine how much metadata there is, there needs to be a reason to go looking for that particular number. We have assurances from our Five Eyes partners, much like we do ourselves, that you don't go searching for a Cana—so you wouldn't do a search to say oh, well, let's just see if 613-such-and-such a number is actually in this pool of metadata so that I can do some analytics around that number. They're prohibited from doing that. They have training, they have policies and processes in place. And the limited amount of people that actually have access to this information in our Five Eyes partners cryptologic agencies are limited in what they actually can – they wouldn't be able to target Canadians, or Canadian metadata for that matter. They wouldn't be able to start with that.

However, as you point out, if they're doing analytics on another number and there's a link to a Canadian number, that's where further interest would come up. But then ultimately that would lead to an end product report that, at that point in time, would also minimize the name, the identity of the Canadian. And that report would be shared with us. And if they ever wanted to reveal the identity of that Canadian, they would have to check with us because ultimately it would have been based on information that we would have shared. And that is the policy and provision and process that we have set up, and there's no reason to believe that they're not following their policies and processes and procedures.

Question: So they're a bunch of Pollyannas. They always follow the rules, they never run a red light --

CSE Official 2: Indeed not.

Question: -- (crosstalk) international – biggest regime of international intelligence. It's hard to believe.

CSE Official 2: Well, like we did here, obviously mistakes occur, and that's why we have review bodies that find mistakes and are able – they're able to actually provide recommendations. And unfortunately, the complexity and the nature of global information today and the way that it works, unfortunately you're bound to fall into some of these mistakes. The – because it's ever-changing in its dynamic.

CSE Official 1: We're going to move on. There's a lot of people who have questions, and we've only got about five minutes left and we're gone – we have to go across the street. Go ahead.

Question: Yeah. So I'm interested in – here there's mention that the Commissioner's office, citing a CBC report – I don't mean to do PR for Terry here, but citing a CBC report, goes to CSE and says we're concerned about the details explained in this report, then explains the back-and-forth. The presentation is kind of explained in more thorough detail. The Commissioner concludes that there is no kind of prima facie breach there, that the actual process doesn't seem to be problematic. Can you kind of get into that a little bit and kind of talk to me about how some of these other disclosures from Edward Snowden don't meet the standard of breaching Canadians' privacy rights, especially in regard to the Spencer decision, which you cite in here, given the fact that, you know, CSE doesn't even have the right to kind of grab this information or analyse it from the get-go? How can – how can the Commissioner be satisfied there that this process isn't doing exactly that, when indeed these – the – these Edward Snowden reports say that you're grabbing millions' of Canadians' data, their metadata for sure? Is there a filter there? What is it? Can you give us even just the sketchiest, vaguest explanation of what that process is?

CSE Official 2: Okay. You danced around a few topics there. But at the end of the day, the National Defence Act, again, gives us our mandate to collect information for various purposes, I mean. Our work essentially helps protect lives of deployed Canadian Forces. It does find foreign targets, foreign threats. It does thwart cyber security attacks. So I don't think what you're saying is that there's not a need for us to be doing what it is we're doing.

How do we do it? It's obviously very complex. The legal landscape is changing. That is one of the challenges, certainly. I don't believe we cited Spencer, but certainly I think the Commissioner in his report cited Spencer as well as a couple of other recent legal decisions to state that, you know, communications 20 years ago were very static; now they're dynamic. And so how do you actually go about doing the type of work that we've been mandated to do in that very complex environment? Obviously, the collection of information and the collection of metadata is at issue. The Commissioner makes very clear that we have a mandate to do that.

In the specific example that you cited, our former Chief appeared before a Senate committee and I think spoke very specifically about the activities around that particular – I believe it was called the airport wi-fi deck, something along those lines. The activities there were, again, the Commissioner came back in and thoroughly – I mean, the Commissioner has staff that have engineering backgrounds, IT backgrounds, and indeed have the appropriate TS clearances to be able to come in and sit down and ask any question they would like and pore through exactly what our activities are. And what he's doing is he's making sure that all of those activities are not directed at Canadians, that we're not just willy-nilly collecting information about Canadians, but at the same time, that we actually are doing so for a foreign intelligence purpose to actually achieve some of the things that we're trying to achieve, and that we're mandated to achieve, in our Act.

Question: Okay. Just one follow-up. Can you give us some explanation of, over the course of the year, how things have shifted with the coming into force of both C-44 and C-51, which evidently changed things for you guys?

CSE Official 2: So we weren't specifically involved in either, other than possibly being part of the new SCIZZA (ph) set-up in terms of information sharing. But I don't think it would be appropriate for me to answer questions related to C-44 or C-51, given that we've only got a couple of more minutes. I'd like to focus on this. But I certainly welcome – if you'd submit any questions to us, we'll be happy to respond to those.

CSE Official 1: Over there in the corner. We're kind of coming up against time, so I'll try to get to you. If not, you can address – you can talk to our media relations (crosstalk).

Question: (Diaphonie) Radio-Canada. Je veux juste savoir combien d'autorisations ministérielles sont actives à l'heure actuelle et est-ce que la collecte de métadonnées fait l'objet d'une autorisation spécifique ou est-ce que c'est englobé dans des autorisations plus vastes? Alors combien d'autorisations ministérielles à l'heure actuelle?

CSE Official 2: Je pense que le commissaire dans son rapport mentionne qu'on en a quatre. Il y en a trois qui sont reliés à la collecte d'information au point de vue de – foreign signals intelligence. There's one related to our cyber defence activities. So we have four. The collection and use of metadata is governed by our National Defence Act. There is no specific ministerial authorization related to that because ministerial authorizations are for private communications. Metadata doesn't fall into the category of a private communication.

Question: (Inaudible, hors micro) la collecte de métadonnées, on n'a pas besoin d'avoir la signature du ministre.

CSE Official 2: Non, le —-

Question: Donc quand le ministre dit que c'est – okay.

CSE Official 2: En effet, pour faire la collecte de métadonnées, on a la loi. The National Defence Act gives us – as is clearly stated in the Commissioner's report.

CSE Official 1: Sorry, actually behind you. I (inaudible) this is going to be the last question. All other questions, you can give our office a call.

Question: So am I to understand that you really don't know how many Canadians were impacted, or you don't want to tell us how many Canadians were impacted? And when you say it's been defined as low, could you define low?

CSE Official 2: So the – low means that – can I define low? It's unlikely that there was an actual interest. In terms of whether we don't know, the actual metadata did not point to any one individual. The information on its own was not enough to be able to say that an individual's privacy was compromised. And so as a result, given that, and given the fact that it's just one of several privacy protection measures that failed, so just because that one failed doesn't mean that should – should that particular privacy interest of that particular metadata be of interest at a later point in the end-to-end signals intelligence process, that we would not have had other privacy protection measures in place to make sure that that particular person, if indeed it led to someone, was compromised.

CSE Official 1: Thank you. Thank you.

Question: And if so, why did it take so long --

Question: Yeah, exactly.

Question: -- for the public to find out?

CSE Official 2: So I'll answer that very quickly by saying it happened – we discovered it in 2013, notified the Commissioner of it. It's part of the Commissioner's report. I believe the Commissioner's report was tabled as – or was provided to the Minister of National Defence within the 90 days of the end of the fiscal year. This would have been last fiscal year. And you're finding out because obviously it was tabled today.

(Crosstalk)

Question: But did you stop sharing --

Question: But did your secret – the government kept it secret, then. The Conservative government kept it secret.

CSE Official 1: If you have any other questions, you can call the office. Thank you.

Question: Did you stop sharing then, or when the Minister told you so (inaudible) the report?

Question: Est-ce que ça a été caché? Je veux juste savoir est-ce que ça a été caché?

CSE Official 2: Non, ça a pas été caché.

Question: When was the sharing --

Question: It's rather important.

Question: -- when was the sharing stopped? Can you just say that?

CSE Official 2: At the beginning of 2014.

-30-

NOTE: TRANSCRIPTS CANNOT BE SHARED OR TRANSFERRED OUTSIDE OF YOUR DEPARTMENT WITHOUT THE CONSENT OF MEDIA Q INC.

Questions? Please contact us at PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca.
Questions? Veuillez communiquer avec nous au PS.PSPMediaCentre-CentredesmediasPSP.SP@Canada.ca

Lacroix-Menard, Gabriel (PS/SP)

From: PSPMediaCentre/CentredesmediasPSP (PS/SP)
Sent: Thursday, February 19, 2015 9:33 PM
To: Today's News / Actualités (PS/SP)
Subject: Transcript: Officials discuss "New Cyber Challenges in the 21st Century" - 2015-02-19 - 14h20 EST

DATE/DATE:
February 19, 2015 – 2:20 p.m.

LOCATION/ENDROIT:
Château Laurier, Ottawa, ON

PRINCIPAL(S)/PRINCIPAUX:
Scott Tod, Ontario Provincial Police Deputy Commissioner - Investigations and Organized Crime;
Admiral Mike Rogers, Director, National Security Agency;
Cheri McGuire, Symantec Corporation Vice President of Global Government Affairs and Cybersecurity Policy;
Dr. Oonagh Fitzgerald, CIGI Director of International Law;
General Richard Evraire

SUBJECT/SUJET:
Panel 2: "New Cyber Challenges in the 21st Century" is held on Day One "A Complex and Dangerous Security Environment" of the 2015 Ottawa Conference on Security and Defence, held by the Conference of Defence Associations and the CDA Institute.

General Evraire: Ladies and gentlemen, mesdames et messieurs, welcome back. Thank you again for returning from lunch so promptly. We're ready for our first panel of the afternoon and I'm very much looking forward to this one. This panel is on the new cyber challenges in the 21st century, les nouveaux défis cyber dans la 21e siècle.

I'm very pleased by the way that CIGI, our platinum sponsor, was of great assistance in putting together this panel and so we thank CIGI very much for that. The moderator for today is Dr. Oonagh Fitzgerald who is the Director of International Law and represents our platinum sponsor. Thank you very much for that Oonagh. We're very pleased that you're willing to help us guide through this very important panel which builds upon and really continues the very interesting and very important story that we've been building over the course of the morning and now into the afternoon.

I'm not going to give you the background on all of the panelists but first we do have Deputy Commissioner Scott Tod with us and Cheri McGuire who is from Global Government Affairs and Cybersecurity Policy. We also have our good friend Admiral Mike Rogers, who you heard from and very eloquently just before we came into the room. With that, Dr. Fitzgerald, I hand you the podium.

Dr. Oonagh Fitzgerald: Thank you very much General. Good afternoon everybody. It's a great pleasure to be here and CIGI is the Centre for International Governance and Innovation is really pleased to be involved in this event. I am delighted to have this wonderful panel to moderate. As you already will know, this will be a very interesting discussion.

Just a little bit of background on CIGI before I introduce my speakers in more detail. There is a real interest in cyber at CIGI right now. There is a global commission on internet governance that has been in existence for over a year now and it's a joint project with Chatham House (ph) which is the British think tank.

We've the Canadian think tank CIGI and Chatham House working on this wonderful commission on global governance with 29 international commissioners from various professional backgrounds and 35 member researchers in an advisory network.

The global commission is chaired by Swedish Prime Minister Carl Bildt and co-chaired by Fen Ove Hansen (ph) who many of you will know. The commission is conducting and supporting independent research on many internet related dimensions of global public policy. There will be a major report issued in 2016.

If you want to learn more about it please don't hesitate to go to the website. You can find it at www.ourinternet.org. At CIGI we're also very interested in innovation questions related to the internet, so any kind of innovation that has an impact on the internet. A discussion about cyber threats and cyber challenges is obviously very dear to our heart.

I would say in a somewhat dystopian manner that a few years ago analogies to George Orwell's 1984 would give shudders to citizens and politicians alike but the climate has changed somewhat in recent years. Today we may be post Orwellian in that we're dealing with both benefits and risks of internet connectedness and we're trying to find the perfect balance.

At the same time as the government is developing the powers and th capabilities to be all-0seeing and all-knowing, the private sector is not far behind. In some cases they've even be leading and is in a position to give us answers to questions we haven't even asked yet and offer services we don't even know we need. Many interesting questions come up about privacy and the individual in this environment.

How do we protect that and we certainly heard there are many policy issues to discuss today. The threats of interconnectedness continue to grow for governments, corporations and individuals and with the threats grows the need of national defence, law enforcement and the private security services to be ahead of the risks.

This discussion should help look at some of those issues. Our illustrious panel will talk about the evolving cyber threat picture and the roles and responsibilities of public and private actors in addressing these issues in ways that comport with our societal values, so no small task and they only have an hour to do it in. Admiral Rogers has been ably introduced to you so I won't spend more time introducing him.

We are absolutely delighted that he has joined us for this panel and I will introduce Cheri McGuire beside him. She is the vice president global government affairs and cyber security policy at Symantec Corporation. She has more than 20 years of government and industry experience and she leads Symantec's global public policy agenda and government engagement strategy that include cyber security, critical infrastructure protection and privacy.

She also served on the World Economic Forum global agenda council on cyber security and she is involved with an initiative that was described to us earlier by Admiral Rogers involving the National Cyber Security Alliance, the US IT Sector Coordinating Council. She's involved in one of the 16 critical sectors identified by the President and the Department of Homeland Security with the government on these issues and cyber security, privacy and cyber security.

She has a background at the Department of Homeland Security and with private sector corporations such as Lewis Allan (ph). Finally I'd like to introduce you to Deputy Commissioner Scott Tod who is Deputy Commissioner for investigations and organized crime Ontario Provincial Police. Yes, he's a police officer but he does have a military background so give him a chance.

What we're going to talk about today is we're going to talk about the criminal prosecution aspects, the private sector aspects and the national security aspects of cyber, a little bit more about Deputy Commissioner Tod. He oversees specialized law enforcement services and criminal investigations including organized crime, intelligence, behavioural sciences, anti-terrorism, electronic crime and drug enforcement for the large deployed police service in Ontario.

He's a member of the Ontario Association of Chiefs of Police, the Canadian Association of Chiefs of Police, the International Association of Chiefs of Police and the International Association of Financial Crime Investigators. That goes to that issue of partnership that's so important. Deputy Commissioner Tod is a graduate of the leadership and counter-terrorism program and received his diploma from the Canadian Forces College, Canadian Security Studies program.

He's a former officer of the Canadian Forces, Maritime Command. In 2008 Deputy Commissioner Tod attended the Governor General's Canadian leadership conference. These are our speakers. We decided for the purpose of this presentation we would first start off with comments by Cheri and Scott regarding the remarks that we heard from Admiral Rogers. Admiral Rogers gave a wonderful overview to us of the challenges that he sees sitting at the head of US Cyber Command from a national security perspective.

He touched on a number of very important issues around national security, national defence, international cooperation, even diplomacy. Some of the other issues that came out through questions are things like fragmentation, democratic oversight, privacy. We really set up the panel to have a broader discussion. What we'd like to know is what is the perspective from law enforcement and from the private sector about the challenges in cyber at this point in time.

Scott Tod: I'd like to speak about the three areas of strategic, operational and tactical challenges that we have today from a law enforcement perspective. I'll couch my comments in the fact that it's based on my experience in law enforcement and that the relationships that we share with our partners both in security and within military.

On the strategic level one of the concerns that I have within the aspect of cyber and dealing with cybercrime and I'll separate strategy, cyber strategy for cybercrime. I'll try to focus my comments towards cybercrime is in regards to the whole discussion that's occurring in the police leadership area of policing our communities in Canada.

In Ontario there's much discussion going on currently and it's happening across Canada too at the senior levels of law enforcement in regards to cost of policing, the sustainability and costs of policing. Similar comments I heard certainly on a much grander level with regards to the military commands in Canada and the United States but certainly the cost of policing and that we're trying to bend the cost curve of policing.

For comparison our budget is about 82% driven by HR, the cost of our members to come to work. 18% is operational and capital. That doesn't leave a lot of room in regards to responding strategically to the speed and the size of cybercrime. At a strategic level that discussion right now is focused on mobilization and engagement strategies in our communities. These are isolated strategies that we hope collectively will make Canada a safer place to live.

They focused around the criminal factors of homelessness, poverty, addictions and mental health, not cyber-crime and terrorism. We're hoping that by identifying those criminal factors that we can make our communities and its' generally done in isolation that we can make them safer by working with community partners. I think the success for us in the police community is in law enforcement is to make that hub environment a national discussion, a convergence of all the people that have some space within the cyber sphere.

That's the strategic level. There's a need for a national discussion by law enforcement and our security partners and also government. The second one, the operational level, is to define the jurisdictional boundaries in which we work as law enforcement. Where does each law enforcement agency respond? Our legislation allows for police services to be created in Canada. The Police Services Act of Ontario was rewritten in 1990 but it's along the jurisdictional boundaries which regions, cities, municipalities and provinces are located.

We heard this morning that the jurisdiction part of cybercrime is not a good way to attack cybercrime. The aspect is the operational level. We need to identify leadership within the space of cybercrime and we need to identify how we attack it whether it's through a regional effort or through national programs.

I have seen national programs that are successful, the national sexual exploitation centre run by the RCMP in Ottawa is a typical example of how a national approach run by the RCMP in Ottawa is a typical example of how a national approach working together with municipal and regional law enforcement providing leadership and direction provides a great success with regards to attacking people who are trafficking in child sexual exploitation.

That's one example of operational that can be successful. I think at the operational level it's the idea is better collaboration amongst leadership and the operations that support the investigations or the intelligence behind cybercrime. Purely at the tactical level, one of the things I talk about is data size. Data size today is extremely significant to us. Unlike some of the security partners that we work with, we're required to store large volumes of data.

I hope to give you an example of that during an example of an investigation I have but storing that data for long periods of time and accumulating it and retaining it perhaps for up to 35 years in regards to archival innovation is really the issue we're dealing with and the forensic ability to look into that duty and use it for the purpose of criminal prosecutions.

The criminal space that we operate in is challenged by data size. The next one is changing technologies, the rapid pace of changing technologies, keeping up with the most recent cellular devices, the ability to archive, the ability to encrypt files and the ability to do all that from a law enforcement perspective and investigation to identify criminals is really challenging.

The last one is the jurisdiction outside of where we operate either municipally, provincially or federally but outside the country of Canada and working to find criminals that are exploiting Canadians at home and abroad but through a law enforcement effort and working with our international partners. We rely on the RCMP and at times the military to work in other countries, to assist us in providing information in regards to cybercrime. I think those are the significant challenges that I see for law enforcement today.

Cheri McGuire: From a private sector standpoint, thank you Admiral Rogers for teeing up so many juicy issues for us to touch on, on the panel today. We are clearly at the nexus in the private sector between government actions and the criminal actions. Sometimes we get caught in the middle.

This is one of the reasons that information sharing is so important. It's been difficult to talk about information sharing in the last two years in the post Snowden environment because the issues have become so inflated between must have privacy over all else or we must have security over all else.

Our position has long been that we need to find the right balance between the two because we cannot have privacy without security in today's data driven world. This notion of information sharing is important. It is a tool in the toolkit to go after the bad guys, to prevent attacks and to protect ourselves more effectively but it is not the sole silver bullet that's going to change the world and fix the issue of cybersecurity today.

What I would say is on the information sharing front many companies including Symantec have been doing this for many years, sharing with our law enforcement partners, sharing with our private sector partners, sharing with national certs (ph) and governments around the world.

What we need to do now is to accelerate that so more organizations can take advantage of the good information that will help protect themselves more effectively in the future. Last Friday at Stanford University in California President Obama was there. He signed a new executive order on information sharing to help promote the development of information sharing and analysis organizations.

There are many that exist today but again this is to try to accelerate and incentivize the development of more of these organizations. They are not just solely US based. Many of them have an international component where they have international based companies that are also members.

This is an area that's very much at the forefront of the cybersecurity discussion today. How do we share the information, minimize the PII and ensure that our customer information is protected, that our proprietary information is protected if we do share and also what are the legal protections whether it be liability protection or other types of legal protection that companies will be able to gain if they do share information.

All of these are very complex policy issues but I do think a big step was taken last week in California by the President to try to move forward. In the US in particular we have some things that the President cannot do within his authority. The Congress has to take action. There's complementary legislation being proposed on information sharing and how to promote that while also providing the safeguards around privacy, one of the many issues that we're faced with today.

Admiral Rogers: There is no silver bullet here. There is no single technology that will fix this problem. There is no single legal structure that will fix this problem. There is no single organization that has the intellectual answer to all of this. I'm always trying to remind people, this will be a series of steps that we're going to take that when taken together can produce a greater whole.

The idea that one single thing is going to solve the cyber challenges we face I find that is a non-starter. The second point is most people tend to default to technology as the biggest challenge when it comes to cybercrime. My experience is quite different. It isn't the technology. It's the cultural issues about how do we move beyond the technicalities to get to a place where we're comfortable.

Lots of people have pretty limited technical knowledge and some have very high. We've got to do this in a way that technology isn't a bar that stops us from being able to address it. We've got to do this in a way that our broad society can understand and can deal with. It's not just about technology. I say that leading two organizations the prism they tend to look at the world through is we're a technically focused organization applying technology to overcome technical challenges. Guys, it is much more than this technology.

Dr. Oonagh Fitzgerald: You've already raised an issue, this question of policy that is extremely complex even though we have a very illustrious panel here. It is a societal problem. It involves the President of the United States. It involves government in Canada, big issues for society to work through.

Maybe we can get to a more operational question. Could you talk a little bit about the dividing line between cybercrime and cyber defence and the convergence between criminal law enforcement and cyber defence.

Scott Tod: I think the issues, I mentioned in my opening comments, I like to distinguish between cybercrime and cyber security. I see it as two hills. On one side the cyber security part as incorporating government, private industry réponse. On the other side I see cybercrime as being a government, law enforcement response. Through the middle there runs that valley in regards to that's where we collaborate together. I hope some days it converges rather than collision.

That is a space where we have to become better at working in and understanding our clarity of responsibilities on both sides. Cybercrime is slowly morphing into a cyber-security discussion. The problem is at the operational tactical level that causes confusion among the employees, our workers, our investigators, our online presence. It causes an issue with regards to what is their role and mandate and mission.

I speak to that whole aspect of the OPP will do whatever is lawful, morally and ethically correct to do in pursuit of its goals. Often people are colliding in regards to what is my role as an investigator, as an analyst, as an online presence for example. We have to do some training and development. The OPP is currently undergoing a cybercrime review. We are looking at our organization across all the silos, where is the footprint for each part of our organization within a cybercrime review in regards to providing the best technology, training, and providing assets in order for us to be successful at combating cybercrime.

It also leads into a bigger discussion of working with the premier organization in law enforcement in Canada, the RCMP, looking at their recently released strategic direction in regards to cybercrime. I think understanding the clarity of role is very important and developing that forensic capacity. The size and speed of data is really concerning to us. At a recent conference I talked about non-traditional forms of data storage, devices we can put in our home to run our furnaces, the ability to store data within the car and the ability of monitoring blue tooth connections, radio stations that you listen to all through the in car computer system.
I think the whole aspect around what are we seized with and why are we looking at it. The last part is how do we analyze it, keeping up with all the devices on the market today and the ability for storage in many places is really challenging a large police service in order to have the facilities to strip data out of those devices.

The next one is fostering partnerships. I talked about those two hills and that valley. I think what it is, is we need to move the hills together, whether it's an earthquake that happens but they need to collide more together in regards to convergence of our roles and responsibilities. I'm looking at is there a role for regulation? Outside of law enforcement is there a better form of regulation that can occur in regards to helping with cybercrime and cybersecurity.

Admiral Rogers: For us on the US side it generally starts with an initial determination, is the activity we're responding to an offensive act or an act of war or is it a criminal issue. If you take a look at Sony as a good example, the first question we were trying to come to grips with is how would we define what we're dealing with.

If you do it as an act of war, traditionally we'd turn to the Department of Defence and say in your role of defending the nation we would expect you to be the lead. In this case for Sony we came to the conclusion it was a criminal act and the Federal Bureau of Investigation was designated as the lead organization.

We treated it as a law enforcement issue because particularly in my NSA hat we have strong partnerships across the federal government. It is becoming quite routine now for some of the largest events that we're dealing with as a nation where the FBI will take the lead as a criminal law enforcement issue but then will come to us and say I need to harness some of the capabilities you have. Can you help us on the data analytics side?

Can you help us in terms of your ability to write counter measures that defeat the software? We've been able to create some great partnerships. We do a lot of work with the Federal Bureau of Investigation. It's a sad comment about the amount of activity collectively we're dealing with that this interaction is very routine. We have standing protocols in place now. It doesn't have to go to a director level. We've got enough of a legal framework where our teams can do what they need to do. That's worked out very, very well.

Cheri McGuire: Maybe I can talk briefly about the work we're doing in the private sector with law enforcement. As you can imagine, the largest security firm in the world but also the largest operator of the largest commercial cyber threat intelligence network, we have a lot of very rich data that we see around the world.

From that we've been able to forge some very strong and productive partnerships with the FBI, with Europol, the European cybercrime centre, and other law enforcement agencies to really go after some of the cybercriminal element that we are seeing today. Some of the biggest and well known cases have been some major botnet takedowns over the last several years. One of the most successful of those was last June with the takedown of the zero access crypto locker bot networks.

That was developed and done in partnership by more than 30 international organizations – law enforcement, academia, private sector, all working together to not only identify the command and control servers but then to sync them and take the botnet off line, very, very successful partnership, first time it had been done with that many partners and beyond simply bilateral engagement between for example the FBI and several private sector entities.

These are the kinds of things we are doing today that are very successful in helping reduce the level of cybercrime, the attacks that are happening across the internet. We need to do more of that. We need to be more aggressive. I'm sure Scott would agree, Admiral Rogers. If we do not have strong deterrents today the cybercriminals and the elements out there that are taking advantage of the internet and frankly it's big business and it's good business for them.

If we are not creating deterrents between private sector, law enforcement and governments in order to deter them as well as putting into place the legal frameworks to prosecute them, extradite them across international borders because cybersecurity is without borders. Today we have a lot of challenges in our ability to do that quickly. The multilateral process today is very slow. It's very cumbersome.

It needs to be modernized to deal with the challenges in real time that we face today. Those are some of the things we need to do in addition to making sure we have strong penalties. I was happy to see a significant hacker yesterday, there was an agreement with the US Justice Department, criminal prosecution. He'll be going away for 7 to 10 years. It's a very significant signal but it's a small step. We need to broaden that and make those penalties a lot stronger and more uniform around the world.

Dr. Oonagh Fitzgerald: Let's delve even further into the operational side. I believe that Scott has a scenario, a typical law enforcement case study that our panel can comment on. He's going to outline that law enforcement case study and then we'll get people's views about how this works. How do you address the challenge?

Scott Tod: As I talked about the size of data nand the speed of data it leads to the point of how big does data get. We talk about Cloud computing environments but eventually the Cloud has a data drop somewhere. It generally goes into a web hosting or file server.

An investigation that's ongoing right now and I'll be vague on the who and the where but I'll talk about the what. It involves a police service coming to the assistance of the Ontario Provincial Police, our child sexual exploitation unit and assisting with locating information for child sexual exploitation.

Traditionally law enforcement is funded for what's called peer to peer contact where it's an officer pretending to be a young child behind a computer, interacting with the person on the other side who is either asking for or sharing child sexual exploitation material. It's peer to peer contact. What we find during these peer to peer investigations that there are thousands of other IP addresses attached to each computer.

In this particular investigation when we commenced the investigation assisting the police service we ended up in a file service and it was owned by a web hosting company, two different companies. We're involved in the acquisition of 1,250 terabytes of information. That's not a lot of data for many of you but for a police service it's a lot of data.

For Admiral Rogers I understand the Library of Congress has about 525 terabytes of information. That was just relayed to me by Blackberry earlier on as an example of what 1,250 could compare to. The idea of 1,250 terabytes we have to secure the storage and then mirror that image. We're up to 2,500 terabytes of information. In order to do that we need further analysis.

We have a large amount of information that requires storage for retention periods too. We ended up having to search for what device is out there and we turned to the military. The military is well experienced in battle campaigns from having something called a portable optimization device, a data server itself, a warehouse of information that can provide communication and storage.

We purchased the pod for a large amount of money and the data now resides on that but within the data itself after looking at 1% of the data we literally had hundreds of people who we suspected of trading in child pornography. It required a further look in regards to how does this work rather than the peer to peer, one to one, we now want to look at corporations. How do corporations profit and benefit from the trading of child sexual exploitation?

That's what we're looking at now in regards to that but to do that you require vast amounts of storage space and you require analysis tools that you can purchase but you also require the technical skill of individuals. Although we hired a young, well trained, competent brilliant people we have at this location relied on bringing back a retired member, one of the original forensic crime individuals we had in the organization who understood the hunting concept in regards to data and not just the searching and analytical part.

Hunting through data is completely different. Now we're at the part of the investigation where we're working with over 100 countries around the world. We're looking at over 1.4 petabytes of information and try to sort through it and identify

suspects around the world. 1.5 million RAR files. RAR is a way of compressing and securing a file of which many are password protected.

We have user accounts, 2,200 user accounts in the United States, 843 in Germany, 534 in Japan, 457 in Russia, 394 in Canada, 380 in the UK, 374 in France for a total of over 7,500 IP addresses that have been trading in what we believe is child sexual exploitation.

A lot of this is uncorroborated at this time. This is an early indication of how big this file is but it speaks to that whole aspect of big data and how do you manage big data as a law enforcement agency not traditionally funded and not traditionally mandated through jurisdiction and legislation to do this. We're lucky enough as an organization. We have by military standards a rather small organization, 9,500 members and a billion dollar budget but the ability to do investigations like this challenges both our human resources, technical capacity and also our budget.

This is a long term investigation. This investigation won't be over in one year, six months. It won't be over within the mandate of the government. It's a long term investigation. Our goal and the importance of this investigation is to look at the money behind the organization. Who makes decisions so profits can be made in a criminal manner? Where do they reside? Who are they?

That leads to jurisdictions in almost 100 countries. It really has been challenging to us. The other part that challenges us is the ability to password crack. Although our security services have great tools we have to create a tool ourselves. The speed of our cracks now is 500,000 cracks per second. I don't know if that's good or bad. We're finding that's the best we can do with the resources we have with the technology today.

I don't think our technology is any more significantly different than what our security partners use. We have over 2,700 high level domains and more than 50,000 lower level domains that we're looking at around the world. That's thousands of end users that are receiving child sexual exploitation material.

I kept this one very close in regards to child sexual exploitation material but I also believe the same is going on in the financial side, there's also servers and environments in which people are profiting criminally by sharing information such as data briefs, personal identification and other things. This is just one investigation that we were asked to assist on which we have taken a different tack with the operational response.

Rather than looking one to one we're now looking at the thousands if not tens of thousands of people but more importantly the corporate mindset. Some of the money figures that we believe right now is $18 million over a three month period that's spent across the file servers. How much of it is legitimate? We're not sure but the money is significant. The efforts are significant. We think it's a large investigation that will take a large amount of time to complete.

Dr. Oonagh Fitzgerald: Would you like to comment on what that kind of a criminal investigation would mean for your organization? How you might be participating and helping?

Cheri McGuire: Through various partnerships we have we are able to look in our big data platform for the kinds of things that that investigation might be looking at. The challenge we have though is we have to make very clear distinction between actively going into our networks and looking for criminal activity because we have to have a level of trust with our customer base.

That doesn't absolve us but it does mean that when we start to see things that look like criminal activity, then we do have a responsibility to report them and to participate in these kinds of investigations. That's where much of the work we do today and the botnet eradication and other kinds of cybercrime, the work we do today, much of that focus is through our deep analytics and the research of our big data platform.

We do see so much threat intelligence on a real time daily hourly by the second basis. Much of what we see is automated. Much of what gets taken care of is automated. When things don't appear to be normal, that's what triggers our deeper analytics. We have over 500 research scientists that just do deep analytics on different types of malware and those kinds of threats.

There's opportunities to work together with law enforcement clearly but there's also a component of that which is directly related to the protection we offer to our customers be they consumers, corporations, academia and governments. They do span all of those.

Dr. Oonagh Fitzgerald: Scott has really pointed out the mouse and the elephant scenario of the specialist in security versus the police. The police used to be walking the beat on the street. Now they have to deal with these huge

challenges. Are you seeing more and more that national security, NSA are being brought into criminal investigations because they're so difficult for the police.

Admiral Mike Rogers: I think the trend we've observed on the US side I would say over the course of the last six months is that less traditional criminal activity in terms of child exploitation for example, although occasionally we'll get queries about analytic capabilities to help us from a capacity standpoint.

The more common scenario we're finding these days is major penetrations into US corporate structures, theft of large amounts of PII data, intellectual property theft, trying to work with law enforcement and identify what was the initial penetration, how did they get in.

What exactly did they take? Did they continue to have a presence on the network right now? Increasingly we find ourselves asked to provide capacity to try to help. It's been a big change for us in the last six months which is not an insignificant challenge from a resource perspective as I'm trying to walk a balance between NSA's primary national security missions and our mission of supporting the rest of our government partners.

Dr. Oonagh Fitzgerald: This raises the question of what are the different roles that government, the police and business and citizens can play in addressing the challenges of cybercrime, cyber-defence.

Cheri McGuire: There's a really bad echo up here. It's hard to hear you. If you could say it again, I'm sorry.

Dr. Oonagh Fitzgerald: My question is about the different roles of government, the police, the business community and citizens in addressing these challenges of cybercrime and cybersecurity.

Cheri McGuire: A very common thing, we all have a shared responsibility in dealing with cybersecurity, cybercrime. Everyone has a role to play in this but that's pretty straightforward, - companies, governments, individuals. However, beyond that we all need to work on developing and building a culture of cybersecurity within our own daily lives, within our organizations that we work for.

We see great disparity in different organizations depending on what roles and functions within companies or government agencies. What I mean by that is the level of awareness can be quite broad. I'll even say that even inside of Symantec which is a security company we have different levels of awareness as well because folks who have traditionally focused on finance and the running of the business functions may not have the same perspective that our technical security engineers would.

That doesn't mean they don't have a role to play. Everyone has a role to play. We have to make sure that level of awareness is there. I always say we leave our house every morning and we lock our door to protect our valuables. We need to start having the same mindset about how we treat our data. We need to do that across all devices and all platforms.

We've done some interesting surveys on mobile device usage and the level of awareness around security that is out there. About 70% of individuals today know about using strong passwords, making sure they have security software, updating their systems, basic cyber hygiene.

If you ask those same individuals about whether or not they should be doing those same things on their mobile devices, 30% are aware they should be doing that. Everyone uses a mobile device today. They're always connected, always online. You think about the additional vulnerability, the additional ways that allows attackers to try to break into your system to steal your data, to create many of these data breaches we're hearing about almost on a daily basis. Again, it's incumbent that we really do build that culture of cybersecurity and that it starts early in the schools and continues on.

Admiral Rogers: I would echo that thought. I try to remind, in the Department of Defence I try to remind our workforce cyber is the one mission set in which if we had given you access to a keyboard you are now both a potential opportunity of advantage but perhaps more significantly you are now a potential point of vulnerability.

We have given everyone access to a keyboard. As you heard depending on what source you want to use, my experience is 70%, 80% of most of the challenges I deal with inherently started with bad organizational choices. What led you to do that? Why would you click on that? Why would you be opening material from users you have no relationship with, you don't recognize?

Guys, this is not going to work. Everybody is a potential point of vulnerability. Your network is only as strong as the weakest link. This isn't about technology. It's about culture. The biggest challenge is changing culture. It's not the

technical piece. We can make technology as easy as we can but if we don't intellectualize it up here about how this impacts me and what I have to do as an individual to engage in cyber hygiene and sound practices, the greatest technology in the world is defeated like that.

It's not either/or. Just more broadly I think increasingly the key to success in the cyber domain is how to recreate partnerships, whether it be law enforcement, whether it be expertise, whether it be the role of the government and its capability. How do we bring this all together? How do we do it in an integrated way in a framework that we're all comfortable with. That is not an insignificant challenge in the world we're living in right now.

It's particularly challenging in representational democracies like the United States and Canada. We're always concerned about what's a private function and what's a public function, what are the implications for us as citizens, are we comfortable with that. I think the reality is we have to blur those lines to some extent but we've got to do it in a very public and direct way so people understand what we're doing and why and also what we are not doing. Half the things I see quite frankly are credited to one of the organizations I run, I scratch my head and go I'm not even sure that's technically possible but I still read about it.

Scott Tod: One of the issues in regards to governance and this would be an internal issue is regards to procurement and supply chain management and getting the best tools we have to the market as quickly as possible and regulation within government and understanding procurement and supply chains. Really at times there's a barrier to the speed at which cybercrime moves. The ability to acquisition the right device, the right course of training, the right piece of information we need from another company, an independent company.

The whole aspect in regards to procurement is one thing that needs to be looked at in a different light at times by government. The other one is in regards to the whole aspect of the unknown jurisdictional issues. A video of a crime that occurs in Canada is uploaded in Japan. Accessing that video and getting the video, getting it back to Canada to be used in a prosecution. How is it stored? How did it arrive in Japan? How as it stored in Japan? How was it retrieved from Japan? There's always the whole aspect of jurisdiction is how many people do we need to involve in that process, the mutual legal assistance process we have to involve lawfully in regards to repatriating evidence back into Canada.

On the case scenario I talked about one of the things we're doing is providing information sharing agreements with the Department of Homeland Security to have direct access to data that belongs to American citizens. That effort working with prosecution was a large collaboration amongst many partners to get there. There's something providing another foreign entity, a security partner for sure but a foreign entity direct access into data with a specific information agreement for American citizens or people who targeted American citizens.

I think that's something challenging the legislation we have on the books in regards to the Criminal Code and others that we're lawfully required to abide by. I think that aspect of renewing and looking at the jurisdictional boundaries and defining who is responsible for cybercrime investigations in Canada. If it's everyone then recognize it. If it's one individual organization such as the RCMP or a combination of large major law enforcement organizations recognize it. We have a great cyber strategy. We don't have a great cyber plan in regards to how do we attack cybercrime in Canada.

Dr. Oonagh Fitzgerald: We've heard a lot about the challenges of speed in procurement, speed in getting extradition to work. We've heard about the legal frameworks, dealing with the digital world. There's gaps. You've all identified the need for this collaboration and it's a high risk collaboration as you've all pointed out. You all have separate spheres of responsibility. You don't want to intermix too much unless you've got a clear framework.

Tell me about some of the governance challenges you're dealing with given that you are dealing with these outdated laws that are limited by jurisdiction as the Deputy Commissioner was saying, limited to Ontario or Canada or the US. How do you deal with these government challenges?

Scott Tod: I think one thing forums such as this are very important. I think the aspect of touching a warm hand and having a discussion, this is a great start to recognizing the leadership that's required on the issues of cybersecurity and cybercrime. The last six months have developed with incredible speed in regards to terrorism within Canada and cybercrime, cybersecurity in Canada.

The speed of discussion has never happened this quickly in my 33 years than it has in the last six months. What I'm concerned about is who steps forward in the leadership role to lead that discussion and continue the discussion with some long term solutions that need to happen. I think that's very important.

There's a lot of people that want to jump on the boat right now. It's leaving. It's moving fast and they want to be on the boat. They want to drive the board. What we really need is the leadership to step forward that can continue this discussion and have the effect and results we need to have to be successful.

Cheri McGuire: I can talk a little about some of the governance challenges of the private public partnership in the United States. There are 16 critical sectors that you've heard about. The structure by which those industry councils and government councils can come together and meet on a regular legal basis had some legal barriers they had to overcome when the initial idea was hatched back in 2004/2005.

We have a law in the United States called the federal advisory committee act and that means that if industry meets a group larger than 8 or 9 in industry meets more than one time on a regular basis with a government entity it must be open to the public and must be transparent. You can imagine when we started talking about critical infrastructure protection, how are we going to share information, how are we going to talk about these hard issues around physical security and cybersecurity in a safe way so companies didn't feel like they potentially would be exposing vulnerability in a public environment.

That had to be constructed in a way that it provided trust as well as the legal foundation by which they could legally meet regularly. That took a lot of time both from the government and industry side to get that worked out. Once it was worked around 2006 those councils began to be able to meet on a regular basis. What we have today is a pretty good structure by which we can communicate, by which we can have the hard conversations but the level of maturation is at different stages depending on which sector you look at.

Financial services is very mature, telecommunications is very mature but at the same time some of the others are taking a little longer .They didn't have as much focus on the cybersecurity area so there was a lot of time that needed to be taken to build the awareness. The foundation of all of this happening has to be trust. It has to be transparency. It has to be a true partnership. It doesn't work very well if you come into a meeting and your industry and your government says industry you shall do X,Y and Z.

This truly is supposed to be collaborative and informative on how we can best protect together the critical infrastructure. Those are some of the foundational elements that I've seen when I was in the government and outside the government sitting on the partnership on both sides.

Admiral Rogers: I think on the US side we have a broad consensus on different roles, who's going to do what. We've got a broad structure for how we're going to implement it. I wouldn't have said that two years ago but I feel much better about it now. The biggest challenge is we've got to move beyond a discussion about who's going to do what to how are we going to do this.

That to me is the next immediate challenge for us. We've got to get down to the execution level about how are we going to do this, using what means, what should the private sector expect from the government. What do I need from the private sector in order to maximize the capabilities we bring to this. What are the paths we're going to use to communicate? What are the data elements we need to share? We can just inundate each other with data.

That doesn't generate value and outcomes. Roll up our sleeves and getting into the how, as I talk to my counterparts to say this is what I really think we need to do. We need to make this easier for the private sector. If you're on the outside looking in at the federal government I still think we're very complicated and it's very difficult at times to understand who should I go see. How is this going to work? We've got to get beyond the who and the what into the how. That's a big challenge for us.

Dr. Oonagh Fitzgerald: In terms of new technology we are hearing about the role of artificial intelligence, unbreakable encryption, new challenges heading towards us quickly. Can you tell me, this is the last question, what do you see as the big challenges looking into the future and how do you think your community, your organizations can contribute to addressing these new challenges. The hope here is we can end with a positive message.

Admiral Rogers: The positive message I can argue is I think the one thing we all have in common is we've got highly motivated men and women who are willing to work hard and bring a lot of expertise and a lot of focus and conviction to the challenge. That's the best thing we've got going for us. It's not our technology. It's our people. It's the power of their intellect and the power of their heart that drives this.

My experience in the military is cyber is no different than any other mission. It's the men and women that really make the difference. That's the real positive. In terms of the challenges, I worry increasingly nation states turning to other groups

as a vehicle to disassociate themselves from attribution, as a way to attempt to obscure their activities. I worry about the challenges in the mobile device arena. As you heard that's where the growth is.

Just look at the market. Look at what's being sold. Look at how much it's integrated in our day to day lives whether that be as individuals or at work, the handheld digital recorder. The encryption piece although again I remind people if it was created by man it can be defeated by man. If we think there's some technology out there that guarantees history would suggest to me I don't believe it.

I don't think there's a single technology that's going to guarantee it. Those are probably the three biggest. I think the challenge in some ways at a macro level on the defensive side as a final thought, most defensive strategies both in the public sector and the private sector are generally built around recognition of activity based on prior knowledge.

We've seen this before so we know what it's like. That is not a long term model for success because it assumes a high level of knowledge and insight. My view is that's not a great defensive strategy. We've got to come up with defensive strategies that are not predicated on advance knowledge and recognition of the activity we're looking at.

Cheri McGuire: I think the biggest challenge I would say IOT. This great innovation we're seeing, the internet of things, they're amazing. Things we're going to be able to do today that we couldn't do even three years ago with technology and where we're going over the next several years is really truly amazing, the pace of innovation.

At the same time, most of that innovation is happening without an eye towards security and so when you think about the proliferation of devices that will open up traditional vectors for vulnerability with IOT, that's a pretty scary place in the future. We've got to be focusing on the internet of things and that whole next generation of technology so we're building the security in at the beginning rather than trying to bolt it on afterwards.

History has shown us that trying to bolt it on afterwards is not very effective. Essentially that's very much what we are trying to do today. On the positive side I think the amount of energy and the amount of focus and attention this issue is getting today is something that even four years ago we did not see.

I'll mention the summit I was at on Friday at Stanford again. It was amazing to see all of the CEO's of Fortune 500 companies that were in attendance who were talking about the security of their corporate networks, the protection of their customer data and their intellectual property. Truly speaking with deep knowledge about how important this was they make sure they protected their crown jewels and their viability and maintaining the trust of their customers.

I think the level of awareness at the highest levels now is greater than it has ever been. I see that at the corporate level, at the government levels around the world as national cyber strategies are being developed everywhere, national cyber plans are being developed by governments around the world, by the cooperation happening between different governments to build cyber capacity for those nations who maybe are not as mature.

There's a lot of very positive energy that's taking place and action that is taking place to try to raise the bar for everyone. That's something I think creates an environment where there is some hope that we can tackle this problem and make a difference going forward.

Scott Tod: One of the things I'll talk about is the trust factor, trusting our partners. An example would be the organizations independent corporations that we want to perhaps sign service level agreements with to provide services to law enforcement to do certain things.

One of them may be data collection, data storage, analysis, the aspect of analysis of the information, providing the reports. Those are things we need to look at. Speed and size are what's problematic for us. I think better collaboration with government, with corporations and educational institutions, leveraging the power they have.

I think that's the success, that's the short term success. I think the long term one is the education of the citizens of Canada and the politicians of Canada as to the extent of what this problem is, how far reaching it is and what the solutions are.

Dr. Oonagh Fitzgerald: Thank you very much for all your wonderful comments. I'm relieved to know that at the center of it all the human being still remains in charge and the possibility of human collaboration and working through complex issues is the real future here which is a great relief for somebody like me who doesn't have the math background of Admiral Rogers.

I know that one of our speakers has to go to the media so if there's one very pressing question we could take it but we can't do that many. If somebody wants to have a quick question.

Question: Thanks for an excellent panel discussion for something that's extremely complex and difficult. I wanted to get any of the panel members to discuss the culture change. That was something the Admiral touched on and all of you have discussed, the ability to create a new understanding of what it takes to defend against a threat that is so broad. Adaptability and speed is the issue.

In Canada we're trying to build an anti-terrorism policy and push that through. Bill C51 you're probably familiar with and a lot of the discussions are about invasive acts by government departments. It really is about information sharing and getting to that point where the government agencies responsible for a particular aspect can respond quickly enough to detect and respond to those cyber threats.

I'm wondering how, it's too bad that the two Senators aren't here because they're fighting that problem in the House right now. What would you see as being an enabler for the professional community, for us to do in terms of beyond passwords. What recommendation would you have to answer those people who have concerns about privacy, not the commercial or industrial side but the public?

Cheri McGuire: I would say first go talk to them because you have to have that open dialogue and have the conversation. I think you might find you're really not as far apart as it might appear. Once many folks that are privacy advocates see the type of information we're talking about sharing, it doesn't have PII, it doesn't have proprietary information.

It truly is meta data. It's zeroes and ones that is machine readable. Many of them say I get it. You're not going to sway all of them but I think it's important that you have that dialogue and you proactively reach out to them. We'll never be able to bridge the divide if we don't have that open dialogue.

Admiral Rogers: The other point I'd try to make is you must own this problem. If you think this is something your CIO or your chief technical officer or in military jargon your six is going to own, that ain't going to work in the digital world of the 21st century. You've got to own this just as if you're a fan of history, if you've read anything from General Marshall in the Second World War on the US side, he always talked about how logistics were one of the things from his perspective that he thought separated the true professional who could look at the strategic level from the traditional commander.

My argument with the leadership in this thing we call the Department of Defence down to individual unit commanders is you must own this problem and you must have a fundamental level of knowledge on this. It doesn't mean you're the expert but you don't understand as a naval officer, you don't understand every system that's on that ship but you understand the fundamentals of propulsion. You know the fundamentals of your plant. If there's no plant, no move, no power, no fight.

You quickly come to the conclusion in the maritime environment I'd better understand the fundamentals of my propulsion even if I'm an operations kind of guy or a combat systems kind of person. I think cyber is the same kind of way. You've got to understand the fundamentals.

Scott Tod: I think just creating the awareness of the issues in your organization, in your own personal space, your family, your children, relatives, in regards to cybersecurity, cybercrime and the awareness of cybercrime and what precipitates cybercrime, data breach or data access.

Lastly there's that national discussion in regards to privacy and lawful access. Those are things that are really engaging discussion. As you may know we've attempted legislation with regards to lawful access. It really is a lightning rod at times in regards to human rights, privacy and the intrusiveness of government organizations.

I think that discussion has to be matured more in regards to what it is Canadians are prepared to do in regards to the access to their personal information. I think those are healthy discussions that start at local levels. One of the things we didn't talk about today is that insider threat aspect. What are we doing internalizing in regards to that insider threat?

Although I look out quite often and look over, I don't look within very often. I think that's something is that look within first and make sure we're practicing cybersecurity, ensuring we're doing our best.

Dr. Oonagh Fitzgerald: Admiral Mike Rogers, Deputy Commissioner Scott Tod and vice president Cheri McGuire, thank you so much for owning this issue and demonstrating to the audience that there's a place for each of us in helping to solve the problem.

(Applause)

General Evraire: Before you leave the stage let me thank you again on behalf of everyone here for your masterful control and management of this panel but also for the great insights everyone brought in respect to this issue. What was really revealing here and perhaps more important was the fact that there was a great mix of military, private sector, police elements, everything you need to do or need to consider, take account of as we deal with this evolving and increasingly challenging threat.

Thank you very much for all of that. We're most grateful. You'll all get our book on the army, 1950 to 2000. I'm sure you'll read it when you have a spare moment. Thank you very much.

(Applause)

Questions? Please contact us at PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca.
Questions? Veuillez communiquer avec nous au PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca.

World News Overview
Aperçu des nouvelles mondiales

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

Tuesday, April 26 2016
le mardi 26 avril 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

Light coverage / couverture légère.

Canada

1- After officials confirmed Monday that **hostage John Ridsdel had been killed, Prime Minister Justin Trudeau called it "an act of cold-blooded murder"** by a "terrorist group" and said Canada would "pursue those responsible for this heinous act."A second Canadian, 50-year-old **Robert Hall, remains captive**, a Canadian government official confirmed. Canadian government defines **Abu Sayyaf largely as a kidnapping racket**, " the *National Post's* **Stewart Bell** points out. Ostensibly, the group's goal is the establishment of an Islamic state government by sharia law," according to the Public Safety Canada website. "In practice, however, the ASG primarily uses terrorism for profit."(extensive coverage / vaste couverture).

2- *La Presse+* rapporte qu'un **groupuscule anti-embourgeoisement aurait planifié son attentat incendiaire au quart de tour**, mais un appel au 911 l'a transformé en violente attaque contre des policiers. C'est la thèse privilégiée par les enquêteurs chargés de faire la lumière sur la **mystérieuse agression au cocktail Molotov** survenue il y a 10 jours dans Hochelaga-Maisonneuve. Pendant la soirée du 14 avril dernier, dans la rue Ontario, entre Moreau et Préfontaine, un groupe d'une vingtaine de personnes a lancé une attaque d'une rare violence contre les quatre voitures de police qui les suivaient sur quelques dizaines de mètres. Des engins incendiaires et des pièces pyrotechniques ont notamment été utilisés pour s'en prendre aux agents.

3- According to the *Ottawa Citizen*, **Mohamed Harkat**'s defence team will use a recent British court ruling to argue that the Algerian born terror suspect **should not be deported** to the turbulent North African country. A panel of judges from the United Kingdom's **Special Immigration Appeals Commission** ruled last week that six Algerian terror suspects cannot be deported because of the "real risk" they'll be tortured in their native country. The judges said the situation in Algeria is unpredictable given the threat of Islamism in the region and the frail health of President **Abdelaziz Bouteflika**. Bouteflika, 79, suffered a serious stroke in April 2013, and questions remain about who's actually running the country. In Canada, the federal government **continues to pursue the deportation of Ottawa's Harkat** 14 years after he was first arrested on the strength of a **national security certificate**. A feature of federal immigration law, the certificates give the government the power to remove foreign-born terror suspects based, in part, on secret evidence.

4- En raison du **blocage du gouvernement de l'Irak, le Canada est pris depuis plus de cinq ans avec une vingtaine de criminels irakiens** jugés particulièrement dangereux pour le public. **Au moins l'un d'eux est détenu à Montréal. Ottawa a tout tenté pour s'en débarrasser, mais Bagdad refuse de les reprendre.** Un résumé du dossier a été présenté au début du mois à la section montréalaise de la Commission de l'immigration et du statut de réfugié, lors d'une audience à laquelle *La Presse+* a assisté. Dans un des documents déposés en preuve, un représentant de l'Agence des services frontaliers du Canada (ASFC) cache mal son exaspération devant la tournure kafkaïenne du dossier.

International

United States / États-Unis

5- Addressing a *Christian Science Monitor* breakfast meeting yesterday, Director of National Intelligence **James Clapper** said the **Snowden leaks** have **accelerated** the **sophistication** of **encryption technologies** by **"about seven years** and "from our standpoint, **it's not a good thing**" because **new, commercially available encryption software** "had and is having **major, profound effects** on our **ability**" to **collect intelligence**, **"particularly against terrorists"**. (When pressed by the *Intercept* to **explain** his **'seven years'** figure, **Clapper** said it came from the **NSA.**) Clapper also said **Isis** has **clandestine cells** that are plotting more **terrorist attacks** in **Germany, Italy,** and **England** prompting the United States to step up efforts to promote more intelligence sharing.

United Kingdom / Royaume-Uni

Light coverage. / couverture légère.

Europe

6- Selon *Le Monde,* **deux faux migrants interpellés en Autriche, un Algérien et un Pakistanais, ont avoué qu'ils devaient participer aux attentats du 13 novembre à Paris.** «Ils m'ont dit que je devais aller en France, pour y accomplir une mission, et que je recevrais des instructions là-bas» .

7- **Sapo** is investigating a possible **Isis threat** to **Stockholm**, reports the *BBC,* after **Iraqi authorities** informed **Sweden** that **seven** or **eight militants** had traveled to the Nordic country.

8- *Fox News* reports that **shortly after** the **Charlie Hebdo attack** in Paris in January of last year, **French intelligence rejected** an **Israeli company's offer** of **terrorist-tracking software** that could have helped them flag terror cells. "**French authorities liked it**, but the official came back and said there was a **higher-level instruction not to buy Israeli technology,**" a **well-placed Israeli counter-terror specialist** familiar with the technology and the company behind it said. "The discussion just stopped."

9- According to **Finnish intelligence**, **2015** was a **very active** year marked by an **aggressiveness** in **espionage activity** not seen in previous years. The news organization *STT* reports Supo also made note of an attempt by foreign powers to influence energy policy decision-making.

Africa / Afrique

10- **Isis** has **claimed** it has **carried out** its **first attack** in **Somalia,** a **strike** against a **convey carrying African Union troops.** There's no word on the exact date of the attack or if there were casualties reports *Horseed Media.*

11- Selon *Jeune Afrique,* la **justice marocaine a décidé de classer sans suite la plainte déposée il y a deux ans à Paris par le kick-boxeur Zakaria Moumni contre le chef du renseignement marocain, Abdellatif Hammouchi.**

Middle East / Moyen-Orient

12- *The National (UAE)* reports that **pro-government forces** set up checkpoints across Mukalla on Monday and said all **Al Qaeda militants** had been cleared from the city where they had been based in Yemen for more than a year.

13- *Press TV* reports that **Iran's Intelligence Minister Mahmoud Alavi** says while the insecurity prevailing in most countries in the Middle East and across the world, the Islamic Republic enjoys **"unparalleled" security**.

14- The *Jerusalem Post* reports that the **Shin Bet (Israel Security Agency)** is reevaluating the way it provides entry permits after large numbers of **Palestinians** were denied entry to Israel due to security concerns.

Afghanistan/Pakistan

15- The *Khaama Press* reports **President Mohammad Ashraf Ghani** has ordered the Afghan National Security Forces (ANSF), specifically the **National Directorate of Security (NDS) directors**, to use all force against the terrorists fighting in the country.

Australia, New Zealand / Australie, Nouvelle-Zélande

16- A Sydney teenager charged with planning an Anzac Day terror attack was reportedly **part of a deradicalisation program** when he was arrested. The 16-year-old had been enrolled in the government-funded police deradicalisation program since last May after coming to authorities' attention for allegedly being in contact with Islamic State recruiter **Neil Prakash**, according to the *ABC News* and *News Corp Australia*. Prakash was said to have **encouraged the boy to take part in a terror attack last year**. The **Australian Federal Police** and the boy's lawyer, **Zemarai Khatiz**, refused to confirm the reports on Tuesday. Counter terrorism police arrested the teenager near his Auburn home on Sunday after he allegedly tried to source a gun before Anzac Day in preparation for a terrorist act.

Asia / Asie

17- The **Philippine military came under increased pressure today to rescue more than 20 foreign hostages** after their **Muslim extremist captors beheaded Canadian John Ridsdel** Monday, but troops face a dilemma in how to succeed and also ensure the safety of the remaining captives. About 2,000 military personnel, backed by Huey and MG520 rocket-firing helicopters and artillery, were involved in the manhunt for the militants, who were believed to be massing in Sulu's mountainous Patikul town, military officials said. (Extensive coverage / vaste couverture).
18- President **Park Geun-hye** said Tuesday that North Korea could **conduct a fifth nuclear test at any time** as she warned of stronger sanctions and pressure in case Pyongyang goes ahead with such provocations. North Korea **"completed its preparations for a fifth nuclear test and it is in a situation in which it can carry out"** the test at any time, Park said in a meeting with chief editors of several dozen newspapers and broadcasters at **Cheong Wa Dae**, South Korea's presidential office. The chief executive's assessment came amid speculation that North Korea could carry out another atomic weapons test to consolidate its internal unity ahead of a rare congress of the ruling Workers' Party early next month (extensive coverage / vaste couverture).

Americas / Amériques

Light coverage. / couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Friday, November 4, 2016
le vendredi 4 novembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1-A Federal Court judge **says Canada's spy agency illegally kept potentially revealing electronic data about people over a 10-year period**. At a hastily arranged news conference late yestreday, **CSIS director Michel Coulombe** said the **spy service had halted all access to, and analysis of, the data in question while it thoroughly reviews the court decision**. ``**I deeply regret the court's serious concerns with respect to meeting our duty of candour, and I commit to continuing my efforts, with the deputy minister of justice, to address this concern," Coulombe said. In a key 2013 ruling**, Federal Court Justice **Richard Mosley** chastised CSIS over a **request for warrants to track two Canadians with help from the Communications Security Establishment, Canada's electronic spy agency**. Mosley said CSIS breached its duty of candour by failing to disclose that CSE's foreign counterparts in the **Five Eyes intelligence network - the United States, Britain, Australia and New Zealand - could be called upon to assist.** (extensive coverage / vaste couverture)

2-Revelations of **police surveillance** of journalists are "troubling" and **could spark further measures to better safeguard the rights of the press, Prime Minister Justin Trudeau** says. At a news conference in Ottawa, held to respond to a Federal Court ruling on his **agency's handling of metadata collected under warrant,** CSIS Director **Michel Coulombe** offered assurances that his agency was not conducting surveillance on reporters. **"I completely agree with the PM on this issue,"** said Coulombe. **"Such a situation is not happening at the federal level." (extensive coverage / vaste couverture)**

3-**Huma Abedin** warned **Hillary Clinton** in **2010 that cables from the U.S. Embassy in Ottawa could cause problems for Stephen Harper's government**, emails released yestreday show. Abedin's email was sent on Nov. 27 2010. On Nov. 29 the *New York Times* published a story detailing a 2008 conversation between the former head of the **Canadian Security Intelligence Service Jim Judd** and senior **State Department counsellor Eliot Cohen**. The significance of Canada's role in the **Five Eyes alliance** became clearer in 2013 when leaked information from whistle blower **Edward Snowden** showed that **Canada's Communications Security Establishment** set up covert spy posts in about twenty countries on behalf of the **United State's National Security Agency,** *Postmedia News* writes.

4-**Le Service canadien du renseignement de sécurité (SCRS) a agi dans l'illégalité en conservant des données personnelles pendant 10 ans, a tranché la Cour fédérale.** Dans un jugement rendu public jeudi, le magistrat **Simon Noël a statué que le SCRS) avait manqué à son devoir d'informer le tribunal de son programme de collecte de données, qui opérait en vertu d'ordonnances judiciaires**. Le juge Noël estime que le SCRS aurait dû communiquer ses activités à la cour, puisqu'elles ne concernaient pas directement la sécurité nationale. Le SCRS a entamé le traitement de ces données en 2006 à l'aide d'un puissant logiciel nommé **Operational Data Analysis Centre (Centre d'analyse de données opérationnelles).** L'agence d'espionnage aurait ainsi obtenu des renseignements susceptibles de révéler des informations personnelles et pointues. (Vaste couverture/extensive coverage).

5-Selon *La Presse+,* se disant préoccupé par les révélations au sujet des **activités de surveillance menées par le Service de police de la ville de Montréal et la Sûreté du Québec auprès de journalistes, le premier ministre Justin Trudeau affirme avoir obtenu l'assurance de la part**

des patrons de la GRC et du SCRS qu'ils ne se livrent pas à de telles activités. En mêlée de presse, jeudi, M. Trudeau a indiqué avoir pris l'initiative de communiquer avec le **commissaire de la GRC, Bob Paulson, et le directeur du Service canadien du renseignement de sécurité (SCRS), Michel Coulombe,** afin de s'assurer que les règles et les lois fédérales qui s'appliquent à ces deux organisations soient respectées.
6-Le premier ministre **Justin Trudeau a indiqué jeudi qu'aucun journaliste ne faisait actuellement l'objet d'une surveillance de la part des services policiers ou de renseignement fédéraux.** Dans une conférence de presse organisée marge d'une séance plénière avec des étudiants, à Ottawa, il a signalé que son bureau s'en était assuré. Il a dit avoir obtenu ces **informations de la Gendarmerie royale du Canada (GRC) et du Service canadien du renseignement de sécurité (SCRS). Le premier ministre Trudeau a réitéré que son gouvernement prenait très au sérieux la question de la liberté de presse.** Il y a quelques mois, on a appris que le journaliste Joël-Denis Bellavance, du quotidien *La Presse*, avait été filé par la GRC. (Vaste couverture/extensive coverage).
7-In its reporting of Thursday's ruling on metadata retention by CSIS, the *Wall Street Journal* said the court issued a **'strong rebuke'** to the Service.

Canada

8-The *Montreal Gazette* writes that **three distinct cases of police forces spying on Quebec journalists emerged this week**. In at least two of them, investigators were trying to **stop police information from leaking to reporters.** The surveillance was launched after then-Parti Québécois public security minister **Stéphane Bergeron** asked then-SQ director general **Mario Laprise** to look into leaks to the news media about an investigation into **Michel Arsenault**.

International

United States / États-Unis

9-The *Washington Post* reports **U.S. intelligence does not see Russia** as capable of **using cyber-espionage** to **alter** the **outcome of Tuesday's presidential election**, but they have warned that **Moscow may continue meddling** after the voting has ended to **sow doubts about the legitimacy** of the **result.** However, they have **not ruled out** a **Russian-sponsored disruption** on Election Day. In recent weeks, officials at the **Department of Homeland Security** have collected **evidence** of apparent **Russian "scanning"** of **state-run databases** and **computer voting systems.** "Whether they were really trying hard to get in, it's not clear," a U.S. official said. Still, the decentralized nature of U.S. polling would make it extraordinarily difficult to subvert a nationwide race. Instead, officials said it is **more likely** that **Russia** would use **hacking tools** to **expose** or **fabricate signs of vote-rigging**, aiming to **delegitimize** an election outcome that Donald Trump has said he may refuse to accept if he does not win.
10-An **FBI agent** told Britain's *Guardian* newspaper that the **Bureau is "Trumpland"** with **Hillary Clinton** considered the **"antichrist personified"**. Other *Guardian* sources **dispute the depth of support for Trump** within the FBI, though they **uniformly stated** that **Clinton is viewed highly unfavorably**. "There are lots of people who don't think Trump is qualified, but also believe Clinton is corrupt. What you hear a lot is that it's a bad choice, between an incompetent and a corrupt politician," said a former FBI official.

United Kingdom / Royaume-Uni

11-Prime Minister **Theresa May** is expected to tell the **president** of the **European Commission Jean-Claude Juncker** that her **timetable for Brexit in March** is **still on track** despite yesterday's ruling in the High Court that parliament must be consulted first. (Extensive coverage / vaste couverture).

12-**Jayda Fransen**, the **deputy-leader** of the **far-right Britain First**, has been **fined nearly £2,000,** reports the *Press Association,* after a court found her **guilty** of **religiously aggravated harassment** for **hurling abuse** at a **Muslim mother wearing a hijab** during a "Christian patrol" of Bury Park in Luton this past January.
13-British Foreign Secretary **Boris Johnson** indicated that according to **available intelligence**, **Isis leader Abu Bakr al-Baghdadi,** is **no longer in Mosul** reports the *Guardian.*

Africa / Afrique

14-D'après *All Africa,* **officiels togolais et béninois entendent renforcer leur coopération sécuritaire**. Depuis mercredi matin les ministres en charge de la **Sécurité des deux pays et les responsables des services de renseignement se concertent**. Au programme de la rencontre, la lutte contre la **criminalité transfrontalière, le banditisme, le terrorisme, la cybercriminalité.**

Middle East / Moyen-Orient

15-The *Times of Israel* reports that Iran commands a force of up to **25,000 Shiite Muslim militants** fighting in the Syrian civil war, a majority of them from Afghanistan and Pakistan, according to **former Shin Bet chief Avi Dichter**.
16-*The National (UAE)* reports that **Abu Bakr Al Baghdadi, the elusive leader of ISIL** has released a message urging his followers to keep up the fight against a major offensive to rout the extremists from Mosul, their last urban stronghold in Iraq.

Afghanistan/Pakistan

17-The *Pakistan Daily Times* reports that **travellers flying to Canada** with a Pakistani passport require a valid visa and an eTA, which are not the same document but some third parties are selling fraudulent eTAs to Pakistani citizens, according to an advisory issued by the **Canadian Embassy** in Islamabad.
18-The *International News* reports that **Pakistan** on Thursday took a step forward to internationalise and reached out to foreign capitals regarding the activities of Indian state-sponsored subversive and terrorist activities inside Pakistan — **having contacts with Taliban and aiming at sabotaging the China Pakistan Economic Corridor** — which has led to nine Indian officials including diplomats at the Islamabad Mission found involved in promoting terrorist activities and terror financing.
19-*Pajhwok Afghan News* reports that President Ashraf Ghani has said **30 terrorist organizations** are operating in **Afghanistan** and the country could not be stabilized by militia forces and illegal armed groups, but by Afghan security forces.

Europe

20-The **Diyarbakır Governor's Office** says the **PKK** is **responsible** for this morning's **car bomb** blast in the **Turkish city** which has **killed eight people** and **wounded 100 others** reports the *Hurriyet Daily News.* The blast occurred not long after the **co-leaders** of the **opposition Peoples' Democratic Party** (HDP) and **10** of their **colleagues** were **arrested** in **'anti-terror' raids.**
21-According to the German media, the **27-year-old Syrian refugee arrested** at his apartment in Berlin on Wednesday on suspicion of being a **member of Isis** and of **plotting a terror attack** is **'Ashraf al-T'**. The suspect is considered to be **"highly dangerous"** and **Interior Minister Thomas de Maizière** said he was **under surveillance** by the **BfV** for **some time.**
22-**Swiss prosecutors** have concluded that a **"significant" number** of **computers** in use at a **Geneva hotel** where sensitive **Iranian nuclear talks** were taking place in 2015 were infected by **malware** for the purposes of **cyber-espionage** but after a months-long investigation, the Attorney General's office was **unable to determine who was responsible** so it has closed the probe reports *The Local.*

23-A **Belgian court** has ruled that the **recruitment activities** conducted by the **PKK** in the country were **within** the **scope of** an **armed struggle rather** than **connected** to **terrorism.** Turkey's *Daily Sabah* speculates "the court's ruling is expected to **sour relations between Brussels** and **Ankara**. **Belgium** once again has **turned a blind eye** to **PKK terrorist activities** in the country despite EU recognition of the group as a terror organization being binding for Belgian authorities".

24-Soupçonné d'être **le tueur du Musée juif de Bruxelles en 2014, il aurait été le geôlier de quatre journalistes français en Syrie.** Pour les Belges, il reste avant tout le principal suspect de la tuerie du Musée juif de Bruxelles. Mais pour les Français, **Mehdi Nemmouche serait aussi le geôlier djihadiste ultraviolent qui fredonnait La Bohème d'Aznavour devant ses quatre compatriotes journalistes, otages en Syrie pendant dix mois.** C'est à ce titre que Paris avait délivré au mois d'août dernier un mandat d'arrêt européen contre le Français d'origine algérienne, âgé de 31 ans et actuellement détenu dans le quartier de haute sécurité de la prison de Bruges. La justice belge a donné jeudi son feu vert à sa remise à la France, mais sans préciser à quelle date elle pourra avoir lieu rapporte *Le Figaro.*

25-**Ziane Mehadjri sort du silence. Indésirable au Petit-Saconnex, il a créé sa propre organisation.** La grande mosquée de Genève, au Petit-Saconnex, ne cesse d'alimenter la chronique. Des **jeunes radicalisés l'ont longtemps fréquentée et deux d'entre eux ont rejoint Daech l'an dernier. On sait que deux imams français employés de la Fondation culturelle islamique de Genève, qui gère l'institution, sont fichés S pour radicalisation par les services de renseignement de l'Hexagone.** La semaine dernière, on apprenait que le **chef de la sécurité de la mosquée était lui aussi fiché S. Un troisième imam a, jusqu'à présent, peu fait parler de lui: l'Algérien Ziane Mehadjri.** Et pour cause. Voilà deux ans qu'il est interdit de prêche à la grande mosquée. Il sort du silence, annonçant son licenciement à la fin de septembre - qu'il conteste juridiquement - et la création par ses soins, à Genève, de l'Organisation européenne des centres islamiques, une initiative qui a suscité l'ire de son employeur révèle la *Tribune de Genève.*

26-Selon *La Tribune de Genève,* le **Ministère public de la Confédération, qui confirme l'information, suspend son enquête, faute de pouvoir identifier les coupables Les entretiens sur le programme nucléaire iranien qui se sont tenus à Genève au printemps 2015 ont bien été espionnés.** Le Ministère public de la Confédération (MPC) l'a confirmé, mais il a décidé de suspendre son enquête, faute de pouvoir identifier les coupables. Les investigations ont permis d'établir qu'un grand nombre d'ordinateurs ont été infectés par un maliciel dans l'hôtel genevois où se sont tenus les entretiens des ministres des Affaires étrangères de l'Iran, des Etats-Unis, de la France, de la Chine, de la Russie et de l'Allemagne. Les recherches effectuées ne fournissent toutefois aucun soupçon par rapport à des auteurs concrets. Même s'ils sont passibles de poursuites pénales, les éléments ne peuvent pas être attribués à une personne déterminée. C'est pour cette raison que le Ministère public de la Confédération a suspendu la procédure ouverte en mai 2015 sur la **base d'informations du Service de renseignement de la Confédération (SRC).**

Australia, New Zealand / Australie, Nouvelle-Zélande

27-**Police have moved to smash a suspected new terror cell of Islamic State extremists** they - believe may have been **planning attacks in Sydney**. The *Australian* reports that officers from the **NSW Joint Counter Terrorism Team** yesterday conducted a string of raids across southwestern Sydney, arresting two men and turning over six houses amid fears that members of the group may have sourced weapons. **The raids were part of larger assault on a suspected cell of about 10 Muslim men.**

28-The growing risk of **cyber attacks** leaves the Australian economy exposed to a potential **$16 billion damage bill over the next decade**, according to one of the world's biggest insurance companies. In a joint study with **Cambridge University**, the *Australian Broadcasting Corporation* writes that the Lloyd's insurance giant has found out of 301 global cities, Sydney ranks 12th in terms **cyber attack exposure with $4.86 billion of economic growth at risk.**

29-**Australia's domestic intelligence agency failed to notify the intelligence watchdog of a controversial "special intelligence operation"** for **10 days** in what is the first **official confirmation of highly secretive missions that give intelligence officers immunity from prosecution,** the *Guardian* reports. In 2014 the government passed controversial national security laws that allow the creation of "special intelligence operations" that must be approved by the attorney general, **George Brandis.**
30-Concrete evidence has emerged that **there has been an attempt to carry out a terrorist attack on New Zealand soil**, the *New Zealand Herald* writes. The **security services will release no details of how the plot was foiled or when it emerged.** The system which was activated to deal with it has been in existence for only two years. The revelation of the threat came from the newly released **National Security System handbook**. It stated the system - which triggers special protocols - had been activated for a "threat of a domestic terrorist incident". The newly released annual report from **the Inspector-General of intelligence and Security, Cheryl Gwyn,** said there had been one case of the **NZSIS needing an urgent warrant for visual surveillance of a target or targets.**

Asia / Asie

31-*The Hindu* reports that **India-Pakistan bilateral relations** plummeted further on Thursday with Pakistan formally naming eight Islamabad-based **Indian diplomats as alleged spies**.
32-The *Dhaka Tribune* reports that **new JMB** had plans to stage a big terror attack in Dhaka, police learnt from four firearms smugglers arrested by the **Counter-Terrorism and Transnational Crimes (CTTC)** unit of police in the capital's Darussalam area on Wednesday.
33-According to the *China Daily*, security and technology experts are calling on African governments to embrace safe-city concepts in an effort to address the **increasing incidence of crime and extremism**. Combating crime, according to the experts, **has become the hardest activity for police and security organizations,** as **available video security systems are faced with blind spots, unclear images, difficult video retrieval and data damage or loss**. To solve these challenges, the experts are recommending a safe-city technology solution provided by **Huawei Technologies Co**, a Chinese **multinational IT company headquartered in Shenzhen**, Guangdong province.
34-The commander of U.S. forces in South Korea said on Friday a **U.S. Terminal High Altitude Area Defense (THAAD) anti-missile system battery** would be deployed to South Korea **within eight to 10 months,** an official from the U.S. forces in South Korea said. The official was commenting on a *Yonhap news agency* report on remarks made by **Vincent Brooks**, commander of United States Forces Korea, in which he laid out plans for the deployment. Brooks said rotating strategic weaponry onto the Korean peninsula would have a deterrent effect against North Korean provocations, according to the agency. He also said the battery would be bigger than one deployed in Guam, writes *Reuters*.

Americas / Amériques

35-**Venezuelan's Opposition** has set a **November 11 deadline** for the **Maduro government** to **act** on its **demands** or it will **quit Vatican-led talks** and **resume protests** reports *Reuters*.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Wednesday, December 7 2016
le mercredi 7 décembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- Citant les **révélations d'Edward Snowden et les cas de journalistes surveillés au Québec, les commissaires à la protection de la vie privée du pays** mettent le gouvernement Trudeau en garde: au lieu de donner de nouveaux pouvoirs aux corps policiers, **Ottawa doit plutôt mieux encadrer les pouvoirs policiers existants en matière de surveillance**. «Sans vouloir faire comparaison» avec les services de renseignement des ex-républiques de l'Europe de l'est, le commissaire **Daniel Therrien rappelle toutefois une décision récente de la Cour fédérale dénonçant le fait que le Service canadien du renseignement de sécurité (SCRS) a conservé de façon illégale pendant plusieurs années des métadonnées** de citoyens canadiens (le SCRS interprétait la loi différemment et s'est plié à la décision de la Cour fédérale). «Nous parlons ici de retenir des données de citoyens ordinaires. Je ne crois pas que c'est le type de société dans laquelle [les Canadiens] veulent vivre», dit le commissaire Daniel Therrien rapporte *La Presse*.

2- Canada's spy agencies should **destroy the data trails of innocent people they incidentally collect** during terrorism investigations once the actual targets have been cleared of suspicion, say Canada's privacy watchdogs. The declaration Tuesday from **privacy commissioners** across the country came after a judge recently ruled the **Canadian Security Intelligence Service** violated the law by **keeping potentially revealing electronic data about people who were not under investigation.** The message was part of a **joint submission signed by federal, provincial and territorial privacy czars** that urged the Trudeau government to strengthen protection of personal information as it revamps the national security regime, the *Canadian Press* reports. Rather than expand state powers and reduce individual rights, it is time to **beef up legal standards and oversight to prevent repetition of mistakes**, said federal privacy commissioner **Daniel Therrien**, flanked at a news conference by counterparts **Brian Beamish** from Ontario **and Jean Chartier** of Quebec.

Canada

3- A Canadian military veteran **who had been detained by Iraqi authorities** after spending six months fighting ISIL **has been released**, his mother said Tuesday. "He's been freed, thank God," **Kay Kennedy** said shortly after her son, **Michael Kennedy**, phoned home from Erbil to say he was no longer being held. She said he told her he had been detained with three Americans and two Germans over travel visa problems. While Kennedy had a valid Iraqi visa, his travelling companions did not (moderate coverage / couverture modérée).

International

United States / États-Unis

4- *Washington Post* columnist Josh Rogin reports that **incoming national security adviser Michael Flynn** will **meet** with **Obama national security adviser Susan Rice** for the **first time today** at the White House. The meeting comes as **Democrats in Congress** are ramping up their **criticism** of **Flynn** and his recent behavior, especially his **use of social media.** Rogin makes note of a a **tally by *Politico*** which found that **Flynn** has **pushed fabricated** or **dubious stories** on

Twitter at least **16 times since August**. When asked if he had any **concerns** about Trump's national security selection, Senate Armed Services Committee chair **John McCain** replied **"none at all"**.
5- Speaking at the University of Maryland, **former NSA director Keith Alexander** said an **early foreign policy test** for **Donald Trump** is how to **respond**, if at all, to a **Russian hacking campaign** designed to interfere with the presidential election. The *Baltimore Sun* reports Alexander **praised James Mattis**, the retired Marine general who is Trump's pick to run the Defense Department, and **Mike Pompeo**, tapped to lead the CIA.

United Kingdom / Royaume-Uni

6- **Mohamed Abrini**, the so-called 'Man in the Hat' suspected of participating in the **Brussels airport bombing** in March, was the subject of a **"low level" investigation** by the **MI5** when he was in **Birmingham in July 2015** but the Security Service concluded that he **did not pose** a **significant threat** to the UK. This, reports the *Daily Telegraph,* was revealed during the **trial** of **Zakaria Boufassil**, a Belgian national living in Birmingham, who has been found **guilty** of **supplying thousands of pounds** to **Abrini** during his secret mission to the UK.
7- Police are investigating a **40 second video** in which the **New IRA displays** what appears to be a **military grade rocket launcher** on the **streets of north Belfast** reports the *Guardian.* The video, which appeared on **social media** on Monday evening, is the second in two years in which the dissident republican group has released propaganda images of weapons it claims to have at its disposal.

Europe

8- **Les budgets des deux principales agences de l'alliance «Five Eyes» ont encore été augmentés** ces deux dernières années, sur fond de **lutte contre le terrorisme.** Au sein du club très fermé des «Five Eyes» qui réunit, depuis la seconde guerre mondiale, les **services secrets techniques américains, britanniques, australiens, canadiens et néo-zélandais, le Royaume-Uni et les Etats-Unis tiennent les deux principaux rôles.** Là où l'Agence nationale de sécurité (NSA) américaine compte 60000 personnes, son homologue française, la direction technique de la **Direction générale de sécurité extérieure (DGSE) emploie 3000 agents.** Chargée d'une mission offensive et défensive, la NSA s'efforce d'avoir accès à tous les réseaux informatiques et de communication afin de collecter et de traiter en masse les données de connexions. Elle dispose d'un budget annuel de plus de 10milliards de dollars, supérieur à celui de la CIA.
9- Selon *L'Agence télégraphique Suisse,* les **moyens prévus pour le Service de renseignement de la Confédération (SRC) sont pour l'instant suffisants**. Fort de cette conviction, le Conseil des Etats a enterré mardi tacitement une motion du National qui réclamait plus de personnel. **Depuis le dépôt du texte en septembre 2015, 86 postes supplémentaires ont été créés dans le domaine de la lutte contre le terrorisme, dont 23 pour le SRC, a rappelé Isidor Baumann (PDC/UR) au nom de la commission.** L'application de la nouvelle loi sur le renseignement s'accompagnera par ailleurs de la création de 19,5 emplois.

Africa / Afrique

10- Libyan fighters have declared that **Isis** has been **defeated in Sirte,** but analysts, reports the *New York Times,* warn the **Islamic State** could **still regroup in other parts of Libya** by **exploiting** the **economic ruin** and **political vacuum** that has dogged the country since the ouster of Col. Muammar el-Qaddafi in 2011. "I'm concerned about the pockets of marginalization, and in some areas **pre-existing jihadist presence,** that they could use to reconfigure," said **Frederic Wehrey**, a senior fellow at the **Carnegie Endowment for International Peace**, citing the **presence of Islamic State forces** in **Tripoli, Benghazi** and the desert town of **Sabha.**

Middle East / Moyen-Orient

11- *Press TV* reports that **Iranian Interior Minister Abdolreza Rahmani Fazli** says **25 terrorist groups** were disbanded during the religious rituals of Arba'een last month.
12- The *Gulf News* reports that police in the strategic Yemeni city of Aden **busted a cell** linked to Daesh responsible for **assassinating intelligence officers** and carrying out other terror attacks.
13- The *Saudi Gazette* reports that **Saudi Arabia suffered more than 128 terrorist operations** in the last 15 years that killed or injured as many as 1,147 Saudis and expatriates, according to spokesman of Interior Ministry Maj. Gen. Mansour Al-Turki.

Afghanistan/Pakistan

14- The *International News* reports that **Pakistan** on Tuesday said it had established a comprehensive and effective national **nuclear security regime**, which is at par with the latest international standards and guidelines.
15- *Pajhwok Afghan News* reports that **National Directorate of Security (NDS) chief for Nangarhar Brig. Gen. Dad Mohammad Harifi** told a press conference that their operatives had seized **eleven militants, including a would-be bomber** tasked with targeting the Indian diplomatic mission in eastern Nangarhar province.

Australia, New Zealand / Australie, Nouvelle-Zélande

16- According to *Scoop.co.nz,* the **Government Communications Security Bureau** wants to **give internet service providers more information** and **power to block cyber threats** which are increasing, its director told the **intelligence and security select committee** yesterday. The **communications-focussed spy agency has recorded 338 cyber security incidents in the last year**, from 109 a year earlier, which director Andrew Hampton said was due to both the number of threats increasing and the improved system picking up more threats.
17- A Melbourne man has been sentenced to a two-year corrections order plus time already served in custody for **funding an American man's travels to Syria** to fight against the Assad Government. **Hassan El Sabsabi**, 25, of Seabrook pleaded guilty in the Victorian Supreme Court to funding terrorism in August 2015 (moderate coverage / couverture modérée).

Asia / Asie

18- According to *Yonhap News Agency*, a recent **intelligence-sharing** deal that Japan reached with South Korea is a **"necessary"** step to **guarantee its national security in the face of threats** from **China** and **North Korea**, a former Japanese envoy to Seoul has said. Last month, South Korea and Japan signed the **General Security of Military Information Agreement (GSOMIA)** aimed at **expanding intelligence sharing** between the two neighbors and better countering the threat, in particular, from North Korea. The deal, however, sparked strong opposition from some politicians and civic groups in South Korea as they argued that Japan is working to expand its military power and overseas role without sincerely apologizing for its wartime atrocities decades ago.
19- Military investigators looking into the first **hacking of South Korea's cyber command intranet** said Wednesday the **suspected North Korean attackers accessed the network through a server** at the armed forces' **main information center**. The findings raised **concerns that confidential information may have been compromised** as the affected server is connected with the information systems of the **Army, Navy and the Air Force**. But the ministry said **information saved on the server system was not stolen**, reports *Yonhap News Agency*.
20- The *Times of India* reports that **terror-related violence in Jammu & Kashmir** has peaked to the highest level in past four years, with incidents up 47% and killing of terrorists witnessing a 300% spike over 2015.
21- The *Jakarta Post* reports that the **Islamic State (IS)** group's attempt to create a fully pledged wilayat or province in the southern Philippines poses a **serious security threat to Indonesia**, the Indonesian Military (TNI) has warned.

Americas / Amériques
Light coverage / couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Thursday, December 8 2016
le jeudi 8 décembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- The civil servant in charge of the government's spy-watchdog agency says Canada may have to **reconsider how it shares intelligence with the United States** if president-elect **Donald Trump** makes good on his promise to **torture terrorists to gather intelligence**. The federal official also **remarked that had former U.S. intelligence analyst Edward Snowden** worked for Canadian intelligence and leaked secrets, "**he should be shot**," but quickly backed off the opinion. **Michael Doucet**, the executive director of the **Security Intelligence Review Committee**, made the off-the-cuff remarks to a small audience in Toronto last week. An audio recording of his talk was provided to *The Globe and Mail* by a student journalist from the *Eyeopener*, a campus newspaper at **Ryerson University**, which was the venue for the talk. For 1 1/2 hours, the former intelligence analyst held forth on intelligence issues. Members of SIRC rarely make unscripted or unguarded remarks publicly because they are sworn to secrecy about their work reviewing the highly classified spying operations of the **Canadian Security Intelligence Service.** When contacted on Wednesday, Mr. Doucet acknowledged he made the comments, but said he was not expecting them to be recorded. **Should the CIA revert to practices such as simulated drowning techniques known as "waterboarding," it could cause problems for CSIS and other Canadian agencies**. Harking back to his years when he worked for Canada's signals-intelligence agency – the **Communications Security Establishment** – Mr. Doucet told the audience intelligence-sharing is vast, and alliances are important. He pointed out that in the mid-2000s, he was **CSE's embedded liaison officer at the U.S. National Security Agency.**

Canada

2- D'après *Radio-Canada - Nouvelles* - (site web), un **groupe de jeunes Québécois s'est joint secrètement aux milliers de combattants étrangers en Syrie pour lutter contre le régime de Bachar Al-Assad. Aujourd'hui, ils sont soupçonnés d'avoir commis des actes terroristes.** Nous avons découvert qui ils sont. Une dizaine d'amis se retrouvaient régulièrement dans un centre de tir de la région de Montréal pour s'entraîner avant le **départ de sept d'entre eux pour le Moyen-Orient entre l'été 2012 et l'été 2013**. Lors des séances de tir, ils prennent souvent des pauses pour prier. Plusieurs d'entre eux s'étaient convertis à l'islam. Un jour, un client aurait entendu un jeune dire qu'il était malheureux que les cibles ne soient pas des mécréants.

3- The case against an Egyptian man long **branded a terrorist threat** has been riddled with so many problems over the years that a judge should have ended the proceedings, Federal Court of Appeal heard Wednesday. Instead, his lawyer argued, Judge Edmond Blanchard **upheld the national security certificate** imposed on **Mohamed Mahjoub** despite finding the government had violated his rights, reports the *Canadian Press*. "The remedies provided in relation to the violations found by Justice Blanchard were inadequate," Mahjoub's lawyer Paul Slansky said. Mahjoub, 56, of Toronto, has been in prison or under severe restrictions since the government first decided in 2000 _ **based in part on secret evidence supplied by foreign agencies linked to torture** _ that he posed a threat to Canada's national security. Among other things, **Canada's spy agency alleged Mahjoub was a leading member** of the Egyptian terror group **Vanguards of**

Conquest, and a trusted associate of former terrorist mastermind, **Osama bin Laden** _ accusations Mahjoub has always denied.
4- D'après *Radio-Canada - Nouvelles* - (site web), un **groupe de jeunes Québécois s'est joint secrètement aux milliers de combattants étrangers en Syrie pour lutter contre le régime de Bachar Al-Assad. Aujourd'hui, ils sont soupçonnés d'avoir commis des actes terroristes.** Nous avons découvert qui ils sont. Une dizaine d'amis se retrouvaient régulièrement dans un centre de tir de la région de Montréal pour s'entraîner avant le **départ de sept d'entre eux pour le Moyen-Orient entre l'été 2012 et l'été 2013**. Lors des séances de tir, ils prennent souvent des pauses pour prier. Plusieurs d'entre eux s'étaient convertis à l'islam. Un jour, un client aurait entendu un jeune dire qu'il était malheureux que les cibles ne soient pas des mécréants.

International

United States / États-Unis

5- 'For reasons that remain unclear', *Time* reporter Michael Scherer writes in a profile of **Donald Trump**, the magazine's **Person of the Year**, Trump **still refuses** to **acknowledge** the **U.S. intelligence community's conclusion** that **(Russian) agencies** were **responsible** for stealing the Democratic National Committee and Clinton campaign emails. **"I don't believe it. I don't believe they interfered,"** Trump said. Asked if he thought the **conclusion** of **America's spies** was **politically driven**, Trump responded **"I think so."**
6- Despite making regular remarks on the campaign trail disparaging military brass, **Donald Trump's probable selection** of **retired Marine Gen. John Kelly** to **lead** the **Department of Homeland Security** would be the **third general** he's named to **top positions in his administration. "I'm concerned,"** said **Democratic Senator Chris Murphy,** a member of the **Foreign Relations Committee**. "Each of these individuals may have great merit in their own right, but what we've learned over the past 15 years is that when we view problems in the world through a military lens, we make big mistakes.". However, **Senator Thomas R. Carper**, the former chairman of the Homeland Security panel, told the *Washington Post,* that with the **selection of Kelly,** Trump has **" hit a home run with runners on base".**
7- Combing the files of the **NSA's internal news site 'SIDtoday' from 2004** which were provided by Edward Snowden, *The Intercept* described **information overload** at the **Agency,** how the **NSA trained FBI agents, enabled U.S. intervention in Latin America,** and, with the help of a gifted analyst at the Defense Intelligence Agency, learned the value of simply reading information that was already public. One document even suggests that NSA personnel routinely got dangerously chatty at restaurants near headquarters.

United Kingdom / Royaume-Uni

8- With a warning that the **terrorist threat** is **"more acute and complex"** than ever, the **British government** has drawn up a **plan** to deal with a **biological weapons attack** reports *The Times of London.*
9- Police in **Cork** are searching for **one, possibly two gunmen** who opened fire on **Aidan 'The Beast' O'Driscoll** as he walked on a city street Wednesday evening, **killing** the former **high-ranking member** of the **New IRA.** (Extensive coverage / vaste couverture).

Europe

10- **Le GCHQ britannique a espionné l'Etat hébreu tout en coopérant avec Ruffle, son homologue israélien.** On ne se méfie jamais assez de ses amis, surtout les plus proches. Officiellement, Israël et les deux agences de surveillance anglo-saxonnes les plus puissantes, **l'Agence nationale de sécurité (NSA)** américaine et son homologue britannique, **le Government Communications Headquarters (GCHQ)**, sont unis par une sacro-sainte alliance. L'été 2009 verra néanmoins pour la première fois l'organisation d'une **réunion à quatre au siège du GCHQ,**

" avec la NSA, le Centre canadien de sécurité des communications et Ruffle ", pour une mise en commun d'informations, notamment sur l'Iran et les Palestiniens. Ce partage ne va pas de soi parce qu'Israël n'appartient pas au cercle très fermé des " Five Eyes "qui ne comprend que les services anglo-saxons (Etats-Unis, Royaume-Uni, Canada, Nouvelle-Zélande et Australie) rapporte *Le Monde.*

11- Selon *Le Monde,* au sein du club très fermé des **" Five Eyes " qui réunit, depuis la seconde guerre mondiale, les services secrets techniques américains, britanniques, australiens, canadiens et néo-zélandais, le Royaume-Uni et les Etats-Unis tiennent les deux principaux rôles**. L'Agence nationale de sécurité (NSA) américaine compte 60 000 personnes, son homologue française. **Chargée d'une mission offensive et défensive, la NSA s'efforce d'avoir accès à tous les réseaux informatiques et de communication afin de collecter et de traiter en masse les données de connexions.** Elle dispose d'un budget annuel de plus de 10 milliards de dollars (9,3 milliards d'euros), supérieur à celui de la CIA. " *Le Monde* " a travaillé sur la totalité des **archives de l'ex-consultant de la NSA Edward Snowden, qui sont loin d'avoir révélé tous leurs secrets Pour beaucoup, les révélations liées aux documents extraits des archives de l'Agence nationale de sécurité (NSA) américaine par un ancien consultant, Edward Snowden, aujourd'hui réfugié en Russie, étaient de l'histoire ancienne. Il n'en est rien.** Trois ans après sa décision de dénoncer, preuves à l'appui, l'existence d'un système de surveillance construit sur la collecte massive des données de communications, il reste de nombreuses leçons à tirer du stock -**impressionnant de documents soustraits à la NSA et à son homologue britannique, le Government Communications -Headquarters (GCHQ). Comment " Le Monde " a travaillé Grâce à un partenariat exclusif avec le site d'information The Intercept , fondé, notamment, par les deux premiers destinataires des archives Snowden, Glenn Greenwald et Laura Poitras,** Le Monde a pu travailler, en 2016,
directement sur l'intégralité de ce fonds documentaire.

12- **Germany's BfV** released a statement this morning **accusing Russia** of **ramping up propaganda** and **disinformation campaigns** aimed at **destabilizing German society** reports *Reuters.* **Director Hans-Georg Maassen** is quoted as saying "we see **aggressive** and **increased cyber spying** and **cyber operations** that could potentially endanger German government officials, members of parliament and employees of democratic parties".

Africa / Afrique

13- Le **Premier ministre belge, Charles Michel, a indiqué à Alger, avoir eu avec le Premier ministre, Abdelmalek Sellal des échanges "denses et intenses sur des sujets important" dans l'intérêt du partenariat algéro-belge.** Le responsable belge estime, que "pour réaliser tout développement économique, il faut de la **stabilité et de la sécurité", relevant que l'Algérie "connait très bien c'est quoi la lutte contre le terrorisme pour avoir payé un lourd tribut" lors des années de tragédie traversée par l'Algérie** rapporte *All Africa.*

14- Selon *All Africa,* l'organisation jihadiste **Etat islamique** a perdu Syrte mais le danger de son éparpillement en Libye est plus grand que jamais.

Middle East / Moyen-Orient

15- *Asharq Al-Awsat* reports that the leaders of **Canada, France, Germany, Italy, the UK and the U.S.A.** have declared readiness to consider additional restrictive measures against supporters of Head of Syrian Regime Bashar al-Assad regarding the situation in Aleppo.

16- The *Jerusalem Post* reports that the **Shin Bet (Israel Security Agency)** recently arrested a **terrorist cell** suspect carried out several shooting attacks against the Ofra settlement in the Binyamin region of the West Bank.

17- *The National (UAE)* reports that the **Gulf States and Britain** pledged to work together to counter **Iran's "destabilising activities"** in the region as they announced a wide-ranging "strategic partnership" at the GCC Summit in Bahrain on Wednesday.

18- The *Times of Israel* reports that **Israel** was responsible for recent attacks in Syria, saying on Wednesday that they were meant to prevent **"advanced weapons, military equipment and weapons of mass destruction"** from reaching Hezbollah.

Afghanistan/Pakistan

19- The *Pakistan Dawn* reports that Adviser to Prime Minister on Foreign Affairs Sartaj Aziz on Wednesday informed the Senate that evidence was being collected regarding the role of **Indian spy Kulbushan Jadhav** in Pakistan.
20- *Pajhwok Afghan News* reports that **NATO Secretary General Jens Stoltenberg** on Wednesday said the situation in Afghanistan "is and will remain difficult and tough" but "our commitment to Afghanistan's security is strong and steadfast.

Australia, New Zealand / Australie, Nouvelle-Zélande

21- According to the *Australian Associated Press*, Prime Minister **Malcolm Turnbull** has declared terrorists should face the **"full severity of the law"** a day after a Melbourne teenager was sentenced to seven years in jail for preparing a bomb attack. A Victorian Supreme Court judge on Wednesday said the 18-year-old, who cannot be named, had "every intention" of using the partially constructed pipe bombs found in his home and the only reason he didn't go through with his plot was that he was arrested. Mr Turnbull on Thursday was asked if he thought the sentence was too lenient. The prime minister replied **that sentencing was a matter for the courts and he wouldn't comment on any particular case.** "(But) terrorist offences should be dealt with with the full severity of the law," he told *3AW*.
22- Police are using **aggressive disruption tactics** normally used on organised crime gangs to thwart a **suspected Sydney terror cell** they fear is intent on **carrying out a terrorist attack**, reports *The Australian*. State and federal detectives from the **NSW Joint Counter Terrorism Team** have been targeting a cell of about **10 young suspected extremists** operating in the southwest of Sydney. The operation, which stemmed from the arrest last month of **Mehmet Biber**, who police allege fought with an Islamist group in Syria in 2013, has been under way for several months. It is understood **Junaid Thorne**, a young preacher well known to authorities thanks to his radical sermonising, is thought to be the spiritual head of the group.

Asia / Asie

23- The *Times of India* reports that the **Twitter handles of Rahul Gandhi and the Congress** which were recently hacked were operated from five countries- Sweden, Romania, the US, **Canada** and Thailand, Delhi Police on Wednesday said.
24- The *Manila Bulletin* reports that members of the **terror cell** who planned the foiled bomb attack in Manila near the **US Embassy** last month were found to have been communicating through Facebook and other social media platforms.
25- Chinese State Councilor and Minister of Public Security **Guo Shengkun** on Wednesday met with U.S. Attorney General **Loretta Lynch** and U.S. Secretary of Homeland Security **Jeh Johnson**, the *Xinhua News Agency* reports. During his meeting with Lynch, Guo noted that China-U.S. cooperation in law enforcement has **developed steadily**.

Americas / Amériques

Light coverage. / couverture légère

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.

Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Friday, December 9, 2016
le vendredi 9 décembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1-**The federal public safety minister is keeping the door open to the idea of Canada's spy agency crunching potentially sensitive data about innocent people**, the *Canadian Press* writes. **Ralph Goodale** told MPs at a House of Commons committee Thursday he is weighing views on whether the **Canadian Security Intelligence Service** should be allowed to retain and use such information. Last month Federal **Court Justice Simon Noel said CSIS violated the law by keeping electronic data about people who were not actually under investigation.** CSIS director **Michel Coulombe** told the committee he hoped the spy service would be in a position within about six months to decide what to do with the associated metadata collected over the 10-year period. Conservative public safety critic **Tony Clement** wondered why CSIS was keeping the data in question at all. **Coulombe said the law dictates that CSIS must hang on to any data used in criminal or administrative proceedings**. As a result, the agency is going through the material to see what it needs to keep. ``**So before we rush and destroy that information, we have to make sure that by destroying it we're not going to be contravening another court decision,'' Coulombe said.** ``**We have to take the time to do that analysis.''**

2-**Public Safety Minister Ralph Goodale has rebuked a Canadian spywatcher for publicly suggesting Edward Snowden "should be shot."** "That remark strikes me as highly inappropriate," the minister told reporters in Ottawa yesterday. He was not the only person offended. From Russia, the famous fugitive American at the centre of the comment also found it disturbing, *Globe and Mail Online* writes. **"Canadian spy, charged with keeping spies from breaking the law, wants man dead for showing spies broke law,"** read a Tweet from Mr. Snowden on his verified account. He then added wryly, "Bonus: he's mad he was recorded." When a member of the audience asked Mr. Doucet what Mr. Snowden's fate would have been had he been Canadian and leaked intelligence secrets, he replied: "**Do you want my opinion on that? Do you really want it? I'll give it to you. If Edward Snowden had worked for CSIS and did what he did, he should be shot."**

Canada

3-*CBC News* reports that **Canada has quietly imposed additional sanctions on Russian nationals over the annexation of Crimea and Moscow's ongoing support for separatists in eastern Ukraine**. The new measures, including **asset-freezing** and a **prohibition on business dealings**, were passed by the Liberal cabinet on Nov. 28 and released, without much fanfare compared with the former Conservative government, on the Global Affairs Canada website the same day. **Russian Foreign Ministry spokeswoman Maria Zakharova says her country regrets Canada's decision and "this unfriendly action" will not go unanswered.**

International

United States / États-Unis

4-President-elect **Donald Trump** is receiving an average of **one presidential intelligence briefing a week** reports *Reuters,* **far fewer** than most of his **recent predecessors**. In contrast, **Mike Pence**, Trump's vice president-elect, has been getting his own classified President's Daily

Brief at least **six days a week**. Writing in *USA Today,* **Senators Ben Cardin and Dianne Feinstein** said **Trump's apparent lack of interest** in intelligence briefings is **"particularly troubling"**.
5-The **U.S. military** believes that approximately **50,000 Islamic State fighters** (a **"conservative estimate"**) have been **killed** since the United States started battling the extremist group more than two years ago. (Extensive coverage / vaste couverture)
6-**Georgia's Secretary of State Brian Kemp** has dispatched a **letter** to **Department of Homeland Security Secretary Jeh Johnson** asking the **DHS** to **explain** what appears to be an **attempted breach** on **November 15** of the **state's computer systems** that house its **voter registration database** by someone with an **IP address associated** with the **DHS** reports the *Wall Street Journal.*

United Kingdom / Royaume-Uni

7-Delivering an **'unprecedented' speech** from **MI6 headquarters** in London, director **Alex Younger** warned a **highly organized Islamic State cell** in **Syria** is **actively planning attacks against Britain** and its **allies.** Younger indicated the **Secret Intelligence Service has infiltrated Isis** and **helped MI5** and the police to **identify** and **stop threats** to the UK and elsewhere. Younger said that the **scale** of the **threat from terrorism** is **unprecedented** and issued a warning about the **"increasingly dangerous phenomenon"** of **hybrid warfare**, such as **cyber attacks** and **propaganda operations** by hostile countries such as **Russia.**"The risks at stake are profound and represent a fundamental threat to our sovereignty," he said. (Extensive coverage / vaste couverture)

Africa / Afrique

8-*Reuters* reports there was **no immediate claim of responsibility** for a **bomb blast** at a **security checkpoint** in **Cairo** this morning which **killed six police officers** and wounded three others.
9-**International Criminal Court judges**, reports *Reuters,* have asked **South Africa** to **send representatives** to a **hearing this coming April** to determine whether it **breached its obligation** to **arrest Sudan's President Omar Al Bashir** in June.
10-Selon *Le Monde,* la **surveillance des employés permet d'accéder au réseau interne des opérateurs téléphoniques Parmi les cibles du -Government Communications Headquarters (GCHQ), l'agence de -renseignement technique britannique**, ils côtoient trafiquants d'armes, leaders politiques du Moyen-Orient et chefs de groupuscules terroristes. Leur tort? Travailler pour un opérateur de téléphonie. Un document du 10 juin 2009, intitulé " Réseau intranet Zain ", décrit les tests menés par le GCHQ sur un flux satellitaire -faisant transiter des communications internes à l'opérateur -téléphonique Zain. Basé au Koweït, il est présent dans huit pays, essentiellement au Moyen-Orient. En 2010, **Zain a vendu ses activités dans ces pays à l'indien Bharti Airtel, troisième opérateur mobile mondial. Mais, à l'époque des documents, il est très présent en Afrique et opère encore dans quinze pays, du -Burkina Faso au Niger en passant par l'Ouganda et le Tchad.**

Middle East / Moyen-Orient

11-The *Jerusalem Post* reports that the **Shin Bet (Israel Security Agency)** announced on Thursday that security forces have foiled a **Hamas plan to carry out terrorist attacks** and kidnappings in order to negotiate a prisoner swap.
12-*The National (UAE)* reports that **ISIL has called for its followers to launch attacks** on Bahrain, including on American military personnel stationed in the country ahead of a visit by the US defence secretary.

Afghanistan/Pakistan

13-The *International News* reports that the **United States** on Thursday told Pakistan they were concerned about **"safe terror havens"** being provided to the Afghan Taliban groups such as the Haqqani Network.
14-*Pajhwok Afghan News* reports that **Russia contacted Taliban** to encourage them to join the peace process in Afghanistan, the country's envoy to Kabul said on Thursday.

Europe

15-*Le Monde* rapporte que Londres et Washington aident Paris à libérer ses ressortissants et agissent, en coulisses, pour l'empêcher de payer. La France ne compte pas que sur elle-même pour libérer ses ressortissants des mains de ravisseurs à l'étranger. Elle s'appuie souvent sur les Etats-Unis et le Royaume-Uni. Mais de nouveaux documents extraits par *Le Monde* , en collaboration avec le site The Intercept montrent que cette coopération n'est pas aussi loyale qu'on pourrait le croire, malgré la sensibilité du sujet. Dans d'autres lettres internes du GCHQ les **Britanniques se félicitent de leur efficacité dans la libération d'un otage français, Antoine Falsaperla. Enlevé le 23mai 2009 au Pakistan,** il est libéré trois mois plus tard. Les services secrets français **(Direction générale de la sécurité extérieure, DGSE) ont demandé l'intervention du GCHQ pour des interceptions et des géolocalisations.**
16-**L'hébergeur français OVH, qui défend une approche libérale de la liberté d'expression, avait été tancé par l'ONU et Paris Politique ou économique, la surveillance pouvait aussi avoir un but technique C'est un pseudonyme bien connu des informaticiens. « Oles » figure dans une liste de cibles des services de renseignement britanniques,** extraite par *Le Monde*, en collaboration avec le site *The Intercept*, des archives de l'ancien consultant de **l'Agence nationale de sécurité (NSA) américaine Edward Snowden, confiées à Glenn Greenwald et Laura Poitras. « Oles », pour l'état civil, c'est Octave Klaba, le fondateur d'OVH, le plus grand hébergeur de sites Internet d'Europe.** Son adresse e-mail figure dans un document émis par les services de renseignement britannique (GCHQ), parmi d'autres « sélecteurs » – des personnes identifiées comme des cibles par les **services de renseignement américains, canadiens, néo-zélandais, britanniques et australiens, au sein de leur alliance, les « Five Eyes »** indique *Le Monde.*

Australia, New Zealand / Australie, Nouvelle-Zélande

17-The **Chinese ship assigned to search for Malaysia Airlines Flight MH370 has sailed for home**, months before completing the hunt and soon **after being exposed by security experts as probably spying on the side**. The **Australian Transport Safety Bureau** yesterday said the **Dong Hai Jiu 101** had this week stopped looking for MH370 in the southern Indian Ocean and would return to Shanghai after dropping off an underwater search robot in Fremantle. As revealed by The *Australian*, since its deployment to the MH370 project in February, **the Chinese vessel has spent very little time in the target zone actually searching for the aircraft.**
18-It took the jury just over a day to find **Ali Al-Talebi**, 27, **guilty of two counts of supplying funds to IS and one charge of knowingly making those funds available to them**, marking the first time charges of **providing material support for a terrorist group** have been tested and successfully prosecuted in an Australian court, since terrorism legislation was introduced in 2003, the *Australian Broadcasting Corporation* reports.

Asia / Asie

19-The *Press Trust of India* reports that the **Federal Bureau of Investigation** of the U.S. is set to interrogate arrested Islamic State (ISIS) and **Jamaat-ul-Mujahideen** Bangladesh (JMB) terrorist **Mohammed Musiruddin** alias Musa, an NIA official said here on Thursday.
20-The *Gulf News* reports that Philippine authorities on Thursday recovered an **improvised explosive device (IED)** in Bulacan, nearly two weeks after another bomb placed near the **US Embassy** last was discovered.

21-According to *Kyodo News*, South Korea's opposition-controlled parliament **voted to impeach** President **Park Geun Hye** on Friday over a **corruption and abuse-of-power** scandal implicating her and her longtime close friend. The motion, which needed 200 votes to pass, was approved at a plenary session of the National Assembly, with 234 of its 300 members voting in favor and 56 against.
22-North Korea on Friday **denied its involvement in a hacking attack against South Korea's military**, saying Seoul is pulling off "a childish plot" to divert public attention from its political crisis. South Korea accused North Korea this week of being behind the **first infiltration of the intranet of its cyberwarfare command** in August, noting that the Internet Protocol address linked to the attack was traced to a **location in China that was previously used by North Korean hackers**. North Korea's main propaganda website, **Uriminzokkiri**, rebuffed the claim, saying hackers never make the mistake of exposing their IP addresses or methods, which could risk revealing their identities, *Yonhap News Agency* reports.
23-According to the *Xinhua News Agency*, the third China-U.S. ministerial dialogue on fighting **cyber crimes** and other related affairs issued Thursday a list of positive fruits as the **two sides worked hard to strengthen cooperation in cybersecurity**. The dialogue was co-chaired by China's State Councilor and Minister of Public Security **Guo Shengkun** with U.S. Attorney General **Loretta Lynch** and Secretary of Homeland Security **Jeh Johnson**. During this round of dialogue, **both sides endorsed the establishment of the dialogue mechanism as beneficial to bilateral communication and enhanced cooperation,** and both regarded further **solidifying, developing, and maintaining the dialogue mechanism as beneficial to mutual interests.**

Americas / Amériques

Light coverage. / couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Friday, December 23 2016
le vendredi 23 décembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

No mentions in the mainstream media / Pas de mentions dans les médias traditionnels.

Canada

1- *Radio-Canada - Télévision* (Ottawa) rapporte que des documents révèlent que des **dizaines d'agents de la Gendarmerie royale du Canada (GRC) se sont servis de bases de données policières pour chercher des informations sur la vie privée de Canadiens sans autorisation.** Selon des documents obtenus grâce à la Loi sur l'accès à l'information, de 2010 à 2015, 62 agents de la GRC se seraient servis sans permission de bases de données policières pour fouiller dans la vie privée de proches ou de citoyens. En 2015-2016, le **Commissariat à la protection de la vie privée du Canada a reçu 107 plaintes contre la GRC, incluant 12 alléguant une atteinte à la vie privée.**

International

United States / États-Unis

2- In an interview with *NPR,* CIA director **John Brennan warned against tit-for-tat retaliation** by the **U.S. government** for **Russian hacking** during the election. "I don't think we should resort to some of the tactics and techniques that our adversaries employ against us," said Brennan. "I think we need to remember what we're fighting for. We're fighting for our country, our democracy, our way of life, and to engage. And the **skullduggery** that some of our opponents and adversaries engage in, **I think is beneath this country's greatness."**
3- **Citing classified U.S. intelligence** to **support its conclusion, newly declassified passages** from a **House Intelligence Committee report** on **Edward Snowden** assert that **since arriving in Moscow** the former NSA contractor **"has had, and continues to have, contact with Russian intelligence services."** Minutes after the report was released Thursday, **Snowden's chief lawyer, Ben Wizner** called the report **"petulant nonsense." Snowden responded** it was**"rifled with obvious falsehoods"** and presented no evidence that his disclosures were made "with harmful intent, foreign influence, or harm". (Extensive coverage / vaste couverture).
4- The **U.S. government**, reports *Politico,*has quietly began **requesting** that **select foreign visitors** entering America on the **visa waiver program**, provide their **Facebook, Twitter** and **other social media accounts**, a move designed to spot potential **terrorist threats.**

United Kingdom / Royaume-Uni

5- Speaking to the *BBC,* **former MI6 director Richard Barrett** said there are **550 "really extreme potential terrorists" in Germany** and with a total of approximately **7,000 "live cases"** that's almost "an **impossible number to control"**.
6- **Four** of the **six people arrested 10 days ago** suspected of **planning a terrorist attack remain** in **custody** reports the *Independent.* The alleged **targets**, said security sources, were **one or more shopping centers** crowded in the run-up to Christmas.

Europe

7- **Italy** has announced that **"without a shadow of doubt"**, Berlin attack suspect **Amis Amri** was **killed this morning in Milan. Italian Interior Minister Marco Minniti** said Amri was was **stopped** by **two policemen** at approximately 3 a.m.local time **in front** of the **Sesto San Giovanni train station, north of Milan**. When **asked for his identification papers, Amri pulled a gun**, reportedly **yelled "Allahu Akbar"**, and **shot one of the two policemen,** lightly wounding him in the shoulder. Amri, in turn, was then **shot dead.** A rail ticket found on Amri's body indicated he had traveled by high speed train from France to the northern Italian city of Turin. He then caught a regional train to the Milan suburbs. **Italian authorities identified Amri** on the basis of **fingerprints** of the suspect **previously taken in Italy** where he served four years in prison. (Extensive coverage / vaste couverture).
8- D'après l'*Agence France-Presse,* **l'auteur présumé de l'attentat au camion-bélier de Berlin a été abattu dans la nuit de jeudi à vendredi à Milan** lors d'un contrôle de la police italienne, mettant fin à une chasse à l'homme en Europe de quatre jours. L'homme tué par la police est "sans l'ombre d'un doute" l'auteur présumé de l'attentat sur le marché de Noël de la capitale allemande, ayant fait 12 morts, à savoir le **Tunisien Anis Amri, a indiqué à Rome le ministre italien de l'Intérieur, Marco Minniti.** Son arrestation a été effectuée par une patrouille de deux policiers alors qu'il circulait de façon "suspecte" devant la gare milanaise de Sesto San Giovanni.
9- Acting on a **tip** from the **BfV**, **two brothers born in Kosovo,** ages 28 and 31, were **arrested** this morning by special forces in the **German city of Duisburg** on suspicion they planned to **bomb** the **Centro shopping mall in Oberhausen**, one of the largest shopping centers in the country. (Extensive coverage / vaste couverture).
10- **"Laughable"** was the word **Russia used** to describe an assertion by the **Lithuanian government** that the **Kremlin** is **responsible** for a series of **cyber-attacks** on its **state computer systems** during the past two years reports *Reuters.*

Africa / Afrique

11- An **Airbus carrying 118 passengers** on a **domestic flight** in **Libya** has **landed** in **Malta** after being **hijacked** by a **"pro Gaddafi" man** claiming to have a **hand grenade** reports *Reuters.*
12- Negotiations are continuing but the **Nigerian government denied** a report in the media that a **further 21** of the **kidnapped Chibok schoolgirls** have been **released** reports the *Guardian* (Nigeria).
13- Selon *Espace Manager,* (Tunisie) le terroriste, **Moez Fezzani, présumé impliqué dans les attentats du Bardo et de Sousse, sera probablement, remis aux autorités sécuritaires tunisiennes** dans un très proche avenir par l'Etat soudanais qui l'a arrêté, il y quelque temps sur son territoire. Le terroriste en question est également réclamé par la Grande Bretagne et, surtout, par l'Italie, mais il semble que les **services sécuritaires tunisiens sont les mieux placés pour le récupérer après avoir obtenu l'extradition de sa femme et ses enfants revenus à Tunis** après une escale en Egypte.

Middle East / Moyen-Orient

14- The *Times of Israel* reports that **Israeli security agents busted a 20-member Hamas cell** that was plotting suicide bombings and shootings against Israeli citizens in major Israeli cities, including Jerusalem and Haifa, the **Shin Bet** disclosed on Thursday.
15- *The National (UAE)* reports that the **Syrian army** said Thursday that it had retaken complete control of Aleppo after the **last rebel fighters were evacuated from the city**, handing President Bashar Assad his biggest victory of the war.

Afghanistan/Pakistan

16- The *Pakistan Dawn* reports that **Lt Gen Naveed Mukhtar** called on Prime Minister Nawaz Sharif, in the first such visit since his appointment as **chief of Inter-Services Intelligence (ISI)** earlier this month, a statement from the Prime Minister's Office said.

Australia, New Zealand / Australie, Nouvelle-Zélande

17- Four alleged would-be terrorists are behind bars after **police foiled a "horrendous" Christmas Day plot** in Melbourne, with authorities now confident Victorians can safely celebrate the festive season. Police allege an **Islamic State-inspired "cell"** planned to use explosives and weapons to attack Flinders Street Station, Federation Square and St Paul's Cathedral on Christmas Day. Victoria Police Chief commissioner **Graham Ashton** warned a **"substantial number"** of people could have been killed or injured in the attack, while **Australian Federal Police** commissioner **Andrew Colvin** revealed the plot concerned him **"more than any other event that I've seen"**. Three men arrested in raids by heavily armed police across the northern suburbs overnight **faced court on Friday afternoon.** A fourth man has been charged, remanded and is expected to face Melbourne Magistrates Court on Saturday morning. Two other men and a woman were arrested but released without charge, reports the *Australian Associated Press*.

Asia / Asie

18- The *Malay Mail* reports that a fugitive in India, controversial **Islamic preacher Dr Zakir Naik** is free to travel in Malaysia because he is not on the terror list here, Datuk Nur Jazlan Mohamed said. The Salafist preacher has also been banned from several countries like **Bangladesh, Canada and the UK**.

19- The *Times of India* reports that six months after the **National Investigation Agency (NIA) busted an ISIS module** in Hyderabad, the agency on Thursday filed a chargesheet against 8 members including their leader **Mohammad Ibrahim Yazdani**.

20- Hong Kong is seeking to catch up with **tougher international anti-terrorism rules** with the government **proposing legislative amendments** to fast track the **freezing of terror suspects' assets** by avoiding lengthy notification procedures, reports the *South China Morning Post.*

However, veteran Democratic Party lawmaker and security monitor **James To Kun-sun** warned yesterday of **"the devil in the details"** as he argued that **without clearly defined terms there could be hidden grey areas leading to unrelated parties being incriminated.** Under the proposed changes to the **United Nations (Anti-Terrorism Measures) Ordinance**, any person or entity would be prohibited from dealing with assets owned by a terrorist or terrorist's associate once they are gazetted under the law, unless they are under the authority of a licence granted by the security minister.

Americas / Amériques

Light coverage / couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Wednesday, August 19, 2015
le mercredi 19 août 2015
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1-As a **Canada's spy watchdog investigates** allegations **CSIS spied on environmental groups** — a former member says it's **not fair to call the proceedings "secret hearings."** Ex-**"Security Intelligence Review Committee"** member **Shirley Heafey** says once hearings wrap, any information that doesn't violate national security will be made public. And she says CSIS will need to prove why information **should *stay* secret**, Vancouver's *News Talk 980 CKNW* reports.

Canada

2-A lawyer who was **suspended last spring from the federal security roundtable** has just received a **letter of appreciation** from the government, reports the *Canadian Press.* In the letter, Public Safety Minister **Steven Blaney** and Justice Minister **Peter MacKay** thank **Hussein Hamdani** for his decade of work on the Cross-Cultural Roundtable on Security. There is no mention of the Hamilton, Ont., lawyer's suspension from the roundtable following a media report alleging links to extremism - accusations Hamdani flatly denies.
3-The *National Post* writes that the **Canadian government's attempt to deport two Pakistani citizens** arrested in **Toronto for terrorism is lagging**, and the lawyer for one of them said Tuesday **Pakistan was refusing to take his client back. Jahanzeb Malik and Mohammed Aqeeq Ansari** were to be deported more than a month ago, but their departure was put on hold at Pakistan's request.

International

United States / États-Unis

4-**Senior U.S. intelligence** and **law enforcement officials** have disclosed to *Bloomberg View* that the **window** for **Edward Snowden** to reach a **plea agreement** with **Justice Department is closing quickly.** Columnists Eli Lake and Josh Rogin have learned that any **momentum** for these negotiations is **gone**; Snowden's lawyers have not even had conversations about such a deal for **nearly a year** with the U.S. attorney prosecuting the case. The officials say **the chance that Snowden will be offered a plea deal** in exchange for cooperation is now **close to non-existent.**
5-**Local law enforcement agencies** are buying **cellphone-tracking equipment** that is **cheaper and smaller** than earlier systems, according to documents reviewed by the *Wall Street Journal*, but it **isn't always clear whether court orders are needed** to use the devices.

United Kingdom / Royaume-Uni

6-A **forensic analysis** by two British researchers of ***Guardian*** **laptops ordered destroyed** by **British intelligence** reveal the **GCHQ** was **very meticulous** in just how the computers, which had contained **Edward Snowden's trove of files**, be handled reports the *Washington Times.* "They were very precise," said researcher Richard Tynan. "They came in with their shopping list and said, 'Drill this chip; turn it over; drill that chip.'"

Africa / Afrique

7-**Human Rights Watch** leveled **harsh criticism** at **Egypt's new anti-terrorism law** this morning reports the *Voice of America,* saying the measure has an **overly broad definition** of what **constitutes a terrorist act** and leaves Egyptians open to stiff sentences for things that may amount to "civil disobedience."
8-*African Manager* rapporte que selon des informations tirées du quotidien Al Chourouk, **près de 300 cellules terroristes dormantes existent en Tunisie**. Les éléments de ces cellules sont répartis sur la capitale et les autres régions de la Tunisie. Près de 60% des membres de ces cellules auraient annoncé leur **appartenance au mouvement terroriste Deach**. Il appert que ces individus ont eu des **cours d'entraînement et de combat en Libye** et projettent commettre des **opérations terroristes en Tunisie.**

Middle East / Moyen-Orient

9-Yemeni Houthi leader **Abdul Malik Al-Houhi** issued directives on Sunday calling on senior commanders to **implement a state of emergency** in different parts of Yemen, including the group's northern stronghold of Saada Province, activists and residents told *Asharq Al-Awsat.*

Afghanistan/Pakistan

10-The *Gulf News* reports that in an ongoing wave of law enforcement encounters with terrorists and outlaws at least **two local commanders of Al Qaida** were gunned down and a **senior intelligence official** killed.
11-**Suspected militants on Tuesday kidnapped four judges**, including the appellant court chief, in northern Sar-i-Pul province, police told the *Pajhwok Afghan News*.

Europe

12-Light coverage / couverture légère.

Australia, New Zealand / Australie, Nouvelle-Zélande

13-The *Australian* writes that a Melbourne man, **Hassan El Sabsabi**, 24, of **Seabrook**, will stand trial for **allegedly sending thousands of dollars to an American man who travelled to the Middle East to fight with a terrorist organisation.**
14-**Canada's Prime Minister** wants to **follow Australia's lead** and make it a **crime for his nation's citizens to visit designated areas abroad that are under terrorist control**, *The Australian* writes. He has announced that if his Conservative government were re-elected, it would create a new category of **banned foreign travel zones within foreign countries where listed terrorist entities such as Islamic State operate and where they are recruiting and training followers**. The Canadian move apparently followed discussion about Australia's declared areas legislation during a meeting of the "**Five Eyes" intelligence-sharing alliance made up of the US, Britain, Australia, Canada and New Zealand.**

Asia / Asie

15-The *Times of India* reports that the **National Investigation Agency (NIA)** on Tuesday released the sketches of **two suspected LeT terrorists** who infiltrated India along with Udhampur attacker Mohammed Naveed but are absconding.
16-**North Korea** repeated its demand yesterday for **South Korea and the United States to suspend their ongoing joint military drills**, calling them a "blatant" provocation **against the North**. South Korea and the U.S. kicked off their annual joint military drills on Monday, which **Pyongyang has denounced as a war rehearsal** for an **invasion of the North**, *Yonhap News Agency* reports.
17-Police yesterday were still hunting for a **man in a yellow T-shirt** who was captured by a **security camera** putting his **backpack under a bench** at the **Erawan Shrine** and leaving the scene shortly **before the deadly bomb exploded** on Monday night, *The Nation* reports.

18-**Security experts** say Monday's deadly blast in **downtown Bangkok** does not fit the **pattern of operations of known groups in Thailand**. The groups include **southern Malay-Muslim separatists and radical political "red shirt" opponents of the military regime**, the *Straits Times* reports.

Americas / Amériques

19-Light coverage / couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Monday, February 15 2016
le lundi 15 février 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

No mentions in the mainstream media. / Pas de mentions dans les médias traditionnels.

Canada

1- After nearly a year and a half behind bars, a **Canadian-Libyan businessman Salim Alaradi** is scheduled to go to trial on Monday in **Abu Dhabi**, in a case that has been scrutinized by a **United Nations human-rights panel because of allegations that he was arbitrarily detained and tortured**. The **Vancouver** resident has pleaded **not guilty to three terror-related charges**, the *Globe and Mail* notes.

2- The **federal Liberals** are open to **restoring funding** for a controversial UN **agency that works with Palestinians and was cut off by the former Conservative government over its alleged ties to Hamas**, **International Development Minister Marie-Claude Bibeau** confirmed Sunday. The Liberals are eyeing a plan to provide $15-million to the Palestinian relief agency, *The Globe and Mail* reported earlier this month. But **B'nai Brith Canada**, a leading Jewish lobby group, said Sunday that it strongly opposes the resumption of funding to UNRWA.

3- *Le Journal de Montréal* rapporte que **Sami Bebawi** est généreux avec ses proches. **Accusé de fraude, corruption et blanchiment d'argent, l'ancien vice- président directeur de SNC-Lavalin** vient de **transférer une quatrième propriété à un membre de sa famille**. Le nouveau cadeau de Sami Bebawi, un condo de plus d'un demi-million $ situé dans cette tour du chemin de la Côte-Sainte- Catherine, est allé à son gendre. Cette fois-ci, c'est le gendre de l'ingénieur déchu qui profite de ses largesses. **Sami Bebawi est accusé d'avoir détourné 34 M$, selon l'accusation, notamment en pots-de-vin au régime de Kadhafi, en Libye.**

International

United States / États-Unis

4- When asked directly by *60 Minutes* whether **Isis is coming to the United States, CIA director John Brennan** replied "I think (the Islamic State) **does want to eventually find it's, it's mark here**... I'm expecting them to try to put in place the operatives, the material or whatever else that they need to do or to incite people to carry out these attacks, clearly. So I believe that their **attempts are inevitable**. I don't think their successes necessarily are."

United Kingdom / Royaume-Uni

5- The **Home Office,** reports the *Guardian,* has admitted it **holds no record** of **British citizens barred from boarding transatlantic flights** despite them being **identified** by **US security officials** as **potential threats** at UK airports.

6- **Dissident republican groups,** such as the **Provisional IRA**, are boasting they have more than a **ton** of **Semtex plastic explosive** that escaped the decommissioning process and could now be used against **mainland targets** reports the *Daily Telegraph.*

Europe

7- Selon *Le Figaro,* le 6 octobre, la **Cour de justice de l'Union européenne a déclaré illégal le système dit « Safe Harbor »** , qui régissait les transferts de données entre les États-Unis et l'Europe. Au travers de cette invalidation, la justice européenne s'est attaquée à l'empire des grandes entreprises américaines du Web, qui hébergent souvent les données de leurs clients européens dans des centres situés aux États-Unis. Trop dangereux pour la Cour, qui a rappelé dans sa décision les **révélations d'Edward Snowden sur la surveillance de la NSA**.
8- Speaking with *Euronews TV,* **Russian Prime Minister Dmitry Medvedev** said Moscow **will not pursue legal action** over the **British accusation** that the **state was complicit** in the **death of Alexander Litvinenko**. "As for any legal action, this is simply ridiculous. We don't need this and the Russian Federation will never sue any country over some **foolish fabrications** or funny films," Medvedev said.

Africa / Afrique

9- Selon *All Africa,* **deux attaques ont été perpétrées le même jour au Mali, soit à Kidal et Tombouctou**. Toutes deux rapidement revendiquées par des groupes islamistes : **Ansar Dine** d'un côté, **Aqmi** de l'autre.

Middle East / Moyen-Orient

10- The *National Iraqi News Agency* reports that **Security Advisor of the Kurdistan region, Masroor Barzani** discussed in Arbil with the **Canadian Ambassador Bruno Saccomani** developments in the war on terrorism and the Canadian aid to Kurdistan province.
11- *The National (UAE)* reports that Turkey shelled a Kurdish militia in northern Syria for a second day on Sunday and **Russia continued to heavily bomb rebel groups**, raising further doubts for a temporary truce.

Afghanistan/Pakistan

12- The *Express Tribune* reports that days after the army claimed to have busted a nexus of the top three militant outfits in Karachi by arresting their senior commanders, **intelligence agencies** on Sunday warned of **possible terror attacks** on key government officials and politicians in Karachi.
13- Afghanistan's newly appointed **ambassador to Pakistan, Omar Zakhilwal** told the *Voice of America* that he's **"very positive"** that **direct peace talks with** the **Taliban** will take place **before the end of this month** with no conditions from either side.

Australia, New Zealand / Australie, Nouvelle-Zélande

14- **Terrorism** is the defining issue of the early 21st century and it has now become an **academic discipline** with more than **5000 Australian students enrolled in anti-terrorism and cyber-security courses**, the *Age* writes. In fact, industry **demand for students with cyber-security expertise is so strong** that the master of **policing intelligence and counter-terrorism** will next year change its name, by incorporating the word **"cyber"**, to emphasise that the course offers training in **cyber terrorism, cyber intelligence and cyber warfare.**
15- *Stuff News News Zealand* writes that **Daniel Mellsop** has been named **New Zealand's next High Commissioner to Canada**. He will be based in **Ottawa** and start late February 2016. Mellsop has 15 years of experience serving New Zealand in various capacities, but the four-year High Commissioner posting in Canada will be the first time he takes the top role. Tasks on his agenda will include business promotion, hosting an ANZAC Day ceremony, discussing **Canada's role in the war against ISIS,** and tourism or education promotion.

Asia / Asie

16- **Abu Sayyaf bandits** are demanding P1 billion for the release of **three foreigners** and the Filipino woman they kidnapped in September last year. **Senior Supt. Roberto Fajardo,**

National Police Anti-Kidnapping Group (AKG) commander, said the victims were abducted on Samal Island, Davao del Norte. Norwegian Kjartan Sekkingstad and **Canadians John Ridsdel and Robert Hall**, and Hall's Filipino girlfriend Maritess Flor were **still being held by the bandits in a still-undisclosed area in Sulu**, the *Business Mirror* reports.
17- **China** won't take part in any coalition **fighting "terrorist groups" in the Middle East**, but will do its fair share in its own way and is **already helping Iraq**, Foreign Minister Wang Yi said. China wants to **develop deeper defence and anti-terrorism ties with the Arab world**, including **joint exercises, intelligence sharing and training**, the government said in a policy document released last month, *Reuters* reports.
18- **Beijing's top representative in Hong Kong** has blamed **radical separatists** for riots that erupted in the Chinese-ruled city almost a week ago, the worst violence since pro-democracy protests paralyzed parts of the Asian financial center in 2014, *Reuters* reports.
19- **North Korean hackers** sent massive amounts of **spam emails to South Korean public organizations** last month, **South Korea's police chief** said today, the latest in a series of **cyberattacks against the South** in recent years, *Yonhap News Agency* reports.
20- The **No. 1 challenge the United States** is facing right now is how to cope with **threats posed by North Korea and China**, Republican presidential runner Marco Rubio said. Rubio made the remark during a Republican presidential candidate debate Saturday night, putting the **North Korean issue** ahead of Middle Eastern problems and tensions with Russia, *Yonhap News Agency* reports.

Americas / Amériques

21- **U.S. State Department cables** obtained by the advocacy organization **Judicial Watch**, provide evidence that **al Qaeda leader Adnan G. el Shukrijumah**, who was **killed by Pakistani forces** in **2014**, **hid in 2004** with two Arab militants in the **northern Mexican border town of Agua Prieta** just across from **Douglas, Arizona** reports the *Miami Herald.*

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Monday, February 29 2016
le lundi 29 février 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- Two days after a terrorist killed a soldier at the National War Memorial and ran into the Parliament Buildings, **Dwayne Boissoneau** logged into **Twitter** to **offer himself up to the Islamic State of Iraq and the Levant**. "Hey brother, I'm ready to fight and support ISIS till death," Boissoneau, 30, wrote to a Canadian ISIL member in Syria who uses the alias **Abu Turaab al-Kanadi**. "I'm a Canadian and I'm sick of the face (fake) politics here." ISIL recruiters apparently believed they had found what they were looking for: a Canadian extremist willing to do what **Michael Zehaf-Bibeau** had done in Ottawa, a simple but headline-grabbing strike from within. They sent him a message on Twitter that said, "Who wants to do something to some top kaffirs (non-believers)?" They said they could get addresses. "Give me Canadian addresses," Boissoneau responded. "I will ensure something happens." The exchange was detected by the **RCMP's Tactical Internet Operational Support Unit** and Boissoneau was arrested for uttering a threat. But the judge who heard the case last month found he was not really a terrorist after all. According to the judge's decision, the man ISIL was trying to recruit is a low-toaverage functioning First Nations man from Longlac, Ont., who suffers from a **childhood brain injury and Fetal Alcohol Spectrum Disorder**, and who did not attend high school. After Boissoneau's arrest, he told police he'd never actually met a terrorist in person and "wasn't that serious about going down there." He said he was going through a rough time and just wanted to **"test the system"** to find out if the **Canadian Security Intelligence Service "can actually detect stuff like that**."

Canada

2- The **RCMP** spent just over **$900,000 in overtime pay** over the course of a five-month undercover operation that led to the arrests of two terrorism suspects in British Columbia. Documents obtained by *The Canadian Press* through a freedom-of-information request show the Mounties paid at least 200 people, mostly police officers, $911,090.54 for overtime work during the investigation, which was code named **Project Souvenir**. The operation culminated in the arrests of common-law spouses **John Nuttall** and **Amanda Korody** on July 1, 2013. They were found guilty last summer of plotting to blow up the B.C. legislature on that Canada Day.

3- A Canadian media outlet squares off against the government Monday in a legal battle that pits media freedoms against the ability of police to investigate terrorism offences. *Vice Media* and its journalist **Ben Makuch** want Ontario Superior Court to quash an order that they hand over **material related to their interviews with a suspected terrorist to the RCMP**, writes *The Canadian Press*. "Courts should be wary of allowing the state to conscript journalists as investigative arms of the police," *Vice* and Makuch state in their factum. A year ago, Ontario court Judge **Jack Nadelle** ordered the online news outlet to hand over materials that Makuch used to produce three articles in 2014 about **Farah Shirdon**, of Calgary, including that he had left Canada to fight for Islamic State. The stories were based on conversations Makuch had with Shirdon via an online instant messaging app called Kik Messenger.

4- *La Presse canadienne* rapporte que le **gouvernement libéral de Justin Trudeau a tranquillement commencé à recueillir des renseignements au sujet des drones** qu'il souhaite

acheter pour les **Forces armées canadiennes** et s'attend à ce que l'industrie de l'armement lui revienne avec des propositions d'ici la mi-avril.

International

United States / États-Unis

5- **NSA deputy director Rick Ledgett** told Washington's *WTOP Radio* that **U.S. intelligence** has **hard proof** that **almost 1,000 foreign intelligence targets**, including terrorists tracked by the U.S., have **changed their communications methods** because they were tipped off by **Edward Snowden's leaks.**

6- **Secretary of Defense Ashton Carter,** reports the *Los Angeles Times,* will **visit a Pentagon outpost** in the heart of **Silicon Valley**, speak at a cyber-security conference in San Francisco and go to **Microsoft** and **Amazon headquarters** in Seattle **this week** to highlight the risks of **cyber-attacks** and the need for **greater digital cooperation** with the Pentagon.

United Kingdom / Royaume-Uni

7- Concerned about several **privacy** and **surveillance** provisions contained within the **Investigatory Powers Bill**, a revolt **against** the legislation by **Conservative backbenchers** is anticipated reports *The Times of London.*

8- *The Times* is also reporting that the **National Crime Agency** is complaining that **technology companies** are **routinely blocking law enforcement requests** for **communications information** in serious cases such as the importing of firearms, human trafficking, fraud and **money laundering.**

Europe

9- Selon *Le Monde,* si la **DGSI ne manquait pas d'informations sur les tueurs de " Charlie Hebdo ", elle n'a pas su les analyser** L'abondance des données collectées sur les **frères Kouachi** entre 2010 et 2013 confirme que ces deux " objectifs " ont fait l'objet d'un travail sérieux en raison de leur connexion établie avec " la mouvance terroriste " . La défaillance se situe ailleurs, dans l'analyse qui a été faite de ces informations. **Après deux ans d'écoutes, la DCRI met un terme au suivi** des frères Kouachi au motif qu'il n'a pas permis de " détecter d'éléments relatifs à la préparation d'une action violente " ni " de matérialiser des éléments permettant l'ouverture d'une enquête -judiciaire " . **Ces deux arguments soulignent les limites du système français.** La DGSI est une agence hybride, à la fois service de renseignement et de police judiciaire. L'arrêt de la surveillance des Kouachi au motif qu'elle n'a pas permis l'ouverture d'une enquête est révélateur de ce mélange des genres : la mission judiciaire de la DGSI a pris le pas sur le renseignement pur, la matérialisation d'une infraction sur l'interprétation des signaux faibles.

10- *Le Soir,* (Belgique), se demande si **l'enquête menée sur Salah Abdeslam en 2015 a-t-elle été menée dans les formes?** Le 7 mars, **le Comité P** se penchera à huis clos sur la manière dont les **services de renseignement et la police ont alors travaillé**. Au lendemain de l'assaut de Verviers, qui a débouché le 15 janvier 2015 sur la mort de deux djihadistes, **Sofiane Amghar et Khalid Ben Larbi, les policiers molenbeekois, se sont intéressés aux Abdeslam. Salah et Ibrahim ont été auditionnés.** S'étaient-ils radicalisés ? Comptaient-ils partir en Syrie pour se battre dans les rangs de l'Etat islamique, comme on le prétendait alors dans le quartier ? **Auditionné le 28 février, Salah Abdeslam ne lâchera rien, sinon que lui et son frère connaissent Abdelhamid Abaaoud**.

11- A comprehensive study of **31 European countries** by the **Royal United Services Institute, Chatham House**, the **Institute for Strategic Dialogue** and the **University of Leiden** in the Netherlands reports the *Guardian* (UK), has concluded while **Islamist plotters** are given **full**

attention, individuals and small groups of **right wing extremists** are in fact **more lethal**, **almost as numerous**, and **much harder to detect by security services**.

Africa / Afrique

12- **Security** has been **beefed up** in **major airports** in **Kenya** following intelligence reports on Sunday evening of **impending attacks** by **al Shabaab** reports the *Star* (Kenya).
Isis has used **female fighters** and a **woman suicide bomber** in **western Libya** reports *The Times of London,* a **first** for the jihadists.
13- Selon *Yabiladi.com*, (Maroc), **l'armée algérienne a procédé à l'arrestation de neuf Marocains soupçonnés de vouloir rejoindre Daesh en Libye, indique le ministère de la Défense** dans un communiqué relayé par la presse locale.

Middle East / Moyen-Orient

14- *Al Jazeera* reports that the **Canadian government's plan to repeal citizenship-revocation laws** has been welcomed by civil liberty groups in the country.
15- *The National (UAE)* reports that gunmen killed **Col Adham Mohammed Al Ga'ari, Aden's deputy chief of intelligence** in the latest assassination targeting high-ranking officials in Yemen's southern port city.
16- While the UN **Security Council approved the "cessation of hostilities"** agreement in Syria which came into effect at midnight yesterday, a White House official told *Asharq Al-Awsat* about the details of a plan B that the United States has talked about in the event that the truce failed.

Afghanistan/Pakistan

17- The *Pajhwok Afghan News* reports that an arms depot containing **"Iranian-made"** ammunition and explosives has been discovered in central Bamyan province, an **intelligence official** claimed on Sunday.

Australia, New Zealand / Australie, Nouvelle-Zélande

18- The number of **Australians** being **hauled off planes by counter-terrorism units on national security grounds has risen to an average of almost two a day**, it has been revealed. And in a trend that is of concern to **security and intelligence agencies**, the number of those among them suspected of trying to reach the **Middle East and join terrorist groups is also on the rise**. Figures obtained by *The Courier-Mail* reveal that since the **counter-terrorism units (CTUs)** were deployed to major airports in August 2014, there had been 652 "offloads". **ASIO Director-General Duncan Lewis** told a Senate Estimates hearing the number of passports being cancelled was also "ticking" up every day.**The number is now more than 160.**
19- Almost **half a million dollars in cash** has been seized at **Melbourne airport** in three weeks amid suspicions of **links to the financing of terror groups**. The *Courier Mail* writes that a combined taskforce of Australian law enforcement officers detected more than $400,000 in undeclared excess currency at customs late last year and the seizure of items, including one crossbow and two electronic shock devices.

Asia / Asie

20- **China's ruling Communist Party** has **expelled two senior officials** in the **violence-prone far western region of Xinjiang for corruption** and transferred them to prosecutors, an **anti-graft watchdog** said. **China** has jailed dozens of senior officials since **President Xi Jinping** launched a sweeping campaign against deep-seated graft after assuming office three years ago. In June, authorities announced an investigation over **serious discipline violations**, a euphemism for **corruption**, into **Alimjan Maimaitiming**, 56, a **former secretary general in the government of Xinjiang**, home to many of **China's ethnic Muslim Uighurs**, *Reuters* reports.

21- An **American student held in North Korea** since early January was detained for trying to steal a **propaganda slogan** from his Pyongyang hotel and has confessed to **"severe crimes" against the state**, the **North's official media** said today, *Reuters* reports.
22- The *Press Trust of India* reports that **Delhi Police** is likely to rope in **cyber cell** to trace the numbers from which CPI(M) general secretary Sitaram Yechury claimed to have received multiple threat calls and messages and will take strict action, a senior officer said on Sunday.

Americas / Amériques
Light coverage / couverture légère

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Friday, March 18, 2016
le vendredi 18 mars 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1-In an *Ipolitics* op-ed, Michael Harris writes: When **Ralph Goodale** and **David McGuinty** headed to the UK and France last January to get ideas about overseeing national security issues in Canada, it seemed like an intelligent thing to do. But did our public safety minister and his MP colleague go to the wrong place? The Liberals, after all, are trying to amend **Bill C-51**, a controversial piece of anti-terrorism legislation that Canadians don't like. No wonder. What's to like about a government—sanctioned police state law? Under Harper-era legislation, the **Canadian Security Intelligence Service (CSIS)** was empowered to operate outside the Charter of Rights, which gave it authority to violate citizens' constitutional rights. And Canada's cyber intelligence agency, the **Communications Security Establishment (CSE)** was allowed to conduct mass collection of information on Canadians without a specific target. Based on their attitudes towards mass surveillance, Britain and France are hardly the countries to help Canada rein in the excesses of Bill C-51. According to a **YouGov survey** of 15,000 people reported this week by **Amnesty International**, citizens of Britain, France and the Philippines were most comfortable with government eavesdropping. Britain was one of three countries out of 13 surveyed where more people favoured surveillance of all people — British citizens, foreigners, and foreign countries, than favoured monitoring none of them.

2-It was supposed to be **Prime Minister Justin Trudeau's** weak point, but according to an **Angus Reid Institute survey**, Canadians think his **Liberals are doing a good job handling national security and terrorism -** and his plans to amend the Conservatives' controversial **antiterror bill appear to have found a political sweet spot,** *the Globe and Mail* writes. The law widened the definition of **national security threats**, **expanded sharing of information held by government departments**, and gave **the Canadian Security Intelligence Service broad new powers to disrupt threats and even, with a judge's warrant, break the law**. And while they rate the Liberals highly on dealing with terrorism, respondents disagree with a symbol of Mr. Trudeau's approach: the move to repeal the Tory bill that strips Canadian citizenship from convicted terrorists.

Canada

3-*TVA Nouvelles* rapporte qu' **Adil Charkaoui doit comparaître aujourd'hui à Montréal pour faire face à des accusations de voies de fait et d'agression armée** à la suite d'une altercation avec un agent de sécurité du Collège de Maisonneuve. S'il est reconnu coupable, il risque quelques mois de prison ou une amende.

4-A British Columbia man convicted in the **Air India bombing deaths of 331 people has been denied his request to participate in political matters.** "Your associations with others of a similar mindset were directly risk-related and led to the murders of many innocent people," the Parole Board of Canada said in a ruling against **Inderjit Singh Reyat**. The board said in its decision released Thursday that it considered comments by Mr. Reyat's lawyer about his client's rights under the charter to participate in political issues. Mr. Reyat became eligible for statutory release in January after serving two-thirds of his nine year sentence for perjury at the trial of two other men charged in Canada's worst mass murder 30 years ago. The board also imposed a second

condition for Mr. Reyat to not associate with anyone involved in political or criminal activity or extremist views, reports the *Canadian Press*.

International

United States / États-Unis

5-He has no doubt **more Snowden documents** will be **released** but **NSA deputy-director Rick Ledgett** told *NPR* that the **classified information** contained therein is **getting old,** technology is changing fast and the **Agency has adapted** to these **changes.**
6-**"We get that," Apple CEO Tim Cook** mused to *Time Magazine* on the fact that **encryption** can **protect terrorists** as well as law abiding citizens. "**But you don't take away the good for that sliver of bad**. We've never been about that as a country. We make that decision every day, right? There are some times that freedom of speech, we might cringe a little when we hear that person saying this and wish they wouldn't. This, to us, is like that. It's at the core of who we are as a country."

United Kingdom / Royaume-Uni

7-Statistics from the **Home Office** reveal a **record number (16)** of **teenagers** under the age of 18 were **arrested** for **terrorism offenses last year**, up from **10** in 2014. Additionally, reports the *Daily Telegraph,* the number of **females** detained **increased by 50 per cent** to 45 in 2015.

Africa / Afrique

8-Once focused on **taking hostages** for **ransom** and **striking military targets** in **West Africa, al Qaeda** has switched its strategy in the region to **'soft targets'** reports the *Los Angeles Times.* "It's almost a symbolic reminder that this is a **serious force** to be reckoned with," said **Paul Rogers, a terrorism analyst** at the University of Bradford in England, describing al Qaeda's recent attacks and its fight for relevance. "It doesn't have the capacity to take on military forces head on, so it's **concentrating on soft targets with high impact."**
9-Selon *l'Agence de Presse Africaine,* **AL-Qaïda au Maghreb Islamique (AQMI) a publié des photos qu'elle attribue aux trois auteurs de l'attaque terroriste.** Dans un communiqué rapporté par l'Agence de surveillance des sites islamiques (SITE), AQMI a affirmé que les deux premiers auteurs des attaques, qui ont fait 19 victimes selon un dernier bilan, sont **Hamza Al-Foulani et Abou Adam Al-Ançari du groupe Al-Mourabitoune, dirigé par Mokhtar Belmokhtar** et le troisième auteur, **Abderrahmane Al-Foulani de l'Emirat du désert, dirigé par Abou Al-Ahamam.**
10-*African Manager* rapporte que mercredi soir à **Béja en Tunisie, une patrouille de la police a fait une descente musclée dans la Grande mosquée** située au centre de la ville, après avoir encerclé le bâtiment. **Cinq suspects ont été cueillis dans la mosquée par les éléments de la sécurité**. D'après les informations recueillies, la même source indique que **deux d'entre eux étaient recherchés par la brigade de lutte contre le terrorisme d'El Gorjani alors qu'un autre individu est interdit de voyage.**

Middle East / Moyen-Orient

11-The *Jerusalem Post* reports that **Meir Dagan, head of the Mossad from 2002-2011**, died on Thursday at the age of 71 following a long battle with cancer.
12-The *Fars News Agency* reports that over **4,000 Saudi mercenaries, including 178 commanders**, have been killed during the year-long Riyadh-led war against Yemen, a **Yemeni intelligence source** said on Thursday.

Afghanistan/Pakistan

13-The *Pakistan Dawn* reports that the **Pakistan Foreign Office** said that efforts to arrange direct talks between the **Afghan government and Taliban** were continuing despite insurgents' refusal to participate in the dialogue.
14-The *Pajhwok Afghan News* reports that a **senior intelligence official** on Thursday said the **Islamic State or Daesh militants** would likely to look for finding a hideout in eastern Kunar province after being wiped out from Nangarhar province.

Europe

15-Une **directive relative à la lutte contre le terrorisme dans l'Union européenne est actuellement en préparation**, précise *Le Figaro*. Le 14 mars dernier, elle a fait l'objet d'un consensus au sein du Conseil « justice et affaires intérieures » qui réunit les ministres de la Justice et de l'Intérieur de l'Union.
16-Le **frère du meurtrier jihadiste Mohamed Merah, Abdelkader, va faire appel de son renvoi devant une cour d'assises spéciale pour complicité dans les sept assassinats commis en 2012 dans le sud-ouest de la France**, a annoncé vendredi son avocat Eric Dupond-Moretti à *l'Agence France-Presse*. "Abdelkader Merah n'a jamais été le complice de son frère" dans la préparation et la commission des tueries de mars 2012, a déclaré Me Dupond-Moretti. "Il a pris des positions radicales. Si on considère que tous les radicaux sont très dangereux, il faut tous les enfermer", a ajouté l'avocat.
17-**Markus Reichel,** the **former BND employee** found **guilty** of furnishing **classified documents** to the **CIA** and **Russian intelligence** on the grounds he was bored at work, has been sentenced to **eight years** in prison (Extensive coverage / vaste couverture).
18-**Swedish intelligence** (Sapo) has accused the **Russian state** of using a **compliant news media**, "a loyal tool" for **propaganda purposes**. In its reporting of the story, ***Sputnik*** dismissed the charge as **'baseless'.**
19-The **Danish government's plan** to **re-introduce** the **mass collection of data** on residents' internet use has been **dropped** after an analysis showed that it would cost upwards of **one billion kroner** ($197 million Cdn,) reports *The Local*. **Justice Minister Søren Pind** said that he would go back to the drawing board to find a **new way to monitor online activity.**

Australia, New Zealand / Australie, Nouvelle-Zélande

20-A **collective of hackers** that claims to have **taken down thousands of social media accounts used by Islamic State supporters** has warned of a **disproportionate number belonging to Australians**. **Ghost Security Group** also says that while the death of a **British hacker** and jihadist linked to plots to attack **Western targets** had dealt a blow to Islamic State's cyber operations, it is only a matter of time before they **recruit more skilled operatives**, the *Australian Associated Press* writes.

Asia / Asie

21-*The Hindu* reports that an **intelligence alert** from Pakistan about 10 terrorists sneaking into India sent the **security establishment** into a tizzy.
22-**South Korea's military** said it suspects **North Korea** fired a **second missile** this morning, after the **North** earlier **launched a ballistic missile that flew about 800 km** (500 miles) and into the sea **off its east coast**, *Reuters* reports.
23-**North Korea** appears to be **continuing efforts to develop a submarine-launched ballistic missile**, a U.S. website monitoring the communist nation said yesterday. The website **38 North** said, citing **recent satellite imagery of the North's Shinpo South Shipyard**, that the North is **believed to be forging ahead with development of the KN-11 SLBM**, also known as **Bukkeukseong-1**, as well as a **Gorae-class experimental ballistic missile submarine**, *Yonhap News Agency* reports.

24-**China** expressed **its opposition** yesterday (17/03) to **unilateral sanctions against North Korea** saying they could raise tension, after the **United States** imposed new curbs on the isolated country in **retaliation for its nuclear and rocket tests**. US President Barack Obama on Wednesday imposed sweeping **new sanctions on North Korea** intended to further isolate its leadership after recent actions seen by the United States and its allies as provocative, *Reuters* reports.

Americas / Amériques

25-Ahead of President Obama's visit to Argentina next week, reports *Reuters,* the **United States** announced it will **declassify** military and **intelligence documents** related **Argentina's 1976-83 'Dirty War',** the seven-year period when a military dictatorship cracked down on left-wing opponents.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Tuesday, April 5 2016
le mardi 5 avril 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- **Canada is not at war with ISIS**, but **security and intelligence forces need special powers to fight the "sophisticated" terror group**, says the outgoing security adviser to the prime minister. **Richard Fadden**, who announced his retirement last week after nearly 40 years of public service, told *CBC Radio's As It Happens* that **ISIS does not pose an "existential" threat to Canada**, but it is accomplishing its prime objective of breeding terror. Military personnel deployed in Syria and Iraq may feel like they are fighting a war, but Fadden said that is **not the perspective of Canada's security intelligence agencies**. **"I think people would think we are fighting a very, very serious situation that requires a great deal of attention and probably some new powers and resources. But I think most of my colleagues would say no, it wasn't war,"** Fadden told host **Carol Off**. Prime Minister **Justin Trudeau** has faced sharp criticism for similarly rejecting the label "war." He said the word suggests the fight can be won by one side or the other, and in this case there is no path for ISIS to win against the West. Fadden added that constitutionally a war is formally declared by the Queen or her representative, the Governor General. Last month, **CSIS** director **Michel Coulombe** revealed that **agents have used new powers to disrupt suspected terrorist threats nearly two dozen times since last fall.** In the wide-reaching interview, Fadden also said **he does not believe the fast-tracked process to bring 25,000 Syrian refugees into Canada presented significant security risks, because equivalent checks were put in place.**

Canada

2- Canada's top general says there's **no end in sight in the battle against ISIS**, and Canadians should **prepare for news of casualties now that Canada has stepped up its mission on the ground in Iraq and Syria.** Gen. **Jonathan Vance** made the comments in a wide-ranging interview with **Rosemary Barton**, host of *CBC News Network's Power & Politics*, when asked if victory against ISIS should be expected soon. "I don't think it's in sight, I think we are thinking through the problem, we understand more and more and when you say ISIS, or ISIL or Daesh, it comes in many forms," Vance said. While the general said he was **confident all the right steps were being taken to eventually defeat ISIS** in Iraq, action also **had to be taken socially and politically to oppose the organization**. "There is a wider effort in the counterterror world that needs to work at defeating this across the board, including countering the messaging seeking those root causes and trying to incentivize people to either leave the fight or not go in the first place," Vance said.

3- Menacé de recevoir une «balle entre les deux yeux», **Haroun Bouazzi**, le **porte-parole d'une association québécoise de musulmans a porté plainte à la police de Montréal** et affirme craindre pour sa sécurité, rapporte le *Journal de Montréal.*

4- Un bref reportage dans *Le Droit* souligne qu'un peu plus d'un an après son arrestation pour des **allégations de terrorisme**, un Ottavien de 22 ans tente à nouveau d'obtenir sa liberté provisoire en attendant la suite de son procès. **Suliman Mohamed** est placé en détention préventive depuis janvier 2015. La Gendarmerie royale du Canada l'a interpellé après l'arrestation des jumeaux **Carlos et Ashton Larmond**, dans la même semaine. Les trois suspects se connaissent.

International

United States / États-Unis

5- The *New York Times* reports that a **"foreign fighter surge team" of experts from the F.B.I., the State Department and the Department of Homeland Security** met with their **Belgian counterparts a month before the Brussels terrorist attacks** to try to correct gaps in Belgium's widely criticized ability to track terrorist plots. **Andrew M. Liepman**, a former deputy director at the **National Counterterrorism Center** who is now a senior policy analyst at the RAND Corporation, said there were dual challenges ahead for European Union countries to overhaul their internal security bureaucracies as well as to enhance cooperation and intelligence-sharing among themselves. Some countries, like Germany and the Netherlands, take the need to share seriously, Mr. Liepman said. Others share a common language that engenders trust, most notably the so-called **Five Eyes** countries: the United States, Britain, Australia, **Canada** and New Zealand.

6- Writing in *The Intercept* on the release of the **Panama Papers**, **Glenn Greenwald** states: "The key revelation is not the illegality of the specific behavior in question but rather the light shined on how our political systems function and for whose benefit they work. That was true of the **Snowden leak**, and it's true of the Panama Papers as well."

7- *Reuters* reports that **Jhon Jairo Cruz Trejos**, a Colombian who pleaded guilty to U.S. narcotics charges stemming from a probe that began with him trying to help a **paramilitary group get uranium for a "dirty bomb"** to attack the **U.S. embassy in Bogota** was sentenced to 13 years in prison.

United Kingdom / Royaume-Uni

8- *The Independent* reports that **ISIS supporters have released a new video calling for terror attacks in London, Berlin and Rome** against a backdrop that suggests the terror group's propaganda machine may be in crisis.

9- Britain's biggest Islamic sect allowed a **militant linked to al-Qaeda to tour dozens of mosques on a jihadist recruitment drive** that spawned terror plots and murders, the *UK Times* reports. Senior representatives of the **Deobandi** sect, a supposedly moderate movement that controls almost half of Britain's 1,600 mosques, hosted the extremist cleric Masood Azhar during a 30-day visit in which hundreds of young Muslims were urged to seek weapons training at terrorist camps in Pakistan.

Europe

10- **François Sénémaud,** Directeur du renseignement à la direction générale de la **sécurité extérieure (DGSE) du ministère de la Défense depuis 2012,** a été nommé **ambassadeur de France auprès de la République islamique d'Iran**, rapporte *Acteurs Publics*.

11- **Turkey's Interior Ministry** has updated its list of "wanted terrorists" to include 23 **Islamic State of Iraq and the Levant (ISIL)** militants following the jihadist organization's twin suicide bombing in the country's capital on Oct. 10, 2015, *Hurriyet Daily News* states. The government has offered rewards of more than 42 million Turkish liras (more than $14 million) for any information leading to the suspects' capture.

Africa / Afrique

12- Mali President **Ibrahim Boubacar Keita** on Monday declared a **state of emergency** across the entire national territory for a period of 10 days, *Xinhua News Agency* reports. The imposition of a state of emergency was decided upon during a special cabinet meeting presided over by the president. "This state of emergency that follows the previous one that ended on March 31, was declared due to the **prevailing security situation in Mali** and the sub-region which is

characterized by **constant terrorist threats**," said a statement from the cabinet. Malian authorities said the state of emergency that ended on March 31 enabled security forces to arrest suspects and impound vehicles.
13- President **Uhuru Kenyatta** met his French counterpart **Francois Hollande** on Monday, the first State visit by a Kenyan leader to France in the past 14 years. President Hollande said the **European Union** as a whole **needs to support AMISOM's fight in Somalia** following an announcement that it would be cutting its funding to the troops in a couple of months. "We have no choice but to work together because terrorists now know no borders... so why should we?" he posed at a press briefing following bilateral talks with President Kenyatta at the Presidential Palace on Monday evening. Kenya's Foreign Affairs Cabinet Secretary **Amina Mohamed** had earlier told *Capital FM News* that the threatened cuts had been one of President Kenyatta's motivations for visiting France.
14- Après **l'attaque terroriste de Grand-Bassam**, une banlieue abidjanaise dont le cerveau et les supposés auteurs sont des maliens, la crainte de représailles contre la communauté malienne vivant en **Côte d'Ivoire** devient de plus en plus persistante, rapporte *l'Humanité*.

Middle East / Moyen-Orient

15- *Gulf News* reports **that three men charged with setting up an affiliate of the Lebanon-based Hezbollah group in the UAE** were sentenced to six months in prison to be followed by deportation, the Federal Supreme Court ruled on Monday. The men, **Canadian Lebanese Suhail Naif Gareeb**, 62; Lebanese Asa'd Ameen Qansouh, 66; and Ahmad Ebrahim Qansouh, 30, were found guilty of setting up an office of the militant group in the UAE and carrying out commercial, economic and political activities without licences, the court presided over by judge Falah Al Hajeri ruled.
16- According to *Reuters*, **Iran has sent commandos to Syria as advisers**, a military official said on Monday, suggesting it is using its army as well as paramilitary forces to help President Bashar al-Assad's forces in the country's civil war.
17- **Global military spending rose in 2015 to nearly $1.7 trillion**, the first increase in several years, driven by conflicts including the battle against the Islamic State group, the Saudi-led war in Yemen and fears about Iran, a report by the the **Stockholm International Peace Research Institute** shows, the *Associated Press* states.

Afghanistan/Pakistan

18- "**Afghanistan is high on our agenda**. Afghanistan is our biggest military operation ever," **NATO Secretary General Jens Stoltenberg** told reporters on Monday after his meeting with U.S President Barack Obama, *Tolo News* reports. "It shows the importance of unity in North America and Europe, because our military operation in Afghanistan is a direct response to the terrorist attack against the United States on 9/11. And European, **Canadian soldiers** have fought together with the American soldiers in Afghanistan for many, many years," he said.
19- A **suicide bomber** on a motorbike detonated his explosives near a busy bazaar in Afghanistan's northern Parwan province this morning, **killing at least six people**, officials said, the *Associated Press notes*.

Australia, New Zealand / Australie, Nouvelle-Zélande

Light coverage / couverture légère.

Asia / Asie

20- According to the *Yonhap News Agency*, North Korea has **strengthened its surveillance of its people in areas bordering China** to crack down on those contacting defectors in **South Korea** ahead of its key party congress, sources said Tuesday. The **Ministry of State Security**, the North's intelligence agency, has sent a letter expressing its strong allegiance to North Korean

leader **Kim Jong-un**, according to the sources familiar to North Korean affairs. In the letter, the ministry pledged in March to beef up its surveillance along the border as the **Workers' Party of Korea** is preparing to hold its first party congress in more than three decades in May. "The North is trying to strengthen its control over people in the border areas on the grounds that internal information in North Korea has leaked to the South Korean media," a source said.

21- North Korea's continuing attempts to jam South Korea' Global Positioning System (GPS) may be aimed at **disrupting the navigation systems of aircraft**, government officials said as the communist country continued to send jamming signals on Tuesday. In a provocative operation that started in late March, North Korea has been **sending GPS-jamming signals across the border**. The signals began last Thursday and continued on and off into Tuesday, according to military and information and communication technology (ICT) sector officials, reports *Yonhap News Agency*. "An assessment showed that North Korea's near daily GPS-jamming activity seems to be **targeting aircraft's navigation equipment**," an intelligence source said, asking not to be named.

22- *Kyodo News* is reporting that top nuclear envoys of Japan and China agreed Tuesday to **coordinate closely to implement sanctions** on **North Korea**, which were decided by the U.N. **Security Council** in response to **Pyongyang's pursuit of nuclear and missile programs**, the Chinese representative told reporters. **Wu Dawei**, China's special representative for Korean affairs who doubles as the chairman of the long-stalled six-party negotiations aimed at ending North Korea's nuclear weapons program, also said he exchanged views on the resumption of the multilateral talks in his meeting with **Kimihiro Ishikane**, director general of the **Foreign Ministry's Asian and Oceanian Affairs Bureau**, in Tokyo. Tokyo is cautious about restarting the six-party talks, which involve the two Koreas, China, Japan, Russia and the United States.

23- According to *The Times of India*, the The Bombay High Court on Monday **refused to grant bail to alleged ISIS recruit Areeb Majeed** who has been behind bars since November 2014. The HC dismissed an appeal he had filed to challenge denial of bail last May by a special court presiding over cases probed by **National Investigation Agency** (NIA).In November 2014, NIA supervised Areeb return to India from Istanbul. NIA said the Panvel college student had decided to join the extremist outfit ISIS along with three other friends in May 2014 and even went on a pilgrimage for eight days, after which they parted ways to participate in unlawful activities in Iraq and Syria.

Americas / Amériques

24- Panamanians have long shrugged off their country's checkered reputation as a financial haven for drug lords, tax dodgers and corrupt oligarchs. If they're crooks, they've learned from the world's wealthy nations, they like to joke. That same defensiveness has re-emerged amid the fallout from the leak of 11.5 million confidential documents from the Panama-based law firm **Mossack Fonseca** revealing details of how some of the globe's richest people **funnel their assets into secretive shell companies** set up here and in other lightly regulated jurisdictions. **Ramon Fonseca**, a co-founder of the firm, said Monday that his country's success in establishing itself as an offshore banking giant has bred jealousy from first-world rivals at a time of increasing competition and scrutiny of the industry in the aftermath of the global financial crisis. "**It's very unfair what's happening because there's not a level playing field**," Fonseca *told The Associated Press* in an interview. "Without a doubt if this happened to a company in Delaware nothing would happen, but because it's Panama it's the front page of the world's newspapers."

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.

Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Friday, April 22, 2016
le vendredi 22 avril 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1-The RCMP alleges in documents released yesterday that two men arrested after returning to Toronto from **Turkey may "travel to participate" in terrorism unless their conduct is restricted through peace bonds. Kadir Abdul**, 27, and **Samuel Augustin Aviles**, 32, appeared briefly in a Brampton, Ont., court after they were arrested last Friday at Toronto's Pearson airport, the *National Post* writes. Rather than seeking criminal charges, the RCMP wants peace bonds against the pair. Critics want the Liberal government to rescind the change as part of its promised review of the Conservative anti-terrorism law, **C-51,** arguing peace bonds place severe restrictions on those who have not been charged with any crimes. According to the **Canadian Security Intelligence Service**, about **100 people with "a nexus to Canada" are involved in the conflict in Syria and Iraq**. Between 90 to 100 extremists have not left Canada to participate in terrorism but aspire to, **CSIS director Michel Coulombe** told the **Senate Committee on National Security and Defence** on March 7.

Canada

2-Light coverage / couverture légère.

International

United States / États-Unis

3-Given **James Comey's** answer to a question at a security conference in London Thursday that the **FBI paid "a lot"** for the **tool** which allowed the Bureau to **open** the **iPhone** belonging to **San Bernardino shooter Syed Farook**---"more than I will make in the remainder of this job, which is seven years and four months"--- a number of news organizations guestimated, given Comey makes $180,000 annually, the **cost** of the **hacking tool** was in the vicinity of **$1.3 million.** But whatever the cost, the FBI director made clear the expense was **"worth it"** (extensive coverage/vaste couverture).

4-Homeland Security Secretary **Jeh Johnson** has **rejected** a **color-coded scheme** to **measure border security,** reports the *Associated Press,* after hiring a consultant that dismissed the idea as **simplistic** and **misleading.**

5-The *Washington Post* reports a **District of Columbia federal appeals court** has **dismissed** a long-running **ACLU lawsuit** seeking access to more **details** about the **U.S. government's lethal-drone operations**, ruling disclosure "could reasonably be expected to **damage national security.**"

United Kingdom / Royaume-Uni

6-A **Home Office 'whistleblower'** confidentially told the *Daily Telegraph* **UK Border Force guards** have **"zero discretion"** to **detain** and **interview travelers** trying to **re-enter Britain** if they **hold** a **UK passport** and have **not been "flagged"** by police or **security services.**

7-Concluding a visit to Britain, **Maina Kiai**, the **UN's special rapporteur** on the **right** to **freedom** of **assembly,** charged the government's **Prevent program,** designed to **counter Islamic**

extremism, has "created **unease** and **uncertainty** around what can be legitimately discussed in public" reports the *Guardian.*

Africa / Afrique

8-A **refusal** by the **South Sudanese government** to **permit rebel leader Riek Machar** to **return** to **Juba** accompanied by **weaponry** such as **rocket-propelled grenade launchers**, is **stalling** Machar's arrival reports *Reuters.*
9-Selon *Pan African News Agency,* le **Conseil présidentiel du gouvernement d'union nationale libyen a promis de fournir un soutien "total" à la ville de Derna (est),** félicitant, dans un communiqué la ville de **Derna pour sa libération de Daech (Etat islamique) et le peuple libyen pour la libération de la zone d'al-Fattaih** et l'expulsion définitive des restes de Daech de la ville.
10-D'après l'*Agence de Presse Africaine,* le **Burkina Faso va consacrer, en 2016, un montant d'environ 2,3 milliards de FCFA pour la mise en place d'un fonds de lutte contre le terrorisme** et l'acquisition de matériels au profit des forces de sécurité, a appris APA auprès de la Primature. Le gouvernement burkinabè avait déjà créé le **Conseil de défense et de sécurité nationale (CNDSN), ainsi qu'une Agence nationale de renseignement pour la sécurité (ANRS).** Le pays bénéficie de l'**appui technique et financier de la France et des Etats-Unis** dans la formation et l'équipement des forces de sécurité.

Middle East / Moyen-Orient

11-The *Times of Israel* reports that **Israel will close off the West Bank and Gaza Strip for 48 hours beginning Friday**, amid fears of attacks by the **Hamas terror group** during the Jewish holiday of Passover, which begins Friday night, the army announced Thursday.
12-*The National (UAE)* reports that the **United States and the GCC have a "common vision" for the Middle East** and Washington will continue to help Gulf countries enhance their military capabilities and counter Iran's destabilising regional activities.

Afghanistan/Pakistan

13-The *Pakistan Dawn* reports that in an unprecedented move, **Chief of Army Staff General Raheel Sharif** dismissed six army officers, including two generals, from service over alleged corruption, an authoritative source confirmed on Thursday.
14-*Khaama Press* reports that a **deadly suicide attack plot** by the anti-government armed militant groups was foiled by the **Afghan intelligence operatives** in southern Helmand province.

Europe

15-According to its **review of 2015**, the **AIVD**, reports the *NL Times,* warns the **jihadist threat** to the **Netherlands** is **"more complex and difficult than ever before"**. The Dutch intelligence service points out "**weapons** in the **hands of jihadists will not necessarily be used for terrorist attacks,** but given **examples in Canada,** the United States and France, the **risk of this is real."** Additionally, the AIVD states the Netherlands is **"naive"** when it comes to **online security.**
16-The Norwegian law firm representing Edward Snowden said **Snowden** will take the **Norwegian state to court** in a bid to **secure free passage there** reports *Reuters.* Snowden has been **invited to Norway** to receive a **freedom of speech award** from the local branch of the **writers' group PEN International,** but is worried that he would be **handed over** to the **United States.**
17-**CIA director John Brennan** arrived in **Sarajevo** this morning for **counter-terrorism talks** with **Bosnian officials** in a visit that was not officially announced reports the *Associated Press*
18-Selon *DH* (Belgique) le terroriste **Mohamed Abrini devait, lui aussi, mourir en kamikaze**, et que ce n'est pas du tout un renoncement de sa part qui explique qu'il ne se soit pas fait exploser sur place.

19-Un mois après les deux attentats qui ont fait 32 morts et des centaines de blessés à Bruxelles, **l'Europe reste désarmée face à la menace terroriste**, souligne *Le Figaro*. La Belgique sonne l'alarme, car les recrues européennes de Daech reviennent de Syrie et toutes n'ont pas été identifiées.

Australia, New Zealand / Australie, Nouvelle-Zélande

20-The *Australian Associated Press* writes that **extra security screening** will be in place for **Anzac Day commemorative services at Gallipoli** this year following terror attacks in **Turkey**. Representing the **Australian government** on the peninsula will be **Dan Tehan,** Minister for Veterans Affairs and Minister Assisting the Prime Minister for the Centenary of Anzac.

Asia / Asie

21-The *Times of India* reports that Delhi-based endocrinologist Dr RP Singh has resiled from his statement to the Maharashtra ATS where he allegedly admitted to have attended meetings where plots were hatched to avenge **jihadi terror attacks**, in what is yet another blow to the efforts of the prosecution to catch those accused of **"Hindu" terror**.

22-Five global public relations firms have made pitches to the Chinese government for a potential new campaign, four sources said, as Beijing tries to **communicate more effectively with the West**. The competition by the leading Western PR companies comes amid **intensifying scrutiny of Chinese companies abroad**, a **crackdown on dissent at home and rising tensions in the South China Sea**. The **State Council Information Office (SCIO)**, the government's information and propaganda arm, has heard presentations from **Hill+Knowlton, Ketchum, and Ogilvy Public Relations**, according to four people and company communications seen by *Reuters*. The PR campaign under consideration also comes as the government strengthens its control over domestic media and public speech at home. In January, ambassadors from **United States**, **Canada**, **Germany**, **Japan** jointly signed a letter expressing **concern over a new counter terrorism law**, and draft laws **on cyber security law and management of foreign non-governmental organizations (NGOs),** which includes widespread censorship.

23-The chief nuclear envoys of **South Korea** and **China** held talks on Friday as satellite images indicate that North Korea may be preparing to conduct its fifth nuclear test, possibly ahead of its key party congress early next month. **Kim Hong-kyun**, South Korea's Special Representative for Korean Peninsula Peace and Security Affairs, arrived in Beijing earlier in the day and began talks with his Chinese counterpart, **Wu Dawei**, said a South Korean diplomat who was involved in the Friday meeting. Before departing for Beijing, Kim told *Yonhap News Agency* by telephone that he and Wu will have an **"in-depth exchange of views on a range of cooperative measures, including an earnest implementation of U.N. Security Council resolutions, how to curb North Korea's additional provocations and countermeasures in the event of a North Korean provocation."**

Americas / Amériques

24-Light coverage / couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Wednesday, May 11, 2016
le mercredi 11 mai 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1-Light coverage / couverture légère.

Canada

2-**Canada** and the **United States** have set **up a working group to help sort out errors of identity on no-fly lists.** But, the *Canadian Press* writes, **Public Safety Minister Ralph Goodale** says Canada needs **"an entirely new database and information system"** to completely solve the problem of people — including youngsters — being delayed at airports due to false matches.
3-Footage analyzed by *The Globe and Mail* shows **Saudi Arabia using armoured vehicles against minority Shia Muslim dissidents in the Mideast country's Eastern Province**, raising serious questions **about Riyadh's tendency to use these military goods against its own citizens**. Copies of the videos, which date from 2012 and 2015, **were supplied by Saudi human-rights activists who want Canada to suspend shipments of combat vehicles to Riyadh in a $15-billion deal between Canada and the ruling House of Saud.**
4-*La Presse+* rapporte que plus d'un an après leur arrestation, **El Mahdi Jamali et Sabrine Djermane, ces deux élèves du collège de Maisonneuve** accusés d'une **série d'infractions terroristes, sont de retour devant les tribunaux**. Le couple de Montréalais incarcéré depuis son arrestation en avril 2015 aura à compter d'aujourd'hui son enquête préliminaire, ultime étape avant le procès. Les deux amoureux, lui, 19 ans, et elle, 20 ans, **sont accusés d'avoir tenté de quitter le Canada** en vue de **commettre un acte terroriste à l'étranger, de possession d'une substance explosive dans un but criminel, d'avoir facilité un acte terroriste et d'avoir commis un acte au profit ou sous la direction d'un groupe terroriste.** Ils ont plaidé non coupable.

International

United States / États-Unis

5-Given **Director of National Intelligence James Clapper's view** that **intelligence services must co-operate** against **terrorism,** *Washington Post* columnist David Ignatius writes a **'small breakthrough'** seems to have taken place in mid-April when **Clapper met** with **some European intelligence chiefs** in Germany to **discuss better sharing of intelligence.** Speaking to Ignatius, Clapper said the **United States still can't be certain** how much **harm** was done to **intelligence collection** by the **Snowden disclosures.** "We've been **very conservative** in the **damage assessment.** Overall, **there's a lot,"** Clapper said, noting that the leaks made **terrorist groups "very security-conscious"** and sped the move to unbreakable encryption of data.
6-Recent figures published by **New Jersey's Office of Homeland Security and Preparedness** show that at least **75 homegrown violent extremists** were found to be **operating** across the **United States** in **2015**, with the **largest portion** of these individuals **pledging allegiance** to **Isis** reports the *Washington Free Beacon.* The largest number of homegrown extremists were caught providing material support to various terror organizations, while at least **21 per cent** of the **terrorists** were found to be **planning attacks** in the **United States.**
7-**Section 702** of the **Foreign Intelligence Surveillance Act**, which authorizes aspects of NSA

observation, **doesn't expire** for another **19 months** but *The Hill* reports **Congress**, seeking to **preempt privacy advocates** on the issue, is **holding hearings now.**

United Kingdom / Royaume-Uni

8-Lending her voice to the **Brexit debate, former MI5 director Dame Eliza Manningham-Buller** told the *BBC* that "I **believe strongly** that we would be **significantly less safe outside [the** EU] because of all the networks, the relationships, the policy exchanges, the determining on data sets, things like fingerprinting, things like European arrest warrant, things like joint research on explosive detections on arms and so on. We are not going to be able to influence that if we are out."

9-A **London judge** has **rejected** a bid by the **National Crime Agency** to **force alleged cyber-hacker Lauri Love** to **hand over encrypted computer passwords.** The **United States** is **attempting** to **extradite** the 31-year-old **Love** on charges of **hacking** into the **U.S. Army, NASA** and **U.S. Federal Reserve networks.** NCA seized the computers during a raid at Love's home in Stradishall, Suffolk, in October 2013. (Extensive coverage / vaste couverture).

Africa / Afrique

10-According to the **United States**, reports *CNN,* the **number** of people **killed** by **terror attacks** in **Africa** in the **last year** is **as large**, if not larger, than the **deaths** inflicted by **Isis** in the **Middle East.**

11-**Oil companies** in **Nigeria's Delta** region have taken steps to **evacuate employees** after an **escalation** in **militant violence.** In the latest incidents, reports *Reuters,* two police officers and three soldiers were murdered in separate attacks.

Middle East / Moyen-Orient

12-The *Times of Israel* reports that a **teen Hamas operative revealed "extensive information"** about the terror organization's tunnels and plans for infiltrating Israel in order to carry out attacks, after he was arrested by security forces last month, the **Shin Bet** said Tuesday.

13-A **car bomb** in a predominantly Shia district of the Iraqi capital has **killed at least 50 people** and wounded at least 100 others, police sources told *Al Jazeera.*

14-The *Gulf News* reports that **warring parties in Yemen reached a preliminary agreement** on Tuesday to release all prisoners within 20 days, sources at UN-backed peace talks in Kuwait said.

Afghanistan/Pakistan

15-The *Pakistan Dawn* reports that the police informed the administrative judge of the **antiterrorism courts** on Tuesday that they had also released a fourth suspect out of the five allegedly detained for **spying for India** because of lack of evidence.

16-The *Pajhwok Afghan News* reports that at least 10 people were killed and another 23 including public uprising commander wounded in a **car bombing** on Tuesday in eastern Nangarhar province, an official said.

Europe

17-*Neue Osnabrücke Zeitung* reports the morning that **federal investigators** in **Germany** have **opened cases** against **40 asylum seekers,** suspecting **Isis connections.** Meanwhile, authorities have determined the **man arrested** for the **fatal stabbing spree** at a train station near Munich yesterday has **no terrorist links.**

18-**Europol director Rob Wainwright,** reports *Vice,* has tweeted **"encryption dilemma** must be **solved soon. Real problem** in **75% of all Europol cases."**

19-Selon *Le Soir,* **Mohamed Arshad, refuse de livrer le nom de ses complices en cour.** Lors de la deuxième journée d'audience, le jeune homme de 27 ans a livré des détails sur son séjour en Syrie. Il a mis en cause la légitimité de la justice belge. **Abdelhamid Abaaoud, qui pilotait de**

loin la mise en place de la cellule terroriste de Verviers, avait recommandé à son logisticien Mohamed Hamza Arshad Mamood Namji, de « se comporter comme un mécréant » pour ne pas se faire remarquer après son retour de Syrie. Les mécréants sont sans doute aussi des arrogants, pense ce dernier, encore aujourd'hui.

Australia, New Zealand / Australie, Nouvelle-Zélande

20-**More than half of ASIO investigations now target people aged 25 and under – more than triple the proportion just three years ago in a dramatic illustration of the plunge in the average age of terrorism suspects**. *Fairfax Media* understands that just 15 per cent of the security agency's investigations targeted this young age bracket three years ago, but has now risen to more than 50 per cent. ASIO has said in the past that its number of priority investigations doubled between 2014 and 2015, **from about 200 to 400 amid the surge in extremism inspired by the so-called Islamic State and like-minded groups.**

21-**Notorious Islamic preacher Musa Cerantonio is among five men arrested in far north Queensland over an alleged plan to take a boat to Indonesia and join the Islamic State (IS) terror group**. **Shayden Thorne**, the brother of another hardline Islamist, **Junaid Thorne**, was also arrested. Police arrested the men yesterday as they were towing a boat towards Cape York, in far north Queensland. They are being held on suspicion of foreign incursion offences, the *Australian Broadcasting Corporation* writes.

Asia / Asie

22-The *Daily Mirror LK* reports that a **Sri Lanka national** has been caught attempting to travel to **Canada via Taiwan using fake Canadian identification cards**, the National Immigration Agency (NIA) said Tuesday.

23-*Bangladesh Daily Star* reports that Bangladesh on Tuesday **executed Motiur Rahman Nizami, leader of the Jamaat-e-Islami party**, the country's largest Islamist party for **war crimes**, officials said, a move set to exacerbate tensions in the volatile Muslim-majority nation.

24-South Korea will put sanctions and pressure ahead of dialogue with the **Democratic People's Republic of Korea (DPRK),** Unification Minister **Hong Yong-pyo** said on Wednesday. For now, sanctions and pressures are needed more against DPRK, Hong told a forum organized by the **Korea Future Foundation**. "Now is not the right time for talks," he said. Hong made the remarks two days after DPRK closed its four-day 7th congress of the Workers' Party of Korea in 36 years on Monday, reports *Xinhua News Agency*.

Americas / Amériques

25-**Waldir Maranhao** has **reversed course** and now declared that the **recent vote** by **Brazil's Chamber of Deputies** to send the **impeachment process** against **President Dilma Rousseff** to the **Senate** is **valid.** President Rousseff has taken her case to the **Supreme Court.** (Extensive coverage / vaste couverture).

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Wednesday, June 1 2016
le mercredi 1er juin 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- Canada won't confirm exactly what its spies were doing in Afghanistan, but it has been quietly awarding service medals for their service, according to documents obtained by *VICE News*. And it was dangerous. Those medals were pinned on to the spooks' chests by Governor General **David Johnston**, who acts as Canada's head of state, for their work in Afghanistan. But for much of Canada's involvement in the war-torn country, the work of the **Canadian Security Intelligence Service (CSIS)** remained strictly secret. In recent years, CSIS' work in Afghanistan has slowly come to light. Even now, the government will only say that that **CSIS agents were processing detainees and doing basic interviews with possible al Qaeda or Taliban commanders from within Canadian Forces and Afghan military bases.** But these new documents, obtained under the Access to Information Act, reveal that **CSIS agents may have been directly in harm's way**.
2- Chinese Foreign Minister **Wang Yi** will hold high-level talks with Prime Minister **Justin Trudeau** on Parliament Hill today as planning gets under way for Mr. Trudeau's official visit to China in the fall, the *Globe and Mail* reports. Mr. Wang is also meeting Foreign Affairs Minister **Stéphane Dion** in what the Chinese government said is the first annual meeting of foreign affairs ministers. The report briefly notes that Mr. Trudeau's former national security adviser, **Richard Fadden**, said the Chinese have been **heavily engaged in spying and cyberattacks in Canada**. "Their broad approach is to use the vacuum-cleaner approach. They'll, you know, pretty well take anything," Mr. Fadden, a former director of the **Canadian Security Intelligence Service**, said in an interview on Sunday. "So I think it's actually quite difficult to balance all of this and make sure we have a work-a-day relationship, while at the same time making it very clear we don't like the **cyberattacks**."

Canada

3- A Toronto man accused of **attacking Canadian soldiers with a knife** has been **charged with a terrorism offence** just as a judge found him **unfit to stand trial**. **Ayanle Hassan Ali**, 27, was earlier charged with nine counts, including three of attempted murder, following unprovoked attacks at a North Toronto military recruiting centre in March. Witnesses described soldiers subduing a knife-wielding man who had tried to hurt them, allegedly saying, "**Allah told me to come here and kill people**." No soldiers were seriously injured. The Islamic State terrorist group has been urging extremists in North America and Europe to use such tactics against uniformed soldiers. On Tuesday, the **RCMP** announced in a statement that they laid a catch-all terrorism charge against Mr. Ali – specifically, a Criminal Code offence stating he committed all of his other alleged crimes for "the benefit of, at the direction of or in association with a terrorist group" (moderate coverage / couverture modérée).

International

United States / États-Unis

4- Specifically citing the **Euro Football Championship** in **France**, the **State Department** issued an **alert** yesterday advising **U.S. citizens traveling** to **Europe** this summer of a **heightened risk** of **terrorism**. The *Wall Street Journal* notes an 'alert' does not constitute a 'warning' which is seen

as indicative of a higher-level threat. Will Geddes, a security expert, told *The Times of London* that Americans tend to be more alarmist about security alerts but pointed out the alerts are **backed up by available intelligence.**
5- Contrary to the opinion of former Attorney General Eric Holder, reports *Politico,* **White House Press Secretary Josh Earnest** made it clear during Tuesday's media briefing that **President Obama does not think Edward Snowden rendered a "public service"** by leaking NSA documents.

United Kingdom / Royaume-Uni

6- According to the *Guardian,* **British involvement** in **clandestine rendition operations** provoked an **unprecedented rift between MI5** and **MI6** at the height of the 'war on terror'. **MI5 director Eliza Manningham-Buller** was reportedly so **incensed** when she discovered the role played by **MI6 in abductions** that led to suspected extremists being tortured, she **threw out** a **number** of **SIS staff** and **banned** them from **working** at **MI5 headquarters. Manningham-Buller** also **wrote** to **Prime Minister Tony Blair** to **complain** about the **conduct of MI6 officers,** saying their actions **threatened Britain's intelligence gathering** and may have **compromised** the **security and safety** of **MI5 officers** and their informants.

Europe

7- Selon *L'Express,* plus de **six mois après les attentats de Paris et Bruxelles, l'identité des principaux organisateurs se précise**. Parmi eux, plusieurs Français, dont un mystérieux homme clef, **Abou Souleymane.**
8- D'après *Le Soir,* (Belgique), le 25 mai dernier, la **police fédérale d'Anvers procédait à huit perquisitions à Borgerhout dans le cadre d'un dossier de terrorisme et arrêtait trois personnes.** De Standaard révélait ce mardi que les suspects (deux mineurs et un troisième homme non identifié) planifiaient de faire **exploser trois bombes : à la gare d'Anvers-Central et sur la place Astrid. Le cerveau présumé de la cellule terroriste, un mineur âgé de 16 ans, était en charge de se procurer des explosifs.**
9- An **FSB investigation** into to the **cyber-theft** of **1.7 billion rubles** ($25.7 million) from **Russian financial institutions** has resulted in the **arrest** of **50** suspected **hackers** reports *Tass.*
10- Performance artist **Pyotr Pavlensky** has been **nominated** for the **Russian Security Services' (FSB) Prize** for **Literature and the Arts** for the **artistic protest** which saw him **light the door** of the **FSB headquarters on fire** reports the *Moscow Times.*

Africa / Afrique

Light coverage / couverture légère.

Middle East / Moyen-Orient

11- The *Jerusalem Post* reports that the **United States** might start using **Israeli suicide drones** in potential future combat zones around the globe.
12- *Naharnet Newsdesk* reports that Interior Minister Nouhad al-Mashnouq said that the **security apparatuses in Lebanon** were able to uncover and thwart schemes by the Islamic State group to carry out **terror acts**, mainly in crowded areas in Beirut.

Afghanistan/Pakistan

13- The *Pakistan Dawn* reports that **Chief of Army Staff General Raheel Sharif** said that **US drone strikes are regrettable and must stop** as they are a threat to the sovereignty and security of the country.

Australia, New Zealand / Australie, Nouvelle-Zélande

Light coverage / couverture légère.

Asia / Asie

14- *The Pioneer* reports that a recent **intelligence report on the rise of pro-Khalistani terror camps near Mission City in British Columbia, Canada**, for carrying out attacks in Punjab, brings an urgent alert to the Modi Government.

15- According to *Xinhua News Agency*, the Chinese Embassy in Washington on Tuesday rejected the *New York Times'* account about a recent air encounter between **Chinese and U.S. military planes** over the **South China Sea**. The Chinese military aircraft acted professionally while it watched the **U.S. Navy spy plane carrying out close reconnaissance in Chinese coastal waters,** said **Zhu Haiquan**, a spokesman for the Chinese embassy, in a letter to the *Times* published on the paper's website Tuesday. "Our operation was completely compliant with safety and professional standards. The attempt at intimidation by American military aircraft in the South China Sea, however, was not," Zhu pointed out.

16- Chinese President **Xi Jinping** met a visiting North Korean delegation Wednesday, state media reported, in an apparent attempt by Pyongyang to mend frayed ties with its powerful neighbour. Although the official *Xinhua news agency* did not give the names of those in the delegation, the encounter comes on the heels of a rare visit Tuesday by top North Korean politician **Ri Su Yong**, vice chairman of the country's ruling Workers' Party and former foreign minister.

17- North Korea has accused South Korea of **abducting its citizens** in a letter addressed to U.N. **Secretary General Ban Ki Moon** obtained Tuesday by *Kyodo News*. North Korean Ambassador **Ja Song Nam**, sent the three-page letter to the U.N. chief on May 17, describing the **"unsettled case of group allurement and abduction"** of its citizens by **South Korea's spy agency in what it called a "heinous terrorist act."** The case involved 12 women who North Korea claims were taken together with one male manager in Ningbo, located in Zhejiang Province of China, in early April.

18- The *Strait Times* reports that **four Bangladeshi workers** detained in April under the Internal Security Act were yesterday convicted of **financing terrorism**.

Americas / Amériques

Light coverage / couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Tuesday, June 7 2016
le mardi 7 juin 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- When **Roland Eid** launched his $23-million lawsuit a year ago against six high-ranking government officials, including **RCMP Commissioner Bob Paulson** and **Canadian Security Intelligence Service Director Michel Coulombe**, it was a long-shot at best. So it proved. The Ontario Superior Court has **granted the Crown's motion to have the case dismissed**, *The Ottawa Citizen* reports. A former CSIS informant, Eid alleged he had been the victim of, among other things, a negligent investigation and malicious prosecution in connection with the 2008 bankruptcy of his company, **ICI Construction**. Eid was convicted May 2 on all 10 breaches of the Criminal Code and the Bankruptcy and Insolvency Act. Judge **Timothy Ray** found that Eid had fraudulently stripped ICI of $1.7 million that should have been held in trust for subcontractors and suppliers. The judge said this action had triggered the bankruptcy and caused ICI creditors to suffer collective losses of $3.8 million. The hearing in Eid's civil action - before Madam Justice **Bonnie Warkentin** - came just 15 days after his criminal conviction.

Canada

2- D'après *Le Devoir,* la question **des droits de la personne ne devrait pas diviser la Chine et le Canada, écrit Luo Zhaohui. L'ambassadeur chinois** espère clore **l'escarmouche publique qu'ont partagée son gouvernement et Ottawa, après que son ministre des Affaires étrangères eut rabroué une journaliste.** À coup de lettre ouverte sur Internet, le diplomate chinois a reconnu que les deux pays partagent des différends, mais il a martelé que ceux-ci ne doivent pas éclipser les avantages d'une collaboration. **" La Chine n'a jamais prétendu que ses droits de la personne sont parfaits ",** a reconnu l'ambassadeur Luo Zhaohui dans un texte publié sur le site Internet du Globe and Mail dimanche soir. "

3- **RCMP** officers involved in a B.C. terrorism investigation committed criminal offences during the undercover sting – **providing money, resources and expertise to a couple living off social assistance** – a defence lawyer alleged in B.C. Supreme Court on Monday. *The Globe and Mail* reports that **John Nuttall** and **Amanda Korody** were found guilty by a jury in June of last year of conspiring to murder persons unknown and making or possessing an explosive substance – in both cases for the benefit or at the direction of a terrorist group. They were arrested on July 1, 2013, after they placed pressure-cooker devices outside the B.C. Legislature. They have argued they were **entrapped by police** and a hearing into that aspect of the case began in July. **Monday marked the start of closing arguments. Marilyn Sandford**, Mr. Nuttall's lawyer, told the court "none of this would ever have happened" if not for the actions of undercover police.

International

United States / États-Unis

4- The **Obama administration** is seeking to **amend surveillance law** to give the **FBI explicit authority** to **access** a person's **internet browser history** and other electronic data **without a warrant** in **terrorism** and **spy** cases. The *Washington Post* points out the administration made a similar effort six years ago but dropped it after concerns were raised by privacy advocates and the tech industry.

United Kingdom / Royaume-Uni

5- Sourced by a **Snowden document** from **2010**, the *Intercept* reveals a **secret report** prepared by **British intelligence** and dispatched to top government officials **warned** that **MI5** may have put **lives at risk** because their **surveillance systems** were **sweeping up more data** than **could be analyzed,** leading the Security Service to **miss clues** to **possible security threats.**

Europe

6- A **morning rush-hour car bomb attack** in **Istanbul** targeting a **bus carrying riot police killed 11 people**, including **seven police officers,** and wounded 36 others. There was **no immediate claim of responsibility** but *Reuters* notes **Kurdish militants** have staged **similar attacks before**, including one last month in Istanbul.

7- D'après *Le Monde,* à Lyon, **police et secours s'entraînent face à la menace terroriste à la veille de l'Euro 2016**. Deux simulations d'attaques sont organisées à quelques jours du début de la compétition. Le but ? **« Apprendre à travailler à plusieurs dans l'urgence. » Les attentats de Paris ont changé la donne.** La menace terroriste est désormais au coeur des préoccupations dans les dispositifs de sécurité, à l'occasion des grandes manifestations populaires. Les précautions prises pour l'Euro 2016, qui débute vendredi 10juin, fournissent une application à grande échelle d'une doctrine en pleine mutation, selon laquelle **l'ordre public, l'intervention antiterroriste et l'organisation des secours doivent s'articuler différemment.**

8- According to the Polish weekly magazine *Do Rzeczy,* **Russian intelligence**, under **diplomatic guise**, have **stepped up operations** in **Poland** in the run-up to the **NATO** summit in **Warsaw** next month.

9- Le sort des **trois Irakiens reconnus coupables d'activités en lien avec Daech fait débat** sous la Coupole fédérale. Que faire des trois Irakiens condamnés en mars dernier pour avoir participé à des activités en lien avec l'Etat Islamique (EI) au terme de leur peine? C'est la question posée lundi par le **conseiller national Fabio Regazzi (PDC/TI) à Simonetta Sommaruga.** Rien, lui a répondu en substance la ministre de Justice et Police suisse. Les **services de renseignement suisses ne disposent d'aucune base légale pour continuer à surveiller des personnes ayant purgé leur peine** rapporte *La Tribune de Genève.*

Africa / Afrique

10- In the wake of an **American terror alert** on the weekend, the **British** and **Australian governments** have issued a similar **travel advisory** for **South Africa.** The *Guardian* (UK), reports the **British statement** specifically pointed to **upmarket shopping areas** and **malls** in the **commercial hub** of **Johannesburg** and **Cape Town** as the **most likely targets.** In response, **South Africa's State Security Minister David Mahlobo** said "we remain a strong and stable democratic country and there is **no immediate danger posed** by the **alert".**

Middle East / Moyen-Orient

11- **Disenchanted Islamic State members recruited** from the **West** have **increasingly** been **contacting their governments** and **asking for help in getting home** reports the *Wall Street Journal.* Some have turned up at diplomatic missions in Turkey, and others have sent furtive messages to their governments seeking assistance.

12- *Haaretz* reports that **Israeli Prime Minister Benjamin Netanyahu** arrived in Moscow Monday evening to mark the 25th anniversary of relations between Israel and Russia and to discuss the consolidation of **coordination between their militaries** in Syria.

13- *Now Lebanon* reports that one of the **Syrian first lady's staffers has been assassinated** in mysterious circumstances, two months after Asma al-Assad's top bodyguard was killed in Damascus.

Afghanistan/Pakistan

14- The *Pakistan Dawn* reports that **Canadian High Commissioner Andrew Turner** said that the doctrine of reasonable accommodation could counter the phenomenon of xenophobes, which he described as individuals who have never been exposed to people from other backgrounds.
15- *Pajhwok Afghan News* reports that **President Ashraf Ghani** said on Monday those who believed **Afghanistan was in crisis** should think twice before saying this because the Afghan forces would protect their motherland at any cost.

Australia, New Zealand / Australie, Nouvelle-Zélande

16- Australia's military commitment in Iraq should be increased and **Australian Defence Forces** instructors should be allowed to accompany local troops into battle, says an analysis of strategic priorities for the incoming government. The 100-page document, to be released today by the **Australian Strategic Policy Institute**, says with the Islamic State terror group believed to be weakened, **more special forces should be sent to take part in operations with US units in the Middle East.** Mapping out challenges the incoming government will have to face, analyst **Andrew Davies** says recent events in the **South China Sea** have markedly increased tensions and North Korea is a destabilising force in North Asia. ASPI executive director **Peter Jennings** says the **next government should increase its military commitment to Iraq** and argue for other countries, particularly the US, to act decisively to finish the fight, *The Australian* reports.

Asia / Asie

17- The *Hindustan Times* reports that **senior intelligence officials** confided to one newspaper that they had informed a top civilian security institution about the presence of Daesh workers, whose origin is from **India, Syria and Canada**.
18- The *Strait Times* reports that **Singapore Minister for Defence Dr Ng Eng Hen alongside Canadian Minister of National Defence Harjit Singh Sajjan, and Russian Deputy Minister of Defence Anatoly Antonov**, called for countries to "work closely together to build up joint responses, and strengthen intelligence, surveillance and reconnaissance efforts."
19- The United States and China on Tuesday **agreed not to recognize North Korea as a nuclear state** and pledged to exert **joint efforts towards stopping any further provocations**, despite some fundamental differences over how to move toward that end, reports *Kyodo News*. "Neither one of our nations will accept North Korea as a nuclear weapons state," U.S. Secretary of State **John Kerry** told reporters in Beijing after senior officials from the two countries concluded an annual strategic meeting. The two-day meeting, which addressed an array of security and economic issues, was held at a time when North Korea has started signaling a new willingness to engage in diplomacy following months of arms tests and war-like threats.
20- German Chancellor **Angela Merkel** will visit China for the ninth time in her chancellorship from June 12 to 14 for the fourth round of China-Germany intergovernmental consultations, German Ambassador to China **Michael Clauss** told *China Daily* in an interview ahead of the visit. Merkel will bring about 11 ministers and vice-ministers to China for a meeting with Premier **Li Keqiang** and continue discussions according to the action plan of Sino-German cooperation to push relations forward, Clauss said. Issues including Sino-German cooperation in innovation, China's economic reform and opening-up, and mutual trade and investments are expected to be raised during the consultations, Clauss said. **International issues concerning Syria and the global economy** are also on the agenda. In addition, China and Germany will probably **reach an agreement on cybersecurity** that focuses on fighting **economic spying,** said the ambassador, calling on German and Chinese governments to facilitate a framework to protect companies from cyberattacks.

Americas / Amériques

21- An item on the *Inside the Games* website makes note of the establishment, in co-operation with **Intepol**, of a **Joint Integrity Intelligence Unit** for the **Brazil Summer Olympics.**

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Monday, June 27 2016
le lundi 27 juin 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- In advance of the 'Three Amigos' summit in Ottawa on Wednesday, **Mexican President Enrique Pena Nieto** will **arrive** in **Canada today** for a **state visit.** The *Globe and Mail* has learned the **Trudeau Government will offer intelligence** and **training** to **combat Mexico's drug violence.**"We are going to have a **wide-ranging discussion on security,** and for Mexico, it truly has very significant security issues," a **Canadian official** disclosed to reporter Bob Fife. "We have **world-class talent** on that part on all of our institutions, from the RCMP, **CSIS** and **CSE.** We have world-class assets that countries like Mexico could really learn from."

Canada

2- The family of **Canadian academic Homa Hoodfar** told the *Canadian Press* she is being **imprisoned in Iran** for **"dabbling in feminism and security matters".**

International

United States / États-Unis

3- From government and police reports, terrorism databases, news accounts and their own independent reporting, *Los Angeles Times* journalists in the U.S. and around the globe compiled a **record of every fatal act of terrorism during the 30 days of April** and found that **not a day passed during the month where there wasn't a terrorist attack** somewhere in the world. In all, **858 people died in 27 countries** as a result of terrorism **including Canadian John Ridsdel** in the Philippines. An additional 1,385 were injured.

4- A rally by a small group of **neo-Nazi demonstrators** at the **State Capitol in Sacramento** Sunday erupted into a **violent clash with protesters** that left at least **10 people injured, five of them stabbed.** Demonstrators battled with sticks, protest signs and other weapons as the **Traditionalist Worker Party** group ,which said it wanted to **assist supporters** of **Donald Trump,** began setting up for a scheduled noon rally on the west steps of the Capitol. The *Sacramento Bee* reports the **Traditionalist Worker Party** bills itself as a group of about **500 followers nationwide** "defending faith, family, and folk against the politicians and oligarchs who are running America into the ground." It's **led** by **Matthew Heimbach,** a **discredited Trump convention delegate,** who is viewed as a **rising force within the white supremacy movement.**

United Kingdom / Royaume-Uni

5- *The Times of London* reports a **Polish community centre in Hammersmith** was daubed with **racist graffiti** and **far-right demonstrators chanted abuse outside a mosque** in **Birmingham** amid a **surge** in **suspected hate crimes** following the referendum vote to leave the European Union.

Europe

6- Selon *Le Figaro et l'Agence France-Presse,* un **commissaire de police sera jugé à Nanterre pour "violences" sur une avocate, soupçonné de l'avoir giflée lors d'une garde à vue à la Direction centrale du renseignement intérieur (DCRI, devenue DGSI) en avril 2014,** des faits

qu'il conteste. Le policier, 58 ans, toujours en poste à la Direction générale de la sécurité intérieure, comparaît devant le tribunal correctionnel pour "violences volontaires par une personne dépositaire de l'autorité publique sur un avocat dans l'exercice de ses fonctions". Le 1er avril 2014, l'avocate, inscrite au barreau des Hauts-de-Seine, avait accusé le commissaire de l'avoir giflée et insultée alors qu'elle assistait un **suspect gardé à vue dans les locaux du service antiterroriste et de contre-espionnage à Levallois-Perret, près de Paris.**

7- In a **rare intervention** into **Russian politics**, **Edward Snowden** has publicly **criticized enhanced anti-terrorism and surveillance legislation** recently passed by the State Duma as **"dangerous"** reports Britain's *Daily Telegraph.* Meanwhile, *New York Magazine,* in a cover story, has word there's a sense **Snowden is lonely in Russia** with his **conversation preoccupied with the theme of escape.** Snowden is said to muse that although he lives in Russia, he does not expect to die there and is **optimistic he will find a way out.**

8- *Le Soir, (Belgique),* rapporte qu'il y a eu interpellation à **Anvers d'un membre de Sharia4Belgium rentré de Syrie.** Les suspects interpellés à Celles et à Ensival ont été inculpés de **participation aux activités d'un groupe terroriste**. Le parquet fédéral a démenti l'information selon laquelle le duo préparait un attentat lors d'une retransmission publique du match Belgique-Hongrie. Deux suspects ont été inculpés de participation aux activités d'un groupe terroriste et placés sous mandat d'arrêt à la suite de **deux opérations de police menées à Ensival (Verviers) et à Celles (Tournaisis)** dans la nuit de vendredi à samedi. L'un des deux inculpés serait **E.S., un jeune homme de 20 ans domicilié dans la cité Armand Dederich, à Ensival.**

Africa / Afrique

9- **Buri Mohamed Hamza, Somalia's State Minister** for the **Environment** with **dual Somali-Canadian citizenship** and **family in Woodbridge**, was among **15 people who died** as a result of a **powerful car bomb** which **exploded outside** the **Nasa-Hablod hotel in Mogadishu** on the weekend reports *CBC News.*

Middle East / Moyen-Orient

10- *Al Jazeera* reports that weapons shipped into Jordan by the **Central Intelligence Agency** and Saudi Arabia intended for Syrian rebels have been systematically stolen by **Jordanian intelligence operatives** and sold to arms merchants on the black market, according to American and Jordanian officials.

Afghanistan/Pakistan

11- Badly bruised and isolated terrorists will go for softer targets for their survival, warned army chief **General Raheel Sharif** on Sunday as he directed senior security officials to hunt the terrorists and **"pre-empt their moves to frustrate their designs,"** the *Express Tribune.*

12- The *Pajhwok Afghan News* reports that the **National Directorate of Security, the spy service** on Sunday claimed arresting an 11-member Haqqani network group in southeastern Khost province.

Australia, New Zealand / Australie, Nouvelle-Zélande

13- **Seven men, including three Australians and a New Zealander abducted in Nigeria last week have been released, according to a statement issued to media by their Australian employer last night**, *The Australian* reports. "Five of the men have been injured, two of them seriously, and all are currently receiving attention from a team of medical specialists," a spokesman for Perth-based mining company MacMahon said.

14- **Queensland Police have hired experts as they grapple with a soaring number of potential jihadists,** the *Courier Mail* notes. The number of radicalised suspects has significantly increased in Queensland and other states during the past two years, compelling police to reach out

for extra help. While police stress there is no imminent threat in Queensland, it is **believed the large number of social media platforms that terrorists use to groom foreign fighters, and a growing number of potential radicalised youth, have become a liability.**

Asia / Asie

15- The *Manila Bulletin* reports that government forces are prepared to thwart any security threat after the Islamic State terror group rallied its forces to focus their fighting on Southeast Asia, particularly the Philippines. The government earlier launched intensified operations against the **Abu Sayyaf Group (ASG)** responsible for various atrocities in the south, most recently the beheading of two **Canadian hostages**.
16- *The Pioneer* reports that with security agencies in India nabbing a number of the cadres of **Al Qaeda in Indian Subcontinent (AQIS)** module during the last one year, in a statement Al Qaeda chief Ayman al Zawahiri has expressed solidarity with those associated with the outfit here.
17- The *Yonhap News Agency* reports that the **United States' forces stationed in South Korea have expanded their aerial reconnaissance along the inter-Korean border** following **North Korea's recent launch** of Musudan intermediate-range ballistic missiles (**IRBM**).

Americas / Amériques

Light coverage / couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Friday, July 15 2016
le vendredi 15 juillet 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- The New York based website *'News Deeply'* tells the story of **Calgarian Christine Boudreau** and her **son Damian Clairmont**, who was **radicalized** and **died in Syria.** The **Service is mentioned throughout the story** with reporter Alexandra Bradford writing 'like so many mothers who lose their children to radicalization, Boudreau had no support; no one to help her cope with her new, tragic reality. **The CSIS banned her from telling anyone that Damian had joined Isis,** and so she spent her days pretending everything was fine'.

2- **Un simple camion qui fonce dans une foule. La méthode rappelle à plus grande échelle celle utilisée par Martin Couture-Rouleau, qui avait happé deux militaires avec sa voiture à Saint-Jean-sur-Richelieu en 2014**. Et elle pose tout un défi de sécurité aux forces de l'ordre chargées de protéger la population contre les actes terroristes. « C'est très difficile à contrer d'un point de vue de sécurité. C'est un modus operandi super simple, qui ne demande aucune dextérité technique. Aucunes forces de sécurité ne peuvent empêcher la circulation de véhicules », commente **Michel Juneau Katsuya, expert en questions de sécurité nationale et ancien cadre et agent de renseignements au Service canadien du renseignement de sécurité (SCRS)** à *La Presse+*.

Canada

3- **"Clear gaps"** in **how the federal government reports invasive surveillance practices may hide the true scope of police activities**, according to documents prepared for **Canada's privacy watchdog**. Although the number of authorized wiretaps has "plummeted" since 2002, a January briefing for **Privacy Commissioner Daniel Therrien** suggests those numbers **may mask police surveillance practices**. "It would be erroneous to infer from the drop in overall warrants issued that surveillance is affecting fewer individuals," reads the document, obtained under access to information law, the *Toronto Star* writes.

4- A **Chinese man who ran an aerospace firm with offices in British Columbia has been sentenced to nearly four years in jail for stealing confidential information on a U.S. military transport aircraft and the F-35 stealth fighter**. The *Ottawa Citizen* writes that Su Bin had pleaded guilty in federal court in **Los Angeles to helping two Chinese military hackers.** Among the targets of the hacking efforts was information on the U.S. F-22 and F-35 stealth fighters as well as Boeing's C-17 transport aircraft, which is also used by the **Canadian Air Force**. Su did not carry out the actual hacking, which was done by his **two co-conspirators, both members of the People's Liberation Army in China.**

5- Réagissant au drame survenu à Nice, en France, le **premier ministre Justin Trudeau a déclaré que « les actes insensés de ce genre ne sont pas des gestes isolés » . Tard jeudi, un camion a foncé dans une foule de gens réunis pour célébrer la fête nationale en France, faisant au moins 80 morts. Le président français, François Hollande, a parlé d'une attaque « dont le caractère terroriste ne peut être nié »** . M. Trudeau a affirmé par communiqué que le Canada continuerait à travailler avec ses alliés et ses partenaires afin de « combattre le terrorisme sous toutes ses formes » . « J'ai eu le coeur brisé en apprenant que plusieurs douzaines de victimes innocentes avaient été tuées ou blessées à la suite d'un attentat terroriste perpétré lors des célébrations de la fête nationale du 14 juillet à Nice, en France » , a-t-il déclaré. « **Nous**

traduirons les responsables en justice, qu'il s'agisse des auteurs ou de ceux qui participent au financement ou à l'organisation de ces attentats » , a poursuivi le premier ministre indique *La Presse canadienne.*

6- The man that says he lives on the Internet will be the showcase speaker at SecTor, a **Toronto-based security conference this year. Edward Snowden**, the **former CIA employee and government contractor that leaked classified documents about a mass surveillance operation run by the National Security Administration (NSA),** will be appearing at the conference via a video link from Russia, where he's been living under asylum since 2013 *itWorld News* reports. **SecTor** will be Snowden's first and only commercial conference appearance in North America this year, conference organizers say. Beyond NSA's clandestine mass surveillance operations that were leaked by Snowden, Canada's **Communications Security Establishment (CSE)** has also been the subject of some of his classified leaks. He's also said that **Canada's intelligence gathering** operations have the "**weakest oversight" among western nations.**

International

United States / États-Unis

7- **No credible terrorist threat** has been **detected** but **Jeh Johnson** and **James Comey**, reports *Reuters,* told the House Homeland Security Committee that their **agencies** are **preparing for possible violence** at the **Republican National Convention** in Cleveland next week and the **Democratic convention** in Philadelphia the week after. DHS director **Johnson** said he was **concerned** any **demonstrations** could **get out of hand** and **Comey** added the **FBI** was **monitoring** the **threat of violence "very, very carefully".**

8- Appearing before the House Foreign Affairs Committee, **State Department official Richard Stengel,** reports the *Washington Free Beacon,* testified State's latest effort to **counter Islamic State propaganda** and **recruitment** is **relying on foreign states** for **strategic messaging** because the government believes **other countries** can **better deal with terrorist information operations** than the United States. "Our strategy is informed by a core insight: we are not always the best messengers for the message we want to deliver," Stengel said. "Public statements from U.S. government officials condemning ISIL can easily be used by the enemy as a recruitment tool."

United Kingdom / Royaume-Uni

9- Brexiteer **Boris Johnson's** selection as **British Foreign Secretary** has been greeted in **Europe** with **dismay** with **French Foreign Minister Jean-Marc Ayrault** denouncing him as a **"liar"** and **former Swedish Prime Minister Carl Bildt** tweeting **"I wish it was a joke".** (Extensive coverage / vaste couverture).

Europe

10- Selon *Nice Matin*, l'auteur présumé de **l'attentat survenu à Nice qui a fait 84 morts et de nombreux blessés est Mohamed Lahouaiej Bouhlel. Ce Niçois franco-tunisien était connu des services de police** pour des faits de délinquance et de violences conjugales, **mais n'était pas fiché pour radicalisation.** Il avait été placé en garde à vue pour des violences mineures en début d'année à Nice. **Il a été abattu par deux gardiens de la paix.**

11- À 4 heures du matin, le bilan de ce carnage était "extrêmement lourd: **80 morts, 18 personnes en urgence absolue et de nombreux blessés", selon Bernard Cazeneuve. Le ministre de l'Intérieur avait atterri deux heures plus tôt à l'aéroport de Nice. Aussitôt, l'hôte de la place Beauvau a rendu visite à la cellule de crise organisée dans les locaux de la préfecture au Cadam.** Ensuite, il a participé à "une assez longue réunion de police" au palais de la Méditerranée, devant lequel le camion a été neutralisé. Enfin Bernard Cazeneuve est allé salué

les pompiers à la caserne de Magnan avant de s'exprimer pendant une petite dizaine de minutes face à la presse, au pied de la fontaine de la place Masséna. Le ministre a tenu "à exprimer la solidarité du gouvernement". **Bernard Cazeneuve a confirmé que le niveau d'alerte pour le département des Alpes-Maritimes était "relevé à plan Vigipirate attentat"** rapporte *Nice Matin.*

12- It's reported this morning by *Nice-Matin* that a **local 31-year-old delivery truck driver Mohamed Lahouaiej Bouhle,** who had a **criminal record** but was **not known to French intelligence**, was **behind the wheel** of a **25 tonne transport truck** which **plowed at high speed** into a **crowd** celebrating Bastille Day in **Nice** last evening **killing at least 84 people** and injuring many more. The **Tunisia-born Bouhle** was **shot dead** by authorities after he zig-zagged the vehicle through those gathered along the seafront Promenade des Anglais knocking people down "like skittles". **President Francois Hollande** called it a **terrorist act,** extending the existing state of emergency for another three months. **Bouhle** is described as a **'loner'** who **appeared in court** as recently as **this past March** when he was **found guilty** of **violent contact** The *Daily Beast* recalls that **vehicle ramming attacks** were the subject of **two warnings issued jointly** by the **FBI** and the **U.S. Department of Homeland Security** in **2010** and **urged** by **al Qaeda's online magazine *Inspire*** the same year. As the Brookings Institution's William McCants put it to the *Wall Street Journal,* "You have to have a driver's license and that's it. There's nothing more to it."

13- D'après *Ouest-France,* dès 2014, une **note de la Direction générale de la sécurité intérieure (DGSI) révélait qu'un attentat visant le canaval de Nice avait été déjoué. En mai dernier, c'est le principal recruteur de djihadistes français, Omar Diaby, également originaire de Nice, qui refaisait parler de lui.** L'attentat de ce jeudi soir n'est pas le premier à viser Nice. En 2014, une attaque visant le carnaval, l'un des plus célèbres du monde, attirant chaque année plusieurs centaines de milliers de personnes sur la Côte d'Azur, avait été déjoué par les services de sécurité. **Des explosifs artisanaux dans des canettes Ibrahim Boudina, un Français de 23 ans avait été arrêté deux jours avant le début des festivités.**

14- Russia's **FSB,** reports *Reuters,* said it would **reprimand dozens** of **new agents** who **celebrated graduating** from the agency's training academy by **ostentatiously driving** through Moscow in a **luxury convoy,** allowing themselves to be photographed.

Africa / Afrique

15- Selon *Tel Quel,* (Maroc), le **ministère marocain de l'Intérieur a annoncé le 14 juillet le démantèlement d'une cellule terroriste composée de six personnes. La cellule agissait dans les villes d'Agadir, Amzmiz, Chichaoua et Laqliaâ**. Selon le ministère, ces personnes projetaient« de viser des installations vitales et sensibles en perpétuant des attaques d'envergure ». Elles comptaient y mener des attaques « à l'aide de bombes » et par « des attentats-suicides ».

Middle East / Moyen-Orient

16- The *National Iraqi News Agency* reports that President of the Kurdistan Regional Government Nechirvan Barzani discussed with **Canadian Defense Minister Harjit Sajjan liberation the city of Mosul from Daash** and cooperation between the coalition forces and the Iraqi army and the Peshmerga forces and plan to administrate after liberation.

17- *Now Lebanon* reports that **Amer al-Ashi, a top officer in the Syrian regime's feared Air Force Intelligence Directorate** has been appointed governor of the Druze-populated Suweida province, where a number of movements have sprung of challenging government authority.

Afghanistan/Pakistan

18- *Pajhwok Afghan News* reports that **former intelligence chief Rahmatullah Nabil** on Thursday shared some documents along with a write-up with media persons 'proving Pakistan's relations with Taliban.'

Australia, New Zealand / Australie, Nouvelle-Zélande

19- **China** yesterday called in **Australian ambassador to Beijing Jan Adams** for a briefing to contain the damage from an international court ruling that its island building in the **South China Sea was illegal.** The *Australian* writes that Ms Adams was among a number of envoys from countries Beijing considers influential to be called in for a special briefing from foreign ministry officials in the wake of Tuesday's night ruling by the Permanent Court of Arbitration that shredded its sovereignty over 90 per cent of the South China Sea.

20- The **Australian Defence Force** is working on ways to disable remote-controlled model helicopters being used by the **Islamic State in Iraq to spy on Iraqi forces**. And the general in charge of **modernisation and strategic planning in the Australian Army, Gus McLachlan**, said it was likely to be only a matter of time before the terror group packed explosives into these off-the-shelf toys and used them to carry out attacks, the *Australian* writes.

Asia / Asie

21- **North Korea today paraded a defector** accused of involvement in a child abduction plot it says was masterminded by **South Korean agents**, as Seoul demanded the man's immediate release. In a carefully stage-managed press conference in Pyongyang, **Ko Hyon-Chol**, 53, who fled the North in 2013 and was granted South Korean citizenship, "confessed" to attempting to kidnap two orphans and take them to the South. Ko's case comes amid an ongoing dispute between North and South Korea over the April defection to the South of a dozen North Korean women working in a restaurant in China. Pyongyang insists that the women were kidnapped by the South's spy agency -- the **National Intelligence Service** (NIS) -- but Seoul says they fled of their own free will. (Extensive coverage / vaste couverture).

22- The *Times of India* reports that in a **clear message to China to desist from using strong-arm tactics in the South China Sea**, India and Japan on Thursday asked "all parties" to show "utmost respect" for the UN Convention on the Law of the Sea (UNCLOS) of 1982.

The *Associated Press* reports that ineffectual attacks by **ISIL's South-east Asian** followers have shown them to be fragmented and lacking in the expertise that has produced devastating death tolls elsewhere in the world.

23- Japanese Prime **Minister Shinzo Abe told Chinese Premier Li Keqiang that rule-based international order must be respected** in talks on the sidelines of the **Asia-Europe Meeting (ASEM) today,** the *DPA News Agency* reports. The ASEM summit has been overshadowed by the dispute over China's territorial claims in the **South China Sea**.

24- **South Korea will respond firmly to all North Korean threats made against the deployment of the U.S. antimissile system on its soil**, the government said today, making clear that the move is designed to counter Pyongyang's evolving nuclear and missile capabilities, the *Yonhap News Agency* reports.

Americas / Amériques

Light coverage/couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Wednesday, July 20 2016
le mercredi 20 juillet 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- Canada's electronic spy agency won't say how often it shares information that could lead to someone being tortured in an overseas prison. The **Communications Security Establishment** - which monitors threats from foreign terrorists and spies - has censored documents that spell out the figures, even though the **RCMP** and **Canadian Security Intelligence Service** have revealed such numbers in the past. The reticence prompted **Amnesty International Canada** to say "**much greater transparency**" is needed from the Ottawa-based CSE. "At stake is Canada's compliance with crucial international human rights obligations to prevent torture and ill-treatment," said **Alex Neve**, Amnesty's Canadian secretary general. The secretive CSE has been thrust into the national spotlight in recent years due to leaks by **Edward Snowden**, the former spy contractor who worked for the **National Security Agency**, CSE's American counterpart. It is also among a handful of Canadian agencies, including the **RCMP**, **CSIS**, the **Canada Border Services Agency** and **National Defence**, bound by a government instruction that allows it to share information with foreign partners - even when it means someone could be abused as a result of that exchange. Records obtained by *The Canadian Press* under the Access to Information Act offer a glimpse into how the CSE handled such cases in the first three months of 2015. The quarterly report to CSE Chief **Greta Bossenmaier**, labelled Top Secret and for Canadian Eyes Only, told her the number of cases that required a "**mistreatment risk assessment**" and the level of risk associated with passing the information to others. But those details were deleted from the publicly released version of the document. The report says there were "**no known instances" of a recipient country's non-compliance with conditions attached to information-sharing during the three months**. But little else was disclosed. The CSE faces "unique considerations" it must weigh when discussing details of assessments, said **Christopher Williams**, a senior spokesman for the intelligence agency. "With this in mind, we are not able to release the specific number you have requested without risking revealing insight into our capabilities." However, the number and content of such assessments are reviewed by the independent watchdog who keeps an eye on the CSE, said Williams.

Canada

2- Bangladeshi police have confirmed that a **University of Toronto student is being interrogated**, without clarifying his whereabouts or his condition, or saying whether he was being charged – escalating concerns over **possible human-rights violations in his detention**. **Tahmid Hasib Khan**, 22, and a fellow detainee, British citizen **Hasnat Karim**, 47, were among several hostages who survived a terrorist attack at a restaurant in Dhaka that left 23 people dead on July 1. They were then taken in by police for questioning, writes the *Globe and Mail*. Family members have had no contact with Mr. Khan since July 3, aside from a phone call from an unknown agency confirming his detention. "We have to conduct the investigation through interrogation of witnesses, rescuers and others concerned. The puzzle cannot be solved without interrogation," the Dhaka Metropolitan Police commissioner said, according to a report in *The Dhaka Tribune* newspaper.

3- A dysfunctional compensation system that's withholding paycheques from federal workers has also been breaching their privacy, *CBC News* has learned. Newly released documents show senior

officials were warned as early as Jan. 18 that the new Phoenix system has a flaw that allows **widespread access to employees' personnel records, including social insurance numbers.** Despite the warning, the faulty software was broadly implemented this spring — **without alerting the unions or any employees that their private details were no longer** secure. The disclosure of a massive privacy breach appears in documents obtained by *CBC News* under the Access to Information Act, deepening a crisis that has already touched some 80,000 public servants and triggered a wave of hiring to patch the problems.

International

United States / États-Unis

4- *Washington Post* columnist **David Ignatius** refers to an **upcoming forecast** by the Washington-based **Institute for the Study of War** which states that by **January 2017,** the **Syrian al Qaeda affiliate Jabhat al-Nusra** "will have **created an Islamic emirate in northwestern Syria in all but name** and will **merge** with the supposedly more **moderate Ahrar al-Sham.** The merger, even if incomplete, will accomplish a major Jabhat al-Nusra objective to unify the northern Syria opposition under its own leadership".

United Kingdom / Royaume-Uni

Light coverage/couverture légère.

Europe

5- En **dernière heure**, *l'Agence France-Presse* rapporte que **trois militaires français ont été tués en Libye**, a annoncé le ministère français de la Défense, **confirmant ainsi pour la première fois la présence de soldats français dans ce pays**. "Le ministre de la Défense, **Jean-Yves Le Drian**, déplore la perte de trois sous-officiers français décédés en service commandé en Libye", a annoncé dans un communiqué le ministère, sans plus de précisions.

6- En entrevue à L'*Express,* **l'ancien patron du renseignement, sous la présidence de Nicolas Sarkozy, Bernard Squarcini livre son diagnostic sur l'état de la lutte antiterroriste. Il recommande notamment de recourir aux compétences de spécialistes non policiers, pour mieux définir les priorités**. Comment expliquer que **Mohamed Lahouaiej Bouhlel ait pu effectuer près de 2 kilomètres au volant du camion** et provoqué la mort de plus de 80 personnes avant d'être intercepté? La question est légitime, d'autant plus que Nice est une ville bien sécurisée.

7- **Isis** released a **video** yesterday showing **'Muhammad Riyad',** the **17-year-old perpetrator** of the **axe attack** on a **Bavarian commuter train,** proclaiming in Pashto that **"I will do a martyrdom operation in Germany today."** The teenager **pledged allegiance to Isis** saying **Islamic State fighters** had **settled in "infidel" countries,** vowing: "God willing, you will be targeted in your villages, in your cities, in your airports, in your streets. The Islamic caliphate is strong enough to target you everywhere, even in your Parliament." While **German authorities** have **authenticated the video,** they now believe the **attacker**, who **registered in Germany** under the name **'Riaz Kahn'** and is identified in some media reports as 'Riaz A', is **not from Afghanistan,** but rather a **Pakistani** who pretended to be Afghan on arrival in Germany in 2015 in order to have a better chance at securing asylum. (Extensive coverage / vaste couverture).

8- The **FSB raided** the **Moscow offices** of the **Investigative Committee** Tuesday, a move the *New York Times* called **'baffling'** and a **'rare sign of dysfunction** in the **country's domestic security services'**. The FSB **arrested a deputy head** of the headquarters **Denis Nikandrov** on **suspicion** of **taking a bribe** from **Organized Crime** and the two top officials in the department of internal affairs, **Mikhail Maksimenko** and **Aleksandr Lamonov.**

Africa / Afrique

9- **Human Rights Watch** says **security agencies** are **killing** and **abducting men** in **northeast Kenya** who they suspect of **links to Islamist extremists** reports *Agence France-Presse*.
10- Selon *Le Matin*, un élu de Nampala au Mali a déclaré que des **hommes armés ont attaqué mardi le Camp de Nampala.** Il appert que les assaillants «ont actuellement le contrôle du camp, il y a des victimes, mais on n'a pas encore le nombre exact», a indiqué l'élu. Les attaques jihadistes ont été longtemps concentrées dans le nord du Mali, mais elles se sont étendues à partir de 2015 vers le centre, puis vers le sud du pays. **Le centre du Mali est une zone où est basé le Front de libération du Macina (FLM), un groupe apparu début 2015 et dirigé par le prédicateur radical malien Amadou Koufa, un Peul.**

Middle East / Moyen-Orient

11- *Reuters* reports that **European powers** are trying to develop better means for pre-emptively spotting **"lone-wolf" militants** from their online activities and are looking to Israeli-developed technologies, a senior EU security official said yesterday.
12- The *Jerusalem Post* reports that the **Islamic State terrorist group reportedly has dormant sleeper terror cells** in Syrian refugee camps in Lebanon which it may activate, according to a recent Western embassy report.
13- *Asharq Al-Awsat* reports that **experts in radical Islamist groups' affairs** have warned of ISIS's dodging approach and the increasing terrorist attacks it is staging in many countries around the world.

Afghanistan/Pakistan

Light coverage/couverture légère.

Australia, New Zealand / Australie, Nouvelle-Zélande

14- Amid growing concerns about Beijing's assertiveness in the **South China Sea**, **Malcolm Turnbull** and US Vice-President **Joe Biden** have pledged to **step up joint military training to deal with "any challenge"** in the region. Australia has also agreed to **broaden its training commitment in Iraq**, to instruct law enforcement officers in **counter-terrorism techniques to help them retain areas recaptured from Islamic State** and keep order there. Mr Biden said there would be a greater unity between US and Australian forces, stressing "it's important that we stand together". "We also discussed steps Australia and the US are taking so our troops can train more together and increase our interoperability so that we are fully prepared to respond to any challenge — to any challenge — in the Pacific with a united front," Mr Biden said after talks with Mr Turnbull in Sydney. On Iraq, *The Australian* has been told Mr Turnbull and Mr Biden shared a strong view that as more areas were recovered from ISIS, it was crucial they should be stabilised. Law enforcement training will be carried out by **Australian Defence Force** instructors already in Iraq and will not require sending additional trainers.

Asia / Asie

15- The *New York Times* reports **Bangladeshi-Canadian Tamim Chowdhury** is the **'most talked about'** of the **10 'high-value' Isis recruiters** being sought by authorities in Bangladesh. **Chowdhury** is believed by some analysts to act as a **coordinator** of the **Islamic State's activities in Bangladesh** and **parts** of **northeast India. Zayadul Ahsan Pintu**, a **journalist** who has published widely on the country's militant networks, said **"Chowdhury, in particular**, "is the **connection** from **Bangladesh** to **Syria**."
16- According to *Yonhap News Agency*, South Korea's government on Wednesday **condemned North Korea's resumption of encrypted number broadcasting**, a method used in the past to send orders to its spies operating in the country. The Ministry of Unification expressed "deep regret" over the North's latest provocation. Pyongyang on Friday resumed the broadcasting after a 16-year-long hiatus following Seoul's decision a week earlier to deploy an advanced U.S.

antimissile system in South Korea by the end of 2017. "We can't speak conclusively about North Korea's hidden intentions behind the broadcasting. But we urge North Korea desist from such outdated practices and seek ways to promote inter-Korean ties," Unification Ministry spokesman Jeong Joon-hee said in a press briefing. South Korean intelligence authorities are reportedly trying to figure out why Pyongyang resumed this type of communication, particularly in the digital era when it could have simply given out orders via the Internet.
17- Tough religious restrictions on Muslim minorities in China's far west **may have driven more than 100 to join the Islamic State group**, a US think tank said Wednesday. Beijing has long claimed that **IS is recruiting Uighurs from the mainly Muslim region of Xinjiang**, and blamed outside forces for fomenting deadly acts of violence there and elsewhere in China that have claimed hundreds of lives. At the same time, authorities have banned or strictly controlled the observance of certain Muslim practices, such as growing beards and fasting during Ramadan, saying they are symbols of "Islamic extremism". Those policies "could be a push factor driving people to leave the country and look elsewhere for a sense of 'belonging'", the Washington, DC-based **New America Foundation** wrote in a study of leaked registration documents for IS fighters. The findings were based on data from more than 3,500 foreign recruits provided by a defector from the jihadist organisation, writes the *Agence France Presse.*
18- *Press Trust of India* reports that **ISIS operatives in India** had approached Naxalite groups to understand their modus operandi for perpetrating terror and were also planning to buy firearms from them, NIA has said, revealing the sinister plans of the international terrorist outfit.
19- *BDNews24* reports that **Prime Minister Sheikh Hasina** has said that a "special team" comprising members from all the **security agencies** has been formed to probe the root of the current terror menace in Bangladesh.

Americas / Amériques

20- **Brazilian intelligence**, reports *Reuters,* is **investigating all threats** to next month's **Rio Olympics** after a presumed **Brazilian Islamist group** called **'Ansar al-Khilafah Brazil' pledged allegiance** to **Islamic State. Some terrorism experts** in the **United States** are wondering if **Ansar al-Khilafah Brazil even exists** though a **U.S. counter-terrorism official** told *ABC News* that while **Isis isn't known to have any cells in Rio de Janeiro**, "we **should take every threat like this seriously**."

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Friday, July 22, 2016
le vendredi 22 juillet 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

Light coverage / couverture légère.

Canada

1-The **Turkish government is calling on Canada to "take the necessary steps**" to address what it describes as a **terrorist organization responsible for last week's failed coup**. Turkish Consul-General **Erdeniz Sen** told *The Globe and Mail's* editorial board Thursday that his country, which has detained thousands of people since the attempted coup, has "concrete evidence" that the followers of the religious cleric **Fethullah Gulen**, who now lives in selfimposed exile in the **United States**, are behind the plot. Mr. Gulen has denied involvement. Mr. Sen declined to say whether there are **specific actions** it has asked the **Canadian government to take**, but said it's a subject his **country has raised routinely with its Canadian counterparts in the context of terrorist threats.**

2-Public servants had their **private information breached twice when Ottawa launched its new computerised pay system, the government said Thursday**. The deputy minister of Public Works, **Marie Lemay**, confirmed the incidents in an open letter to staff posted on the department's web site Thursday afternoon. The statement comes two days after *CBC News* first reported **on privacy problems caused by 'Phoenix'.**

International

United States / États-Unis

3-Speaking to *Washington Post* columnist David Ignatius, Director of National Intelligence **James Clapper questioned the recent "groundswell" of concern** about **Jabhat al-Nusra**, saying the Syrian al-Qaeda affiliate poses only a "**nascent" danger to the U.S. homeland** and **"doesn't approach the threat"** posed by the **Islamic State.** Jabhat al-Nusra's ability to **attack the United States** and **Europe** is **"aspirational" rather than "imminent,"** he said, describing as overly "strident" recent news reports about increasing evidence of external plots by the group. As for **Turkey's claim** that cleric **Fethullah Gulen planned the attempted coup,** Clapper commented it **lacks credibility** and that Secretary of State John F. Kerry "was right on the ball" to press the Turks to back up their extradition request with evidence of Gulen's involvement. "We haven't seen it yet. We certainly haven't seen it in intel."

4-*The Intercept* reports **Edward Snowden** has been working with **prominent hardware hacker Andrew "Bunnie" Huang** to develop a way for **potentially imperiled smartphone users** to **monitor** whether their devices are making any **potentially compromising radio transmissions.**

United Kingdom / Royaume-Uni

5-Rumors which have been circulating in the British media that **Foreign Secretary Boris Johnson** will **not oversee MI6** and **GCHQ** as is customary have been **squelched** by the **Foreign Office** which informed *Politics.co.uk.* "as has been long standing practice, responsibility for SIS and GCHQ lies with the foreign secretary. This has not changed and will not change".

6-Figures released by the **Office of National Statistics** say that **one in ten British adults** have been **victims of cyber-crime** reports the *Times of London.* An estimated **5.8 million** fraud and **cyber-offences** are committed annually.

Africa / Afrique

7-**President Muhammadu Buhari** announced the **Nigerian government** is in **talks** with the militant **Niger Delta Avengers** in an effort to end a string of **attacks** on oil **and gas facilities** reports *Reuters.*
8-Le Mufti de la Libye considère la présence de soldats français sur le sol libyen comme une déclaration de guerre. Le **Mufti de la Libye, Saddok Al-Ghariani, a estimé que l'annonce par le ministère français de la Défense de la mort de trois de ses soldats à l'ouest de la ville de Benghazi constituait une "déclaration de guerre"** à la Libye, appelant les **Libyens à dénoncer cette ingérence rapporte** *Pan African News Agency.*

Middle East / Moyen-Orient

9-The *Fars News Agency* reports that Iranian Interior Minister Abdolreza Rahmani Fazli announced that the country's **security forces** have discovered a secret tunnel in Eastern Iran that the **terrorists sought to use for sabotage operations**.
10-The *Jerusalem Post* reports that **Al-Qaida-influenced terrorists** have issued directives to **"lone wolf" attackers** to carry out attacks against the Israeli Olympic delegation at the upcoming Rio Olympics, The Foreign Desk reported Thursday.
11-*Naharnet Newsdesk* reports that **Kuwait's court of appeals** on Thursday upheld the death sentence to a Shiite citizen and Hizbullah member convicted of forming a **pro-Iran cell and plotting attacks** in the Gulf state.

Afghanistan/Pakistan

12-The *Pakistan Dawn* reports that India on Thursday alleged that the protests in India-held Kashmir during observance of **'Kashmir's Accession to Pakistan Day'** and 'Black Day' were led by UN-designated terrorists.
13-*Pajhwok Afghan News* reports that a **would-be suicide bomber**, who was after **First Vice-President Gen. Abdul Rashid Dostum** to assassinate him during Eid days, has been arrested in northwestern Jawzjan province, local officials said on Thursday.

Europe

14-In conversation with *Reuters,* **Turkish President Erdogan** said there were **significant intelligence failures** ahead of last week's attempted military coup. "It is very clear that there were **significant gaps** and **deficiencies in our intelligence**, there is no point trying to hide it or deny it. I told it to the head of national intelligence," Erdogan said. **Yasin Aktay**, the **deputy chair** of the ruling **AKP Party,** disclosed to Russia's *Sputnik* that **Turkish intelligence** had those **involved** in the **coup attempt under surveillance. "There were lists [of participants before the coup]. The country's intelligence spied on all of them**… Of course it knows who is who but everything is in line with the law. We never struggle with people only because they are adherents of a certain organization or have certain political views," Aktay said.
15-Both **Amnesty** and **Human Rights Watch** have accused **Ukrainian intelligence** of engaging in **abuse** and **torture** during the current conflict with rebel separatists, a **charge the SBU denies.** However, the *New York Times* points out as recently as May, the SBU **refused** to allow a **United Nations delegation** investigating reports of torture **access to sites** where **suspects were alleged to be held illegally.**
16-Selon *Radio France Internationale,* une **opération anti-terroriste a été menée jeudi dans la ville d'Argenteuil**, dans le Val d'Oise. Deux logements étaient visés. Les **policiers de la Direction générale de la sécurité intérieure (DGSI) avec l'appui des policiers d'élite du Raid**

ont perquisitionné à Argenteuil à deux adresses différentes. Cette opération est sans rapport avec l'attaque menée le 14 juillet à Nice, elle visait à vérifier un renseignement anonyme faisant état d'un **projet d'action violente, a indiqué une source policière, qui a précisé que la section antiterroriste du parquet de Paris est saisie des investigations**. Les policiers sont sortis avec trois femmes et un homme menottés d'un des deux endroits visités. Lors de la visite du second logement, deux personnes ont été arrëtées.
17-Le 20 juillet, la **Sous-direction antiterroriste (SDAT) a envoyé aux agents qui gèrent la vidéosurveillance de la ville de Nice une « réquisition judiciaire urgente » leur demandant « l'effacement complet des enregistrements de vidéosurveillance de l'ensemble des caméras desservant la promenade des Anglais** filmant pour la plupart d'entre elles **l'action terroriste commise le soir du 14 juillet »** . « C'est la première fois que l'on nous demande de détruire des preuves, précise une source proche du dossier rapporte *Le Figaro.*

Australia, New Zealand / Australie, Nouvelle-Zélande

18-**Malcolm Turnbull** has ordered **Australia's counter-terrorism agencies to urgently develop a strategy to prevent rapidly radicalised terrorists carrying out Nice-style attacks in public areas**. Senior sources have told the *Australian* the Prime Minister is particularly concerned that while it would be hard for a **terrorist to obtain a cache of automatic weapons here**, an **attack using a vehicle as a weapon** could cause devastating casualties.

Asia / Asie

19-The *Times of India* reports that days before Bangladesh home minister Asaduzzaman Khan Kamal is to visit India, the **National Investigation Agency (NIA)** has been asked to probe the Dhaka link to Islamic State operative Abu Al-Musa Al-Bangali, who was arrested from Burdwan two weeks ago.
20-The *Dhaka Tribune* reports that investigators suspect that the three local militant groups who carried out the **Gulshan terror attack** were assisted by several foreign extremist groups as well as some home-grown militant leaders now staying abroad. A key suspect behind the Gulshan terror attack is **Bangladesh-origin Canadian citizen Tamim Ahmed Chowdhury**.
21-South Korea is beefing up its government wide countermeasures to prevent **possible cyberattacks by North Korea,** officials said Friday. The **Ministry of Science, ICT and Future Planning** said the number of **cyberattacks by North Korea more than doubled in the first half of this year**. The cyberattacks **"are judged as a part of North Korean provocations to trigger public anxiety"** in South Korea, the ministry said. Last month, South Korean police said North Korea hacked into more than 140,000 computers at 160 South Korean firms and government agencies. About **42,000 documents were suspected to have been stolen, including defense-related information**, writes the *Yonhap News Agency.*
22-According to the China Daily, Islamic leaders in China urged Muslims **not to fall into the trap of religious extremism** and vowed to improve their guidance to help believers stay on the peaceful path of Islam. **"War and violence are never seen as holy in Islam. The extremists' theories of going to heaven after killing and treating non-Muslims as enemies are just not among the teachings,"** said **Ma Guangyue,** imam of Laowang Mosque in Gansu province, at an international forum on eliminating religious extremism on Thursday. About **100 Islamic leaders and scholars from China, Russia, Kyrgyzstan, Tajikistan, Uzbekistan and Kazakhstan participated in the two-day forum** held in Urumqi, capital of the Xinjiang Uygur autonomous region. The forum started on Wednesday.

Americas / Amériques

23-**Brazil's Justice Minister Alexandre de Moraes** said the **10 people arrested yesterday** on suspicion of **supporting** the **Islamic State** and preparing acts of **terrorism** during next month's **Olympics in Rio,** were an **"absolutely amateur cell, with no preparation at all, a**

disorganized cell". de Moraes said those apprehended were **all Brazilian citizens** and in contact via internet messaging groups such as WhatsApp and Telegram, but **did not know each other personally** and were **not in direct contact with Isis** though some of its members had made **"pro forma" declarations of allegiance** to the militant Islamist group. It's **unclear** whether **any of the 10** were members of the extremist **'Ansar al-Khilafah Brazil'**.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Tuesday, August 16 2016
le mardi 16 août 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- Speaking to the *Toronto Star,* **Wayne Driver** said his **son Aaron** had been **estranged** from much of the family for years. **Driver supported** his **son's conversion** to **Islam** until he **realized how radical he had become**, explaining sometime around **Christmas 2014**, he was **contacted** by the **'Canadian Security Intelligence Committee'**. Driver recalled feeling **sick and perplexed** when shown an **inch-thick file** outlining his **son's online comments** saying it included photos of mass graves and people who had been beheaded, with his son allegedly claiming that the people depicted deserved to die. "I don't understand," the elder Driver said, noting that he's always felt such acts epitomize cowardice and cruelty. "It's not like butterflies. It's like somebody has punched you in the stomach."

2- **Ralph Goodale's media announcement** in Montreal yesterday that the **federal government** will allocate **$35 million** over five years on **de-radicalization programs doesn't impress Christianne Boudreau** who told Toronto radio commentator **Tasha Kheiriddin** (as related in Kheiriddin's column in *iPolitics*) that **"it's a camera, election, posturing thing. They really need to start putting action behind their words."** The column briefly notes that Boudreau's son, **Damian Clairmont, was under CSIS surveillance** for two years before he left Canada.

Canada

3- A **friend** of **Aaron Driver** described him to the *London Free Press* as a **"normal guy"** but the **death** of his **infant son** devastated him and **likely** played a **significant role** in his path to **radicalization.**

4- Selon *La Presse canadienne,* **à l'issue de sa tournée de collecte d'informations en Afrique, le ministre de la Défense dit avoir une idée très claire du nombre de soldats** qu'il déploiera dans des **missions d'appui à la paix sur le continent.** « J'ai un chiffre que nous annoncerons bientôt, et qui pourra être maintenu à long terme », a affirmé **Harjit Sajjan en conférence téléphonique depuis la République démocratique du Congo (RDC)**, lundi. Le ministre de la Défense n'a pas fourni davantage de précisions sur les pays et les régions où des Canadiens pourraient être déployés, disant ne pas disposer de toute l'information nécessaire à cette prise de décision. L'analyse des besoins ne se fera pas nécessairement par pays, mais bien par région, a expliqué le ministre.

International

United States / États-Unis

5- The Washington-based non-partisan think-tank the **Stimson Center,** reports *Agency France-Presse,* has compiled a study which warns **America's estimated stockpile** of about **50 nuclear bombs** at the **Incirlik military base** in **southern Turkey** are at **risk** of **being captured** by **"terrorists** or other **hostile forces"** and thus, from a security point of view, it's a **"roll of the dice"** to continue to have the weapons stored there.

6- A **mysterious hacker** or **hackers** going by the name **'The Shadow Brokers'** claims to have **hacked** the **'Equation Group', linked to the NSA,** and **dumped** a bunch of its **hacking tools.** In twist, the hackers are also asking for 1 million bitcoin (approx. $568 million) in an auction to

release more files. *VICE Magazine's* 'Motherboard' notes **Kaspersky Lab unmasked Equation Group in 2015,** billing it as the **most advanced hacking group** Kaspersky researchers had ever seen. While Kaspersky Lab **stopped short** of saying **it's the NSA,** its researchers laid out **extensive evidence pointing** to the **Agency,** including a long series of code names used by the Equation Group and found in top secret NSA documents released by Edward Snowden.

United Kingdom / Royaume-Uni

7- The *Indo-Asian News Service* reports that **British MPs** are being taught unarmed street-fighting techniques used by the **Israeli intelligence agency Mossad** in a bid to protect themselves from stalkers, terrorists, and political extremists in the light of Jo Cox's murder, it was reported on Monday.

Europe

Light coverage / couverture légère.

Africa / Afrique

8- A study released Monday by the **Intergovernmental Authority on Development** has identified **al Shabaab** as a **"Transnational Security Threat",** reports the *Washington Post,* posing a **rising menace** to **nations across East Africa** with its ability to **recruit young men** and **women from countries beyond** its **Somali power base.**

Middle East / Moyen-Orient

9- *The National (UAE)* reports that **security forces in Aden smashed an Al Qaeda cell** as the militants were preparing to detonate a car bomb in the Yemeni city.
10- *Press TV* reports that **security forces in Iran** have killed an "instrumental" member of the Takfiri terrorist group of Daesh and busted the **terror cell** he belonged to during clashes in the country's west, an Iranian official says.

Afghanistan/Pakistan

11- The *Pakistan Dawn* reports that Chief of Army Staff (COAS) General Raheel Sharif on Tuesday confirmed the **death sentences of 11 'hardcore terrorists' involved** in committing **"heinous offences related to terrorism,"** said an Inter-Services Public Relations statement.

Australia, New Zealand / Australie, Nouvelle-Zélande

12- The **New Zealand government is set to break a long-standing ban on the Government Communications Security Bureau (GCSB) spying on New Zealanders** with a sweeping revamp that brings our spy agencies under a single law. The *Dominion Post* explains that **Prime Minister John Key** yesterday said Cabinet had accepted the bulk of changes, including extra powers for the GCSB, as recommended by the Cullen-Reddy review in March. He said the changes were the most significant reform to the agencies' legislation in the country's history.

Asia / Asie

13- *Reuters* reports that **Bangladeshi authorities** named a third prime suspect on Monday in their investigation into the July 1 attack at a Dhaka cafe in which 20 hostages were killed, most of them foreigners. Police say **Tamim Ahmed Chowdhury, a Canadian citizen** and the prime suspect, is still at large in Dhaka. Analysts say ISIS identified him in April as its national commander.
14- *The Hindu* reports that asserting India's right to question **Tahawwur Rana**, a close associate of David Coleman Headley charged in the **2008 Mumbai terror attacks**, senior officials of the Home Ministry quietly visited the United States early this month to press for his extradition.

15- The *Yonhap News Agency* reports that **South Korea said today that more information is needed to analyze whether control of North Korea's intelligence agency** has changed following the latest overhaul of its cabinet organization. The **Ministry of State Security, Pyongyang's intelligence agency,** was previously placed under the control of the powerful **National Defense Commission (NDC)** before the country's parliament replaced the NDC with a newly created state apparatus named the State Affairs Commission (SAC) in late June.
16- **China has tested 21 new pieces of security equipment**, including drones, during a **counter-terrorism exercise** in the western region of Xinjiang, state media said today, as it strengthens its presence in the violence-prone area. *Reuters* points out that hundreds of people have been killed over the past few years in resource-rich Xinjiang, strategically located on the borders of central Asia, in violence between the **Muslim Uighur people** who call the region home and ethnic majority Han Chinese.

Americas / Amériques

Light coverage / couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Wednesday, August 17 2016
le mercredi 17 août 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- Addressing a supportive crowd in Bridgetown, Nova Scotia Tuesday, **Prime Minister Trudeau,** in his **first reaction** to the **death of Aaron Driver**, said that **balancing individual rights** with keeping **Canadians secure from threats** has to be **handled with care. Trudeau congratulated** the **security services** and police for ``having managed to prevent any serious incidents related to this particular individual." In its reporting, the *Canadian Press* observed that during the **last federal election**, the **Liberals pledged** to **guarantee** that **all Canadian Security Intelligence Service warrants respect** the **Charter** and also indicated they would **limit the Communications Security Establishment's powers** by requiring a warrant to engage in the surveillance of Canadians.

2- In the wake of the **Aaron Driver case**, **Phil Gurski,** a **radicalization expert** who **retired last year** after a career with the **Canadian Security Intelligence Service** and **Communications Security Establishment**, told the *National Post* that "I think it calls for a little more **in-depth assessment and analysis of these guys**. We have to come up with a system where **assessments are being done on a regular basis**. So what that means is you're going to have to have **other warrant powers,** or **source powers** or something. Or maybe you **talk to Driver once every two weeks** as opposed to **once every three months** kind of thing."

Canada

3- *Le Journal de Montréal* indique que le **collectif de pirates informatiques dénonce les scandales de corruption Le collectif Anonymous a piraté hier le site de l'Association des firmes de génie-conseil du Québec** qui n'a pas été impressionnée par les prouesses des pirates. Le visage de **Guy Fawkes**, symbole du groupe Anonymous, est apparu sur le site de l'Association des firmes de génie-conseil. Des **noms de dossiers ont aussi été remplacés par des termes faisant allusion au scandale de corruption comme «fraude», «détournement de fonds» «appels d'offres truqués».**

4- Meeting in Ottawa, the **Canadian Association of Chiefs of Police** has **passed a resolution** calling for a **legal measure to unlock digital evidence,** saying **criminals increasingly use encryption** to **hide illicit activities** reports the *Canadian Press*. There is **nothing currently in Canadian law** that would compel someone to **provide a password to police** during an investigation, **RCMP Assistant Commissioner Joe Oliver** said. In response, **David Christopher**, a spokesman for **OpenMedia**, a group that works to keep the internet surveillance-free, called the proposal **"clearly unconstitutional"**. Public Safety Minister Ralph Goodale is scheduled to address the Association this morning.

International

United States / États-Unis

5- Speaking confidentially to the *Washington Post,* **two former members** of the **NSA's hacking division** known as **Tailored Access Operations** (TAO), said they have **no doubt** the **online unmasking** of **Agency espionage tools** with **code names** such as **'Epicbanana', 'Buzzdirection'** and **'Egregiousblunder'** is **genuine**. "Without a doubt, **they're the keys to the kingdom**," said

one former TAO employee."The stuff you're talking about would **undermine the security** of a lot of **major government** and **corporate networks** both here and **abroad**."
6- On his **Twitter account** Tuesday, **Edward Snowden** speculated the exposure of espionage tools from the **'Equation Group'**, allegedly **linked** to the **National Security Agency, is likely a message from Moscow. "Circumstantial evidence** and **conventional wisdom** indicates **Russian responsibility,"** Snowden tweeted. "This leak is likely a warning that someone can prove U.S. responsibility for any attacks that originated from this malware server. That could have significant foreign policy consequences. Particularly if any of those operations targeted U.S. allies. Particularly if any of those operations targeted elections." (Extensive coverage / vaste couverture).
7- Accompanied by **Governor Chris Christie** and **national security advisor retired Lt. Gen. Michael Flynn, Donald Trump** is scheduled to receive his **first classified intelligence briefing** in **New York today.** (Moderate coverage / couverture modérée).

United Kingdom / Royaume-Uni

8- **Radical cleric Anjem Choudary,** whom the *Guardian* reports is believed to have **inspired at least 100 people from Britain into terrorism**, including organizations committed to **campaigns** of **murder against** the **West**, f aces up to a **decade in prison** after he was **found guilty** of **inviting support for Islamic State** in a **series** of **lectures released** on **YouTube. Security sources**, adds *The Times of London,* said that **Choudary's conviction** marked a **seismic moment** in the **fight against terrorism**. Choudary was found guilty last Thursday of terrorism offences after a five-week trial but all reporting was banned until the conclusion Tuesday of a linked trial of other alleged radical preachers. He will remain in Belmarsh high-security prison in southeast London until his sentencing next month.

Europe

9- Selon *La Tribune de Genève,* arrêté à l'aéroport de Zurich, placé en détention, un jeune de 29 ans est accusé d'être en lien avec une organisation terroriste. Un **Genevois parti il y a neuf mois sur le chemin du djihad a été arrêté à son retour en Suisse**, a appris la Tribune de Genève. **H. est accusé par la justice d'être en lien avec une organisation terroriste.**
10- Le 25 septembre, les **Suisses votent sur la nouvelle loi sur le Renseignement, combattue par un référendum de la gauche. L'ancien chef du Service de renseignement suisse, Peter Regli,** la juge nécessaire dans le contexte actuel La loi sur le renseignement (LRens) **élargit les moyens d'action du Service de renseignement de la Confédération (SRC)** rapporte *Le Temps,*(Suisse).
11- **Germany's public broadcaster *ARD*** has viewed a leaked **German government document** which charges **Turkey** has been **deliberately financing Islamist** and **terror organizations** with the **direct consent** of **President Recep Tayyip Erdogan.**

Africa / Afrique

12- Selon *Jeune Afrique,* les **autorités marocaines ont annoncé arrêté quatre sympathisants présumés du groupe jihadiste État islamique (EI),** accusés de planifier des **attentats contre des "sites vitaux" à Casablanca**. « Le Bureau central d'investigations judiciaires (BCIJ) a démantelé une cellule terroriste composée de quatre extrémistes s'activant entre Casablanca et la commune de Mograne », une localité rurale à une cinquantaine de kilomètres de Rabat.

Middle East / Moyen-Orient

13- The *Jerusalem Post* reports that the **Shin Bet (Israel Security Agency)** on Tuesday announced that it had taken down a number of **terrorist cells** in the West Bank whose members had been recruited through Facebook by elite Hezbollah Unit 133 in Lebanon and the Gaza Strip.

14- *The National (UAE)* reports that **Russia** on Tuesday started using **an Iranian airbase to launch strikes on targets in Syria**, further entrenching itself in the Middle East and its conflicts.

Afghanistan/Pakistan

15- `The *Express Tribune* reports that in an attempt to promote restraint and responsibility in South Asia, **Pakistan** has offered its nuclear-armed arch rival for a bilateral arrangement on **non-testing of nuclear weapons**, the Foreign Office said on Tuesday.

Australia, New Zealand / Australie, Nouvelle-Zélande

16- The **Chinese embassy has warned that the rejection this year of two bids by Chinese companies to invest in Australia** showed "clear protectionist tendencies" which would have a "serious impact on the enthusiasm" of firms wanting to invest in Australia. "The Chinese government is highly concerned about the statement by the **Australian Treasurer** on his preliminary decision to block the sale of the 50.4 per cent of Ausgrid in a 99-year lease to foreign bidders on **national security grounds**," the embassy said yesterday in reply to questions from *The Australian*.

Asia / Asie

17- The *Bangladesh Daily Star* reports that banned in 2005 and subsequently broken down, the **Jama'atul Mujahideen Bangladesh (JMB)** took only nine years to reorganise. **Bangladeshi-Canadian named Tamim Ahmed Chowdhury**, who, according to IS propaganda magazine Dabiq, identifies himself as Shaykh Abu Ibrahim Al-Hanif, is leading the group as its operational commander.

18- In **breaking news,** the *Yonhap News Agency* reports that a **high-ranking North Korean diplomat stationed in Britain defected to South Korea**, Seoul's unification ministry said Wednesday, in the latest in a series of high-profile defections by the North's elite.**Thae Yong-ho**, a minister at the North's embassy in London, has arrived in South Korea with his family, the Ministry of Unification said, without unveiling further details.

19- **China's pending cyber security law** will not create obstacles for foreign business, **China's Foreign Ministry** said, responding to concerns by international business lobbies over the planned rules, *Reuters* reports. "As for the legal requirement for internet operators to provide relevant data in the course of **enforcement agencies' counter-terrorism** and criminal investigations, this is necessary for safeguarding national security and investigating crimes. All countries do this," the ministry said.

20- *Kyodo News* reports that **Japan lodged a protest Wednesday after China Coast Guard vessels** entered Japanese territorial waters around the **Senkaku Islands** in the **East China Sea**. Chinese government ships and fishing boats have repeatedly sailed near the uninhabited islands, which China claims and calls Diaoyu, drawing protest from Tokyo.

Americas / Amériques

21- Pointing to the **Rio Olympics** as an **example**, ***The Intercept's* Lucas Figueiredo** lays out a case that **for years Brazilian intelligence** has **stoked terrorism fears for its own benefit**. Figueiredo writes that "for years, the secret service has fought to raise its budget and prestige in the state's hierarchy. Recently, it requested the right for its agents to wiretap and carry firearms. **ABIN** continues to hope for increased power and resources and refuses to abandon its dark legacy from the dictatorship era. Its current general director, **Wilson Roberto Trezza**, is a veteran from the SNI era. After the Olympics, he might be substituted out for Janér Tesch Hosken Alvarenga, yet another agent trained in the National Information Service".

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Tuesday, September 6 2016
le mardi 6 septembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- In an op-ed appearing in *The Hill Times*, Phil Gurski writes: If there is one spy agency in Canada that is poorly understood and about which much of little veracity has been published it has to be **CSE, or the Communications Security Establishment**. CSE has a number of roles, but the one that gets the most public attention is signals intelligence, or **SIGINT**. This method of intelligence collection entails capturing telecommunications in a variety of forms by a variety of techniques, few of which are known. This is indeed a good thing: the spy agency that openly shares how it gathers intelligence will not be in the spy business very long. This may sound sacrilege to some, but some things need to remain secret. CSE is not a law-enforcement agency and does not go to court to acquire warrants to collect information, unlike **CSIS** and the **RCMP**. It is limited to the collection of intelligence outside Canada and it cannot include Canadians (or Americans, British, Australians, and New Zealanders for that matter—Canada's so-called "**five eyes" partners**) in its dragnet.

Canada

2- *La Presse+* révèle que le **controversé imam Hamza Chaoui, au cœur l'an dernier d'un projet avorté de « centre communautaire islamique » destiné aux jeunes Montréalais, offre maintenant ses enseignements religieux dans des lieux publics. L'homme organise occasionnellement des sorties, destinées aux jeunes hommes, qui mélangent « soccer, rappels religieux, barbecue », selon sa page Facebook. Elles s'ajoutent à ses cours hebdomadaires à la mosquée Sounna, dans Parc-Extension.** La dernière sortie a eu lieu à la fin du mois d'août au parc Jarry. Il en a publié des images sur les réseaux sociaux. On l'y voit s'adressant à un groupe d'une douzaine de jeunes, dont au moins deux enfants.

International

United States / États-Unis

3- At the behest of **Director of National Intelligence James Clapper**, **U.S. intelligence** and law enforcement agencies are probing what they see as a **broad covert Russian operation** in the **United States** to **sow public distrust** in the upcoming **presidential election** and in **U.S. political institutions** reports the *Washington Post*. A **senior intelligence official** cautioned that the **intelligence community is not saying it has "definitive proof" of such tampering,** or any Russian plans to do so. "But even the hint of something impacting the security of our election system would be of significant concern," the official said. "It's the key to our democracy, that people have confidence in the election system."

United Kingdom / Royaume-Uni

4- As **Isis loses territory** in its self-proclaimed caliphate, **security services** in the UK and **Europe** are bracing for the return of **'thousands'** of **jihadists** though the *Independent* reports **few foreign fighters** have **left Islamic State ranks** thus far with **under 10 coming home** to the UK in the past **eight months.**

5- With the **Snowden documents** as a guide, *The Intercept* pulls the veil back on **Menwith Hill,**

an **NSA surveillance base** in the **British countryside** near the small North Yorkshire town of Harrogate. Once used to monitor Soviet communications during the Cold War, the base is now utilized to aid **"a significant number of capture-kill operations"** across the **Middle East** and **North Africa**, fueled by **powerful eavesdropping technology** that can harvest data from more than **300 million emails** and **phone calls a day.**
6- Following a summer recess, a **House of Lords committee** has **resumed deliberation** of the government's **Investigatory Powers Bill,** particularly the **bulk powers** outlined in the legislation reports *The Register.* In correspondence with *The Register,* **former GCHQ director Sir David Omond** wrote "the recent **serious rise in global cybercrime** by organised criminal groups...has only reinforced the importance of having the **specialist techniques** and **international liaisons** of the **secret agencies** available to support the investigations of law enforcement".

Europe

7- Based on thousands of pages of **documents** and **photos** from **internal European investigations** and information from **sources** close to the investigation, *CNN* reports the **sophisticated Isis network** that plots **foreign strikes** had planned for the **carnage** in the **November Paris attacks** to be **far worse**, to **occur in other European countries** as well and, investigators believe, had planned to **follow them up** with **strikes in several locations.** Additionally, the documents point to the existence of **another suspected terrorist** -- never before named publicly -- who authorities claim is **linked** to the **Paris terror cell** and was on the loose in Europe for months after that attack. That man, identified by authorities as **Abid Tabaouni,** was only **arrested in July.**
8- Selon *Le Temps,* (Suisse), **cinq ministres latins sont venus défendre la loi soumise au peuple le 25 septembre. La sécurité collective le commande et elle n'est pas dangereuse pour les libertés individuelles, ont-ils plaidé.** Tous derrière la **loi sur le renseignement (LRens)** soumise au vote le 25 septembre. En tant que conseillers d'Etat, nous avons les mains dans le cambouis, explique **Béatrice Métraux**, Verte. **On sait ce que signifie terrorisme et djihadisme et on a le souci de défendre la population avant la politique de son parti.** » Or, assurer la sécurité ne saurait se faire sans autoriser les services de renseignement à agir dans la sphère privée: « On ne lutte pas contre les dangers d'aujourd'hui avec une loi du passé », estime Nathalie Barthoulot, ministre jurassienne socialiste. Pour parer au terrorisme et à l'espionnage notamment, il faut donc permettre les écoutes téléphoniques, les fouilles de domicile ou le hacking de systèmes informatiques. Au vu de l'évolution technologique, le **Service de renseignement de la Confédération (SRC) n'est plus en mesure de remplir sa mission,** selon les magistrats. D'autant plus que la Suisse est dépendante du bon vouloir des services étrangers.
9- D'après *Le Figaro,* un **surveillant a été attaqué à l'arme blanche dimanche par un détenu radicalisé, aidé par plusieurs complices.** Pas un acte isolé, mais concerté entre plusieurs détenus... À la **prison d'Osny, en France, dans un quartier dédié supposé accueillir les candidats à la déradicalisation**, l'agression dimanche de **deux surveillants, dont l'un gravement atteint, fait froid dans le dos. Le détenu auteur des faits, Bilal T.,** a frappé sa victime à l'aide d' « une lame de 25 cm très fine et très aiguisée qui a transpercé de part en part la gorge du surveillant. Selon des personnels pénitentiaires, **l'auteur de l'agression « aurait badigeonné l'une des portes de cellules du sang du surveillant et aurait levé les mains afin de prier » .**

Africa / Afrique

10- La France espionne l'Algérie. Les Etats-Unis espionnent la France. Tout le monde s'espionne. C'est une réalité connue de tous. La nouveauté ce sont **ces révélations confiées par Bernard Barbier, un ancien cadre des services d'espionnage français, Bernard Barbier, rapportés lors du Symposium central supélec.** Cet ancien espion confirme les révélations faites déjà par Le Monde en mars 2014. Le quotidien vespéral français avait révélé que les **services secrets**

français espionnait l'Algérie, le Canada, la Côte d'Ivoire, l'Iran grâce à un logiciel rapporte *Le Matin,* (Algérie).
11- **More than a dozen groups** have appeared since **attacks** on **Nigeria's oil pipelines resumed** earlier this year, each claiming their own constituencies and making their own demands reports the *Voice of America.* Some analysts believe the **government's decision to talk** with the **militant groups** is merely **encouraging them.**

Middle East / Moyen-Orient

12- The *Gulf News* reports that dual citizen **Canadians must show a Canadian passport** to enter the UAE under tightened entry rules effective September 30.
13- The *Jerusalem Post* reports that citing **Iran and its proxy terrorist organizations, Hamas and Hezbollah**, as the greatest existential threats to Israel, former **Shin Bet (Israel Security Agency)** head and current chairman of the Foreign Affairs and Defense Committee, Avi Dichter, said the Middle East is undergoing "tectonic movements."
14- The *Fars News Agency* reports that Commander of the Special Unit of Iran's Law Enforcement Police Brigadier General Hassan Karami announced that his forces have **killed three ISIL terrorists in the Western province of Kermanshah** who were equipped with suicide vests.

Afghanistan/Pakistan

15- The *Pakistan Dawn* reports that there has been a marked reduction in **terrorist attacks and deaths in Pakistan in 2015**, but terrorists seem to have become more lethal as the ratio of deaths per attack has increased.
16- *Pajhwok Afghan News* reports that the death toll from **twin suicide bombings has risen to 24 with another 91 people injured** in the latest attack on central capital Kabul on Monday, officials said.

Australia, New Zealand / Australie, Nouvelle-Zélande

17- A dangerous number of **Chinese nationals in Australia** owe their **primary allegiance** to **Beijing** rather than to Australia, **one of the country's leading strategic experts has warned**. Professor **Paul Dibb** says the **Chinese community** in Australia has adopted an increasingly - **strident pro-Chinese government view in recent years, largely influenced by the Chinese embassy in Canberra.** It is a trend, he says, that **risks fuelling a fresh backlash against foreign investment in Australia.** "The fact is that there are a considerable number of Chinese residents and students here that feel nostalgic about the **People's Republic and its ruling party,**" - Professor Dibb writes in *The Australian* today.

Asia / Asie

18- The *BDNews24* reports that **Mohammad Jahidul Islam**, the suspected militant killed during a raid on a house at Mirpur's Rupnagar is a former army officer, who left the job two years ago after returning from **Canada.**
19- Members of the G20 have agreed to **advance the anti-corruption campaign** and **refuse to offer "safe havens"** for corrupt officials who remain at large in foreign countries, reports the *China Daily.* Speaking to journalists at the end of the two-day G20 Leaders Summit in the lakeside city of Hangzhou, Zhejiang province, President **Xi Jinping** said important breakthroughs have been made this year in the fight against **graft with fugitive repatriations and recovery of assets**. G20 members have decided to **set up an anti-corruption research center in Beijing to provide intelligence support for capturing fugitives and recovering their illegal assets**. The summit also passed the **G20 2017-18 Anti-Corruption Action Plan**, Xi said. "These anti-graft achievements will leave corrupt officials no place to hide in G20 members' territories and in the world at large," Xi said. In recent years, many G20 economies, including the **United States** and

Canada, have become popular destinations for fugitive corrupt officials due to the lack of signed bilateral extradition treaties and legal differences, according to **China's Ministry of Public Security**. Many corrupt officials have transferred billions of yuan in ill-gotten assets to foreign accounts either through **money-laundering and underground banks**, according to the ministry.
20- The *Times of India* reports that probing Indian recruit of **Islamic State Mohammad Masiuddin alias Abu Musa's link with Jamaat-ul-Mujahideen Bangladesh (JMB) leaders** involved in the Dhaka attack, the National Investigation Agency has approached US, Germany, New Zealand and neighbouring Bangladesh seeking information about his online conversations.
21- According to *Yonhap News Agency*, President **Park Geun-hye** on Tuesday held a summit with her U.S. counterpart **Barack Obama** in Vientiane to discuss an array of issues, including North Korea's relentless saber-rattling, her office Cheong Wa Dae said. Their talks came amid **Pyongyang's continued provocations, including its launch of three mid-range ballistic missiles Monday**. The missiles traveled some 1,000 kilometers and fell into waters within Japan's air defense identification zone, Seoul's military officials said. Observers say the two leaders will use their summit to send a unified message against the communist state's provocations, and its evolving nuclear and missile programs.

Americas / Amériques

Light coverage / couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Wednesday, September 7 2016
le mercredi 7 septembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

No mentions in the mainstream media. / Pas de mentions dans les médias traditionnels.

Canada

1- The *National Post* reveals that while **hiding out** in **Hong Kong** in **2013, Edward Snowden** retained the services **Canadian-born** and **trained lawyer Robert Tibbo** who hatched a plan that included a visit to the **UN sub-office** where **Snowden applied for refugee status** to **avoid extradition to the U.S.** "I had minutes to figure out how to get him to the UN, away from the media, and out of harm's way with the weight of the U.S. government bearing down on him. I did what I had to do, and could do, to help him," Tibbo told the *Post*. "They wanted the data and they wanted to shut him down. Our greatest fear was that Ed would be found."

2- *La Presse+* rapporte que l'un des **prêcheurs radicaux les plus influents d'Occident, suivi sur les réseaux sociaux par les terroristes canadiens Martin Couture-Rouleau et Michael Zehaf Bibeau, vient d'être condamné à plus de cinq ans de prison au Royaume-Uni** pour avoir soutenu le **groupe armé État islamique (EI). En 2013, il avait prédit un attentat au Canada.** Les Anglais le surnomment « l'homme le plus détesté » de leur pays, le « prêcheur de haine ». Anjem Choudary, avocat de 49 ans d'origine pakistanaise, prédicateur emblématique dans les milieux islamistes britanniques, marchait sur une fine ligne depuis plusieurs années. Il s'était fait « le porte-parole des extrémistes, faisant des commentaires des plus déplaisants, mais sans jamais franchir le seuil de la criminalité », comme l'a expliqué au Guardian le **commandant Dean Haydon, chef de l'escouade antiterroriste de Scotland Yard.**

3- **Brig.-Gen. Shane Brennan, commander** of **Canada's Joint Task Force-Iraq,** said the number of **Canadian intelligence officers** assigned to the **anti-Isis** effort based in **Kuwait** has **grown to 50.** Their mission, reports the *Canadian Press,* is to analyze the pictures taken by Aurora surveillance aircraft so the coalition can plan air strikes and ground operations.

International

United States / États-Unis

4- The *Associated Press* reports a **congressional committee examination** of the **Office of Personnel Management breach** found that while officials were **closely monitoring** the **online activities** of **one suspected hacker for months** and had devised a plan to **expel him** when he got **too close** to **critical information**, they were **unaware** of the presence of a **second hacker** who had **infiltrated** the **system posing** as an **employee** of a **federal contractor.**

5- While **al Qaeda** has **long provided salaries** and the latest military equipment, **Islamic State**, reports the *Christian Science Monitor,* with wealth generated from oil revenues and taxation in the territories it holds, is **promising foreign fighters higher salaries, housing**, and **additional benefits of $250 per month** for a family of five.

United Kingdom / Royaume-Uni

6- Radical cleric **Anjem Choudary** could be **released** in **two years** after he was was **sentenced** to **5½ years in prison** for **pledging allegiance** to **Islamic State** and encouraging others to join

the terror group. **Mr. Justice Holroyde,** sentencing, said Choudary was a **calculating extremist** who had shown "contempt for the values of the democracy in which we live". (Extensive coverage / vaste couverture).
7- Police in **Northern Ireland** have uncovered a **"significant amount of terrorist material",** specifically **explosives** and **bomb-making components,** at **12 separate locations** in the town of **Larne.** (Moderate coverage / couverture modérée).

Europe

8- *Le Figaro* rapporte qu'en s'appuyant sur une **analyse du contre-espionnage, dont « Le Figaro » a eu connaissance, Manuel Valls assure qu'il faut « se préparer à résister » à « une menace supplémentaire pour notre sécurité nationale »** . Sécurité Manuel Valls a donné le ton ce mardi en matière de sécurité : « Près de 700 djihadistes français ou résidant en France se trouvent actuellement dans les zones de combat en Irak et en Syrie . Leur retour représente une menace supplémentaire pour notre sécurité nationale (...) il faut nous préparer à résister, le combat sera long. ». **La Direction générale de la sécurité intérieure (DGSI) a expliqué que la France doit demeurer très vigilante.**
9- **Prévention de la radicalisation : des "unités dédiées au sein des détentions classiques. C'est extrêmement dangereux" Emmanuel Gauthrin, secrétaire général de FO Pénitentiaire,** a réclamé sur *FranceTv Info* la suppression "des unités dédiées au sein même des détentions classiques" après **l'agression dimanche de deux surveillants pénitentiaires par un détenu à la maison d'arrêt d'Osny (Val-d'Oise), une unité spéciale de prévention de la radicalisation**. Un acte que le syndicaliste qualifie de "prémédité" et de "terroriste". "Ces unités dédiées au sein même des détentions classiques. C'est extrêmement dangereux. On continue malheureusement à polluer le reste de la population pénale".
10- Speaking to the *New York Times* Editorial Board, **Turkey's Deputy Prime Minister Numan Kurtulmus** conceded **"we don't see any evidence** that **U.S. officials supported** the **coup d'état"**.
11- **Each day** there are more than **20 highly specialized attacks** on the **German government's computer networks** reports *The Local.*

Africa / Afrique

12- *Foreign Policy* reports that on July 7, **South Sudanese troops fired between 50-100 rounds** of **ammunition** at **two armored SUVs carrying American diplomats** en route to the **U.S. Embassy** in **Juba.** The **State Department** in Washington **downplayed** the **incident** telling *Foreign Policy* that "we **do not believe our vehicles** and **personnel** were **specifically targeted.** I think we can speak with certainty the people in the convoy did not identify themselves necessarily to the soldiers or say that it was an American convoy."
13- Selon *Pan African News Agency,* le **Premier ministre tunisien, Youssef Chahed estime que "la lutte contre la corruption et le terrorisme" sont les faces d'un même phénomène ciblant le citoyen**, axe central de tout développement", affirmant que la **guerre contre la corruption en demandant des comptes aux coupables est "plus complexe, parfois plus difficile que la lutte contre le terrorisme".**
14- **Tunisia's defence minister Farhat Hachani** implored countries in **North Africa** to **strengthen co-operation** in order to **prevent Islamic State fighters** who are fleeing their **Libyan stronghold** of **Sirte** from **returning** to their **homelands** reports *Reuters.*

Middle East / Moyen-Orient

15- *Asharq Al-Awsat* reports that a **suspected chlorine gas attack** on an opposition-held neighborhood in the **Syrian city of Aleppo** had reportedly caused dozens of cases of suffocation on Tuesday, rescue workers and a monitoring group said.

16- *Press TV* reports that **Iranian Intelligence Minister Mahmoud Alavi** has made an unannounced trip to **Germany**, with observers describing the unprecedented trip — about which little detail has been made public — as highly significant.

Afghanistan/Pakistan

17- *TOLO News* reports that **Rahmatullah Nabil, the ex-chief of the Afghan spy agency—the National Directorate of Security (NDS)** - Tuesday alleged that President Ashraf Ghani's unnecessary meddling in the works of government institutions has fueled political, security and social uncertainties in the country.

Australia, New Zealand / Australie, Nouvelle-Zélande

18- Islamic State has issued a fresh call to its followers to **kill unbelievers in Sydney and Melbourne**, bolstering the theory that as the terror group faces extinction in Syria it is lashing out abroad, repots *The Australian*. The call to arms appeared in the first edition of **Rumiyah**, a new English-language online magazine produced by Islamic State, which in recent months has suffered a string of setbacks prompting some to speculate it has entered a state of terminal - decline. The instruction, which is particularly graphic, even by the standards of Islamic State, was contained in a long feature article about Australian terrorist **Ezzit Raad**, whom the terrorist group claims was killed recently in Syria. In the article Islamic State **calls on its followers to "light the ground'' beneath unbelievers, and scorch them with terror. ''Kill them on the streets of Brunswick, Broadmeadows, Bankstown and Bondi**,'' the article reads (moderate coverage / couverture modérée).

19- The government has spelled out priorities for improving defence capabilities through clever ideas, with **boosting intelligence, surveillance, electronic warfare and cyber** heading the list. Defence Industry Minister **Christopher Pyne** says the new **$640 million Defence Innovation Hub** to be launched later this year will drive growth in defence industry innovation. The government has set six areas for research and innovation, with three given top priority for 2016-17. **"In the intelligence, surveillance, reconnaissance, electronic warfare, space and cyber capability stream we will focus on improving intelligence collection, analysis and dissemination**," he said in the keynote address to the Land Forces conference dinner in Adelaide. Mr Pyne said that would **include biometric data and cyber innovation** to support intelligence capability development, writes *Australian Associated Press*.

Asia / Asie

20- According to *The Korea Herald*, high-ranking defense officials from 33 countries and five international organizations gathered Wednesday to **discuss regional and international security** issues, namely the ongoing challenges involving **North Korea and maritime disputes involving the US, China and Japan**. The Seoul Defense Dialogue 2016, held from Sept.7-9, will kick off with a plenary session Thursday on the denuclearization of North Korea and international cooperation. Seoul Defense Dialogue 2015 (SDD)During the session, the participants will assess the North Korean threat, UN Security Council resolution 2270 and other international cooperation efforts, as well as analyze how the Iranian nuclear deal could be applied to Pyongyang.

21- Japan's nuclear watchdog decided today to make operators of nuclear power plants and other nuclear facilities **check the background of their workers to prevent terror attacks**, the *Kyodo News* reports. Following the recommendation of the **International Atomic Energy Agency**, the **Nuclear Regulation Authority** will introduce the new regulation in late September, although the actual implementation is expected to be from next year or later due to necessary procedures, such a revision of the rules regarding the handling of nuclear materials.

22- The *New Strait Times* reports that **Intelligence gleaned by counterterrorism operatives** in the country suggest that **Malaysia** now has, in its midst, suicide bombers ready to die for the Islamic State (IS) group.

23- The *Bangladesh Daily Star* reports that **Islamic State of Bangladesh (ISB),** founded in Singapore in March, planned to wage "jihad" in Bangladesh from the northern district of Panchagarh, according to a court document.
24- Increasingly assertive action by China's coast guard ships in the **South China Sea** risks destabilising the region, according to the authors of new research tracking maritime law enforcement incidents across the vital trade route. While the risks of full-blown naval conflict dominates strategic fears over the disputed waterway, the danger of incidents involving coast guards should not be underestimated, said Bonnie Glaser, a regional security expert at Washington's **Center for Strategic and International Studies** think-tank. CSIS researchers have detailed some **45 clashes and standoffs in the South China Sea since 2010** in a survey due to be published week on its ChinaPower website and seen by *Reuters*.

Americas / Amériques

Light coverage / couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Wednesday, September 7 2016
le mercredi 7 septembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

No mentions in the mainstream media. / Pas de mentions dans les médias traditionnels.

Canada

1- The *National Post* reveals that while **hiding out** in **Hong Kong** in **2013, Edward Snowden** retained the services **Canadian-born** and **trained lawyer Robert Tibbo** who hatched a plan that included a visit to the **UN sub-office** where **Snowden applied for refugee status** to **avoid extradition to the U.S.** "I had minutes to figure out how to get him to the UN, away from the media, and out of harm's way with the weight of the U.S. government bearing down on him. I did what I had to do, and could do, to help him," Tibbo told the *Post*. "They wanted the data and they wanted to shut him down. Our greatest fear was that Ed would be found."

2- *La Presse+* rapporte que l'un des **prêcheurs radicaux les plus influents d'Occident, suivi sur les réseaux sociaux par les terroristes canadiens Martin Couture-Rouleau et Michael Zehaf Bibeau, vient d'être condamné à plus de cinq ans de prison au Royaume-Uni** pour avoir soutenu le **groupe armé État islamique (EI). En 2013, il avait prédit un attentat au Canada.** Les Anglais le surnomment « l'homme le plus détesté » de leur pays, le « prêcheur de haine ». Anjem Choudary, avocat de 49 ans d'origine pakistanaise, prédicateur emblématique dans les milieux islamistes britanniques, marchait sur une fine ligne depuis plusieurs années. Il s'était fait « le porte-parole des extrémistes, faisant des commentaires des plus déplaisants, mais sans jamais franchir le seuil de la criminalité », comme l'a expliqué au Guardian le **commandant Dean Haydon, chef de l'escouade antiterroriste de Scotland Yard.**

3- **Brig.-Gen. Shane Brennan, commander** of **Canada's Joint Task Force-Iraq,** said the number of **Canadian intelligence officers** assigned to the **anti-Isis** effort based in **Kuwait** has **grown to 50**. Their mission, reports the *Canadian Press,* is to analyze the pictures taken by Aurora surveillance aircraft so the coalition can plan air strikes and ground operations.

International

United States / États-Unis

4- The *Associated Press* reports a **congressional committee examination** of the **Office of Personnel Management breach** found that while officials were **closely monitoring** the **online activities** of **one suspected hacker for months** and had devised a plan to **expel him** when he got **too close** to **critical information**, they were **unaware** of the presence of a **second hacker** who had **infiltrated** the **system posing** as an **employee** of a **federal contractor.**

5- While **al Qaeda** has **long provided salaries** and the latest military equipment, **Islamic State**, reports the *Christian Science Monitor,* with wealth generated from oil revenues and taxation in the territories it holds, is **promising foreign fighters higher salaries, housing**, and **additional benefits of $250 per month** for a family of five.

United Kingdom / Royaume-Uni

6- Radical cleric **Anjem Choudary** could be **released** in **two years** after he was was **sentenced** to **5½ years in prison** for **pledging allegiance** to **Islamic State** and encouraging others to join

the terror group. **Mr. Justice Holroyde,** sentencing, said Choudary was a **calculating extremist** who had shown "contempt for the values of the democracy in which we live". (Extensive coverage / vaste couverture).
7- Police in **Northern Ireland** have uncovered a **"significant amount of terrorist material",** specifically **explosives** and **bomb-making components,** at **12 separate locations** in the town of **Larne.** (Moderate coverage / couverture modérée).

Europe

8- *Le Figaro* rapporte qu'en s'appuyant sur une **analyse du contre-espionnage, dont « Le Figaro » a eu connaissance, Manuel Valls assure qu'il faut « se préparer à résister » à « une menace supplémentaire pour notre sécurité nationale »** . Sécurité Manuel Valls a donné le ton ce mardi en matière de sécurité : « Près de 700 djihadistes français ou résidant en France se trouvent actuellement dans les zones de combat en Irak et en Syrie . Leur retour représente une menace supplémentaire pour notre sécurité nationale (...) il faut nous préparer à résister, le combat sera long. ». **La Direction générale de la sécurité intérieure (DGSI) a expliqué que la France doit demeurer très vigilante.**
9- **Prévention de la radicalisation : des "unités dédiées au sein des détentions classiques. C'est extrêmement dangereux" Emmanuel Gauthrin, secrétaire général de FO Pénitentiaire,** a réclamé sur *FranceTv Info* la suppression "des unités dédiées au sein même des détentions classiques" après **l'agression dimanche de deux surveillants pénitentiaires par un détenu à la maison d'arrêt d'Osny (Val-d'Oise), une unité spéciale de prévention de la radicalisation**. Un acte que le syndicaliste qualifie de "prémédité" et de "terroriste". "Ces unités dédiées au sein même des détentions classiques. C'est extrêmement dangereux. On continue malheureusement à polluer le reste de la population pénale".
10- Speaking to the *New York Times* Editorial Board, **Turkey's Deputy Prime Minister Numan Kurtulmus** conceded **"we don't see any evidence** that **U.S. officials supported** the **coup d'état".**
11- **Each day** there are more than **20 highly specialized attacks** on the **German government's computer networks** reports *The Local.*

Africa / Afrique

12- *Foreign Policy* reports that on July 7, **South Sudanese troops fired between 50-100 rounds** of **ammunition** at **two armored SUVs carrying American diplomats** en route to the **U.S. Embassy** in **Juba.** The **State Department** in Washington **downplayed** the **incident** telling *Foreign Policy* that "we **do not believe our vehicles** and **personnel** were **specifically targeted.** I think we can speak with certainty the people in the convoy did not identify themselves necessarily to the soldiers or say that it was an American convoy."
13- Selon *Pan African News Agency,* le **Premier ministre tunisien, Youssef Chahed estime que "la lutte contre la corruption et le terrorisme" sont les faces d'un même phénomène ciblant le citoyen**, axe central de tout développement", affirmant que la **guerre contre la corruption en demandant des comptes aux coupables est "plus complexe, parfois plus difficile que la lutte contre le terrorisme".**
14- **Tunisia's defence minister Farhat Hachani** implored countries in **North Africa** to **strengthen co-operation** in order to **prevent Islamic State fighters** who are fleeing their **Libyan stronghold** of **Sirte** from **returning** to their **homelands** reports *Reuters.*

Middle East / Moyen-Orient

15- *Asharq Al-Awsat* reports that a **suspected chlorine gas attack** on an opposition-held neighborhood in the **Syrian city of Aleppo** had reportedly caused dozens of cases of suffocation on Tuesday, rescue workers and a monitoring group said.

16- *Press TV* reports that **Iranian Intelligence Minister Mahmoud Alavi** has made an unannounced trip to **Germany**, with observers describing the unprecedented trip — about which little detail has been made public — as highly significant.

Afghanistan/Pakistan

17- *TOLO News* reports that **Rahmatullah Nabil, the ex-chief of the Afghan spy agency—the National Directorate of Security (NDS)** - Tuesday alleged that President Ashraf Ghani's unnecessary meddling in the works of government institutions has fueled political, security and social uncertainties in the country.

Australia, New Zealand / Australie, Nouvelle-Zélande

18- Islamic State has issued a fresh call to its followers to **kill unbelievers in Sydney and Melbourne**, bolstering the theory that as the terror group faces extinction in Syria it is lashing out abroad, repots *The Australian*. The call to arms appeared in the first edition of **Rumiyah**, a new English-language online magazine produced by Islamic State, which in recent months has suffered a string of setbacks prompting some to speculate it has entered a state of terminal - decline. The instruction, which is particularly graphic, even by the standards of Islamic State, was contained in a long feature article about Australian terrorist **Ezzit Raad**, whom the terrorist group claims was killed recently in Syria. In the article Islamic State **calls on its followers to "light the ground'' beneath unbelievers, and scorch them with terror. ''Kill them on the streets of Brunswick, Broadmeadows, Bankstown and Bondi**,'' the article reads (moderate coverage / couverture modérée).

19- The government has spelled out priorities for improving defence capabilities through clever ideas, with **boosting intelligence, surveillance, electronic warfare and cyber** heading the list. Defence Industry Minister **Christopher Pyne** says the new **$640 million Defence Innovation Hub** to be launched later this year will drive growth in defence industry innovation. The government has set six areas for research and innovation, with three given top priority for 2016-17. **"In the intelligence, surveillance, reconnaissance, electronic warfare, space and cyber capability stream we will focus on improving intelligence collection, analysis and dissemination**," he said in the keynote address to the Land Forces conference dinner in Adelaide. Mr Pyne said that would **include biometric data and cyber innovation** to support intelligence capability development, writes *Australian Associated Press*.

Asia / Asie

20- According to *The Korea Herald*, high-ranking defense officials from 33 countries and five international organizations gathered Wednesday to **discuss regional and international security** issues, namely the ongoing challenges involving **North Korea and maritime disputes involving the US, China and Japan**. The Seoul Defense Dialogue 2016, held from Sept.7-9, will kick off with a plenary session Thursday on the denuclearization of North Korea and international cooperation. Seoul Defense Dialogue 2015 (SDD)During the session, the participants will assess the North Korean threat, UN Security Council resolution 2270 and other international cooperation efforts, as well as analyze how the Iranian nuclear deal could be applied to Pyongyang.

21- Japan's nuclear watchdog decided today to make operators of nuclear power plants and other nuclear facilities **check the background of their workers to prevent terror attacks**, the *Kyodo News* reports. Following the recommendation of the **International Atomic Energy Agency**, the **Nuclear Regulation Authority** will introduce the new regulation in late September, although the actual implementation is expected to be from next year or later due to necessary procedures, such a revision of the rules regarding the handling of nuclear materials.

22- The *New Strait Times* reports that **Intelligence gleaned by counterterrorism operatives** in the country suggest that **Malaysia** now has, in its midst, suicide bombers ready to die for the Islamic State (IS) group.

23- The *Bangladesh Daily Star* reports that **Islamic State of Bangladesh (ISB),** founded in Singapore in March, planned to wage "jihad" in Bangladesh from the northern district of Panchagarh, according to a court document.
24- Increasingly assertive action by China's coast guard ships in the **South China Sea** risks destabilising the region, according to the authors of new research tracking maritime law enforcement incidents across the vital trade route. While the risks of full-blown naval conflict dominates strategic fears over the disputed waterway, the danger of incidents involving coast guards should not be underestimated, said Bonnie Glaser, a regional security expert at Washington's **Center for Strategic and International Studies** think-tank. CSIS researchers have detailed some **45 clashes and standoffs in the South China Sea since 2010** in a survey due to be published week on its ChinaPower website and seen by *Reuters*.

Americas / Amériques

Light coverage / couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Tuesday, September 13 2016
le mardi 13 septembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- Selon *Radio-Canada Nouvelles,* « La menace qui pèse sur vous en tant que fonctionnaire canadien en voyage officiel est bien réelle. » **Le Service canadien du renseignement de sécurité (SCRS) vient tout juste de mettre à jour ses directives sur les voyages à l'intention des fonctionnaires fédéraux.** Obtenu par Radio-Canada Ottawa-Gatineau, ce document interne d'une quarantaine de pages insiste sur **l'importance pour les employés du gouvernement d'être extrêmement prudents à l'étranger. Le SCRS soutient que « la menace terroriste qui pèse sur les Canadiens a changé » depuis les attaques survenues à Saint-Jean-sur-Richelieu et au Parlement canadien en octobre 2014.** (Similar reports appeared on *CBC News Ottawa radio and television*).

2- People who have been **deemed a terrorist threat should be incarcerated if they can't be monitored around the clock,** Conservative leadership candidate **Tony Clement** said Monday in **outlining his national security platform**. "If the safety of the public cannot be guaranteed through a peace bond, it has to be guaranteed through incarceration," he told reporters on Parliament Hill. Clement also wants **terrorist suspects to be on a published "wanted" list,** reports *CBC News*. Clement said both measures would be subject to judicial review and require an "**evidentiary threshold**" be met. "I'm not proposing some kind of wanted list that is the figment of somebody's imagination or without some kind of evidence," Clement said. "Clearly, that would not be acceptable in Canadian society." Clement repeated his **proposal for the "enhanced screening" of people coming in and out of Canada** as part of his national security platform. **He said the current process is not rigorous enough**. "**Only nine to 15 per cent of the current intake of immigrants in any given year go through the rigorous screening of CSIS and other security agencies**," he said. "That's just far too low."

Canada

3- Within days of a foiled terror plot that ended in the death of **Aaron Driver**, a known Islamic State supporter in southern Ontario, Canada's federal police arrested **another young man over fears he would participate in terrorism,** *VICE News* has learned. Ottawa man **Tevis Gonyou-McLean**, 24, was **arrested on August 12 and charged with uttering a threat to cause death or harm to another person**. The RCMP are also pursuing a terror-related **peace bond against him over fears that he might engage in terrorism at home and abroad**. At the end of August, Gonyou-McLean was released on a $1,000 bond and 27 bail conditions that heavily restrict his behaviour and movements, according to court records.

4- *Radio-Canada - Manitoba* (site web) rapporte qu'un **jeune homme de 17 ans a plaidé coupable, lundi, à une accusation de terrorisme, devant la Section de la jeunesse de la Cour provinciale du Manitoba. Il a admis avoir conseillé la perpétration d'un acte criminel au profit ou sous la direction d'un groupe terroriste, ou en association avec lui,** selon un communiqué du **Service des poursuites pénales du Canada**. Aucune information supplémentaire n'a été fournie sur la nature des accusations.

5- Canada must acknowledge, and then constrain, the government's use of **portable surveillance devices** that can indiscriminately dredge data from people's smartphones without them knowing, privacy experts say. Everything that is known or suspected about the government's use of these

machines – called "**IMSI catchers**," "**cell-site simulators**" or "**Stingrays**" – is chronicled in a comprehensive, first-of-its-kind, 130-page report written by privacy experts and released to *The Globe and Mail*. Federal police have used these devices for more than a decade, but the practice was confirmed only this year in a series of stories in *The Globe*. Now, researchers **Christopher Parsons** and **Tamir Israel** say it's time for civil society to **debate the pros and cons of IMSI catchers, even if many government agencies still won't discuss them.**

International

United States / États-Unis

6- **Iran threatened to shoot down two US Navy surveillance aircraft** flying close to Iranian territory in the Persian Gulf over the weekend, the latest in a series of recent provocations between Iran and the US military in the region, three US defense officials with knowledge of the incident told *Fox News*.
7- According to *The Intercept*, the **House Permanent Select Committee on Intelligence** will meet this Thursday to discuss former **National Security Agency contractor Edward Snowden**, who in 2013 gave journalists a massive cache of classified documents detailing the U.S. global surveillance regime.

United Kingdom / Royaume-Uni

Light coverage/couverture légère.

Europe

8- Selon *La Dépêche du Midi,* un **jeune interpellé dans un collège du Lot pour des propos approuvant les attentats sur le sol français, un second adolescent lotois paradant en photo avec une Kalachnikov et d'autres encore carrément partis en Syrie pour intégrer les troupes de Daesh**... Bref, la radicalisation touche le Lot. La préfète le dit et agit. Le Lot ne fait pas exception au phénomène ravageur de la radicalisation des jeunes. Phénomène souvent suivi par le départ de ceux-ci vers la Syrie. **Le département n'affole pas les compteurs et reste « dans la moyenne nationale », concernant le taux de signalement seulement, selon la préfète Catherine Ferrier.** En revanche, les départs dans les rangs de Daesh se situent au-dessus de la moyenne française. Les chiffres commentés hier par la **représentante de l'état dans le Lot font froid dans le dos : « 21 départs de Lotois vers la Syrie ont été constatés depuis 2014. Soit neuf adultes et douze adolescents.**
9- D'après *L'Agence France-Presse,* **trois réfugiés syriens, arrivés en Allemagne lors de l'afflux migratoire de 2015 et soupçonnés d'appartenance au groupe jihadiste Etat islamique (EI), ont été arrêtés mardi dans le nord du pays**, a annoncé le parquet fédéral allemand. Les trois hommes **Mahir Al-H., 27 ans, Mohamed A., 26 ans, et Ibrahim M. 18 ans ont été interpellés dans le Schleswig-Holstein et leurs appartements font l'objet de perquisitions.** Ils étaient arrivés en Allemagne en novembre 2015, au pic de la crise migratoire qui a vu un million de demandeurs d'asile entrer dans le pays.
10- A statement from **Germany's Federal Public Prosecutor's** office today confirmed earlier media reports that federal police and agents from **Germany's GSG 9 special operations unit were involved in pre-dawn raids against terror suspects. Three men were arrested in the raids**. All three are **Syrian nationals** and the prosecutor's office listed their names as **Mahir Al-H. (17), Mohamed A. (26), and Ibrahim M. (18).** The full names of criminal suspects in Germany are usually not released by officials. *Deutsche Welle* writes that the men **are suspected of being members of a foreign terror organization, the so-called "Islamic State" ("IS").**
11- **Professor Gilles Kepel**, a scholar of Islam, has warned of civil war across **Europe as more young Muslims facing poor job prospects turn to radical groups**, and has said a growing **'Jihad Generation'** is likely to continue to **carry out terror acts in European cities,** the *Daily*

Mail Online writes. The aim of their terror activity is to **both incite hatred towards Muslims and, in doing so, cause further radicalisation among young people**, the professor of political science said. He told the German newspaper *Die Welt* that this in turn could lead to the point where **Europe enters into civil war.**

Africa / Afrique

12- **The Nigerian military** has **killed a female suicide bomber at a security checkpoint** while attempting **to gain entrance into a cattle market in Borno State on the eve of Sallah day celebration**, *All Africa News* reports.

Middle East / Moyen-Orient

13- The *Tehran Times* reports that **thousands of Canadian citizens** and residents have signed a petition, carried on the official website of the **Parliament of Canada**, calling for the re-establishment of diplomatic ties with Tehran.
14- The *Jerusalem Post* reports that the **Israeli Defence Forces is introducing an encrypted cellphone chat program for commanders**, enabling them to hold conversations in groups and share real-time text, images and other data on developing security incidents.

Afghanistan/Pakistan

15- *Pajhwok Afghan News* reports that as many as **112 insurgents and four Afghan National Army (ANA) troops have been killed** during clashes over the past 24 hours, the Ministry of Defence said on Monday.

Australia, New Zealand / Australie, Nouvelle-Zélande

16- Intelligence officials have revealed that **calls from the public to the national security hotline spiked 50 per cent in the 24 hours** after the alleged ISIS-inspired lone wolf terrorist attack at the weekend. The deluge of tip-offs to **ASIO** and the **Australian Federal Police** has also risen about **40 per cent** since April, to almost 70 a day, *The Advertiser* can reveal. As the Government grapples with the rising terrorism threat, frightening CCTV footage has captured knife-wielding suspect **Ihsas Khan** on his bloody rampage – and how victim **Wayne Greenhalgh**, 59, didn't stand a chance.
17- According to *The Australian*, NSW police are examining whether a **cluster of red flags** concerning the erratic behaviour of 22-year-old terror suspect **Ihsas Khan** was **reported but not passed on to counter-terrorism detectives** in what would amount to a **major breakdown in communication**. News of the review came as sources confirmed police had **reopened a 2015 investigation into a spitting attack** on then-federal Labor MP **Laurie Ferguson**, which police believe may have been committed by Mr Khan. Chief Commissioner **Andrew Scipione** confirmed yesterday that police in southwestern Sydney, where Mr Khan lived, had been told of his bizarre behaviour, which had alarmed his neighbours and seen him investigated by police. "He'd come to the notice of police, local police, and that had been a result of his activities," Mr Scipione said. **There was no evidence to support accounts that he had been reported to the terrorism hotline**. Deputy Commissioner Cath Burn confirmed Mr Khan was known to police but had not been identified as a priority for monitoring.

Asia / Asie

18- The *Bangladesh Sangbad Sangstha* reports that **Prime Minister Sheikh Hasina** leaves Dhaka for Canada and the United States tomorrow morning on an 11-day official visit to the two North American nations. The Bangladesh prime minister will hold a bilateral meeting with her **Canadian counterpart Justin Trudeau.** She will hand over the **"Friends of Liberation War Honour"** award to Justin Trudeau.

19- *Kyodo News* is reporting that Prime Minister **Shinzo Abe** and his Canadian counterpart **Justin Trudeau** agreed Tuesday to **coordinate their response to North Korea's provocative acts**, including last week's nuclear test, through the framework of the United Nations, a Japanese government spokesman said. In their roughly 20-minute telephone meeting, Abe and Trudeau shared their resolute condemnation of North Korea's behavior, Deputy Chief Cabinet Secretary **Koichi Hagiuda** said.
20- China and Canada agreed on Monday to **start discussions on a bilateral extradition treaty** that would facilitate the **return of corrupt fugitive Chinese officials** who remain at large in Canada. The agreement was reached at the **China-Canada High-Level National Security and Rule of Law Dialogue** in Beijing, where discussions were held on ways to improve cooperation on issues such as law enforcement, combating transnational organized crime, judicial cooperation and exchanges on the rule of law, reports the *China Daily*.
21- The United States on Tuesday **sent two nuclear-capable supersonic bombers** streaking over ally South Korea in a **show of force meant to cow North Korea after its recent nuclear test** and also to settle rattled nerves in the South. The **B-1B bombers**, escorted by U.S. and South Korean jets, were seen by an *Associated Press* photographer as they flew over **Osan Air Base**, which is 120 kilometers (75 miles) from the border with North Korea, the world's most heavily armed. The bombers were likely to return to Andersen Air Force Base in Guam, without landing in South Korea.
22- The *Times of India* reports that a **grenade attack by terrorists** in Anantnag's Sherbagh police station killed one civilian and left 14 people including three cops critically wounded shortly after the state government decided to impose **curfew in all 10 Kashmir districts** to prevent any outbreak of violence.

Americas / Amériques

Light coverage/couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Tuesday, September 13 2016
le mardi 13 septembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- Selon *Radio-Canada Nouvelles,* « La menace qui pèse sur vous en tant que fonctionnaire canadien en voyage officiel est bien réelle. » **Le Service canadien du renseignement de sécurité (SCRS) vient tout juste de mettre à jour ses directives sur les voyages à l'intention des fonctionnaires fédéraux.** Obtenu par Radio-Canada Ottawa-Gatineau, ce document interne d'une quarantaine de pages insiste sur **l'importance pour les employés du gouvernement d'être extrêmement prudents à l'étranger. Le SCRS soutient que « la menace terroriste qui pèse sur les Canadiens a changé » depuis les attaques survenues à Saint-Jean-sur-Richelieu et au Parlement canadien en octobre 2014.** (Similar reports appeared on *CBC News Ottawa radio and television*).

2- People who have been **deemed a terrorist threat should be incarcerated if they can't be monitored around the clock,** Conservative leadership candidate **Tony Clement** said Monday in **outlining his national security platform**. "If the safety of the public cannot be guaranteed through a peace bond, it has to be guaranteed through incarceration," he told reporters on Parliament Hill. Clement also wants **terrorist suspects to be on a published "wanted" list,** reports *CBC News*. Clement said both measures would be subject to judicial review and require an "**evidentiary threshold**" be met. "I'm not proposing some kind of wanted list that is the figment of somebody's imagination or without some kind of evidence," Clement said. "Clearly, that would not be acceptable in Canadian society." Clement repeated his **proposal for the "enhanced screening" of people coming in and out of Canada** as part of his national security platform. **He said the current process is not rigorous enough**. "**Only nine to 15 per cent of the current intake of immigrants in any given year go through the rigorous screening of CSIS and other security agencies**," he said. "That's just far too low."

Canada

3- Within days of a foiled terror plot that ended in the death of **Aaron Driver**, a known Islamic State supporter in southern Ontario, Canada's federal police arrested **another young man over fears he would participate in terrorism,** *VICE News* has learned. Ottawa man **Tevis Gonyou-McLean**, 24, was **arrested on August 12 and charged with uttering a threat to cause death or harm to another person**. The RCMP are also pursuing a terror-related **peace bond against him over fears that he might engage in terrorism at home and abroad**. At the end of August, Gonyou-McLean was released on a $1,000 bond and 27 bail conditions that heavily restrict his behaviour and movements, according to court records.

4- *Radio-Canada - Manitoba* (site web) rapporte qu'un **jeune homme de 17 ans a plaidé coupable, lundi, à une accusation de terrorisme, devant la Section de la jeunesse de la Cour provinciale du Manitoba. Il a admis avoir conseillé la perpétration d'un acte criminel au profit ou sous la direction d'un groupe terroriste, ou en association avec lui,** selon un communiqué du **Service des poursuites pénales du Canada**. Aucune information supplémentaire n'a été fournie sur la nature des accusations.

5- Canada must acknowledge, and then constrain, the government's use of **portable surveillance devices** that can indiscriminately dredge data from people's smartphones without them knowing, privacy experts say. Everything that is known or suspected about the government's use of these

machines – called "**IMSI catchers**," "**cell-site simulators**" or "**Stingrays**" – is chronicled in a comprehensive, first-of-its-kind, 130-page report written by privacy experts and released to *The Globe and Mail*. Federal police have used these devices for more than a decade, but the practice was confirmed only this year in a series of stories in *The Globe*. Now, researchers **Christopher Parsons** and **Tamir Israel** say it's time for civil society to **debate the pros and cons of IMSI catchers, even if many government agencies still won't discuss them.**

International

United States / États-Unis

6- **Iran threatened to shoot down two US Navy surveillance aircraft** flying close to Iranian territory in the Persian Gulf over the weekend, the latest in a series of recent provocations between Iran and the US military in the region, three US defense officials with knowledge of the incident told *Fox News*.

7- According to *The Intercept*, the **House Permanent Select Committee on Intelligence** will meet this Thursday to discuss former **National Security Agency contractor Edward Snowden**, who in 2013 gave journalists a massive cache of classified documents detailing the U.S. global surveillance regime.

United Kingdom / Royaume-Uni

Light coverage/couverture légère.

Europe

8- Selon *La Dépêche du Midi,* un **jeune interpellé dans un collège du Lot pour des propos approuvant les attentats sur le sol français, un second adolescent lotois paradant en photo avec une Kalachnikov et d'autres encore carrément partis en Syrie pour intégrer les troupes de Daesh**... Bref, la radicalisation touche le Lot. La préfète le dit et agit. Le Lot ne fait pas exception au phénomène ravageur de la radicalisation des jeunes. Phénomène souvent suivi par le départ de ceux-ci vers la Syrie. **Le département n'affole pas les compteurs et reste « dans la moyenne nationale », concernant le taux de signalement seulement, selon la préfète Catherine Ferrier.** En revanche, les départs dans les rangs de Daesh se situent au-dessus de la moyenne française. Les chiffres commentés hier par la **représentante de l'état dans le Lot font froid dans le dos : « 21 départs de Lotois vers la Syrie ont été constatés depuis 2014. Soit neuf adultes et douze adolescents.**

9- D'après *L'Agence France-Presse,* **trois réfugiés syriens, arrivés en Allemagne lors de l'afflux migratoire de 2015 et soupçonnés d'appartenance au groupe jihadiste Etat islamique (EI), ont été arrêtés mardi dans le nord du pays**, a annoncé le parquet fédéral allemand. Les trois hommes **Mahir Al-H., 27 ans, Mohamed A., 26 ans, et Ibrahim M. 18 ans ont été interpellés dans le Schleswig-Holstein et leurs appartements font l'objet de perquisitions.** Ils étaient arrivés en Allemagne en novembre 2015, au pic de la crise migratoire qui a vu un million de demandeurs d'asile entrer dans le pays.

10- A statement from **Germany's Federal Public Prosecutor's** office today confirmed earlier media reports that federal police and agents from **Germany's GSG 9 special operations unit were involved in pre-dawn raids against terror suspects. Three men were arrested in the raids**. All three are **Syrian nationals** and the prosecutor's office listed their names as **Mahir Al-H. (17), Mohamed A. (26), and Ibrahim M. (18).** The full names of criminal suspects in Germany are usually not released by officials. *Deutsche Welle* writes that the men **are suspected of being members of a foreign terror organization, the so-called "Islamic State" ("IS").**

11- **Professor Gilles Kepel**, a scholar of Islam, has warned of civil war across **Europe as more young Muslims facing poor job prospects turn to radical groups**, and has said a growing **'Jihad Generation'** is likely to continue to **carry out terror acts in European cities,** the *Daily*

Mail Online writes. The aim of their terror activity is to **both incite hatred towards Muslims and, in doing so, cause further radicalisation among young people**, the professor of political science said. He told the German newspaper *Die Welt* that this in turn could lead to the point where **Europe enters into civil war.**

Africa / Afrique

12- **The Nigerian military** has **killed a female suicide bomber at a security checkpoint** while attempting **to gain entrance into a cattle market in Borno State on the eve of Sallah day celebration**, *All Africa News* reports.

Middle East / Moyen-Orient

13- The *Tehran Times* reports that **thousands of Canadian citizens** and residents have signed a petition, carried on the official website of the **Parliament of Canada**, calling for the re-establishment of diplomatic ties with Tehran.
14- The *Jerusalem Post* reports that the **Israeli Defence Forces is introducing an encrypted cellphone chat program for commanders**, enabling them to hold conversations in groups and share real-time text, images and other data on developing security incidents.

Afghanistan/Pakistan

15- *Pajhwok Afghan News* reports that as many as **112 insurgents and four Afghan National Army (ANA) troops have been killed** during clashes over the past 24 hours, the Ministry of Defence said on Monday.

Australia, New Zealand / Australie, Nouvelle-Zélande

16- Intelligence officials have revealed that **calls from the public to the national security hotline spiked 50 per cent in the 24 hours** after the alleged ISIS-inspired lone wolf terrorist attack at the weekend. The deluge of tip-offs to **ASIO** and the **Australian Federal Police** has also risen about **40 per cent** since April, to almost 70 a day, *The Advertiser* can reveal. As the Government grapples with the rising terrorism threat, frightening CCTV footage has captured knife-wielding suspect **Ihsas Khan** on his bloody rampage – and how victim **Wayne Greenhalgh**, 59, didn't stand a chance.
17- According to *The Australian*, NSW police are examining whether a **cluster of red flags** concerning the erratic behaviour of 22-year-old terror suspect **Ihsas Khan** was **reported but not passed on to counter-terrorism detectives** in what would amount to a **major breakdown in communication**. News of the review came as sources confirmed police had **reopened a 2015 investigation into a spitting attack** on then-federal Labor MP **Laurie Ferguson**, which police believe may have been committed by Mr Khan. Chief Commissioner **Andrew Scipione** confirmed yesterday that police in southwestern Sydney, where Mr Khan lived, had been told of his bizarre behaviour, which had alarmed his neighbours and seen him investigated by police. "He'd come to the notice of police, local police, and that had been a result of his activities," Mr Scipione said. **There was no evidence to support accounts that he had been reported to the terrorism hotline**. Deputy Commissioner Cath Burn confirmed Mr Khan was known to police but had not been identified as a priority for monitoring.

Asia / Asie

18- The *Bangladesh Sangbad Sangstha* reports that **Prime Minister Sheikh Hasina** leaves Dhaka for Canada and the United States tomorrow morning on an 11-day official visit to the two North American nations. The Bangladesh prime minister will hold a bilateral meeting with her **Canadian counterpart Justin Trudeau.** She will hand over the **"Friends of Liberation War Honour"** award to Justin Trudeau.

19- *Kyodo News* is reporting that Prime Minister **Shinzo Abe** and his Canadian counterpart **Justin Trudeau** agreed Tuesday to **coordinate their response to North Korea's provocative acts**, including last week's nuclear test, through the framework of the United Nations, a Japanese government spokesman said. In their roughly 20-minute telephone meeting, Abe and Trudeau shared their resolute condemnation of North Korea's behavior, Deputy Chief Cabinet Secretary **Koichi Hagiuda** said.
20- China and Canada agreed on Monday to **start discussions on a bilateral extradition treaty** that would facilitate the **return of corrupt fugitive Chinese officials** who remain at large in Canada. The agreement was reached at the **China-Canada High-Level National Security and Rule of Law Dialogue** in Beijing, where discussions were held on ways to improve cooperation on issues such as law enforcement, combating transnational organized crime, judicial cooperation and exchanges on the rule of law, reports the *China Daily*.
21- The United States on Tuesday **sent two nuclear-capable supersonic bombers** streaking over ally South Korea in a **show of force meant to cow North Korea after its recent nuclear test** and also to settle rattled nerves in the South. The **B-1B bombers**, escorted by U.S. and South Korean jets, were seen by an *Associated Press* photographer as they flew over **Osan Air Base**, which is 120 kilometers (75 miles) from the border with North Korea, the world's most heavily armed. The bombers were likely to return to Andersen Air Force Base in Guam, without landing in South Korea.
22- The *Times of India* reports that a **grenade attack by terrorists** in Anantnag's Sherbagh police station killed one civilian and left 14 people including three cops critically wounded shortly after the state government decided to impose **curfew in all 10 Kashmir districts** to prevent any outbreak of violence.

Americas / Amériques

Light coverage/couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Wednesday, September 14 2016
le mercredi 14 septembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- Just two days after known ISIS supporter **Aaron Driver** was killed in a confrontation with police in Strathroy, Ont., **RCMP in Ottawa arrested a 24-year-old man over concerns he would engage in terrorism**. *CBC News* reports that police took **Tevis David Gonyou-McLean** of Ottawa into custody on Aug. 12, alleging he **uttered a threat to cause death or bodily harm "to unspecified persons,"** according to court documents. RCMP are now trying to convince a judge to **issue an extraordinary peace bond** against Gonyou-McLean. On Aug. 26, after two weeks in custody, Gonyou-McLean was released on a $1,000 bond with orders to abide by 27 conditions. Gonyou-McLean is also **barred from communicating with six people**, including Ottawa twin brothers **Ashton and Carlos Larmond**, who are currently serving prison sentences for terror-related offences. He also can't communicate with **Awso Peshdary**, who is awaiting pre-trial in December for terror-related offences, and **Luqmann Abdunnur**. At least one security expert doesn't believe those conditions go far enough, however 'Why isn't he being held?' "It would seem to me that if he's charged, then why isn't he being held?" asked **Phil Gurski**, a **former CSIS agent** who now runs a private security firm. "That's an interesting question about whether or not people accused of terrorism offences, or potential terrorism offences, should be released on bail. That's a whole other argument we have to ask."

Canada

2- Selon *Le Monde,* la **République islamique détient au moins huit binationaux, dont trois Américains, trois Britanniques et une Canadienne.** Vendredi 9septembre au matin, **Nazanin Zaghari-Ratcliffe a pu téléphoner depuis la prison d'Evin, à Téhéran, à son mari Richard, à Londres.** Cela faisait des semaines qu'ils n'avaient pas été en contact direct, mais les nouvelles n'étaient pas bonnes. L'Anglo-Iranienne a révélé le verdict qui venait de lui être signifié: cinq ans de prison. Les charges qui pèsent contre elle? Elles n'ont pas été dévoilées. «Sécurité nationale» , s'est contenté d'indiquer le gardien de prison qui surveillait l'appel téléphonique.

3- An Ottawa mosque visited by Prime Minister **Justin Trudeau** this week said it's **"categorically false"** that their Imam has **links to a terror group**. *The Ottawa Sun* reported Monday that **Ottawa Muslim Association's** imam, **Samy Metwally**, is listed as a member of the **International Union of Muslim Scholars** on the OMA's website. The IUMS was **designated a terrorist organization** by the **United Arab Emirates** and faces criticism from various experts for its supposed ties to the **Muslim Brotherhood**. **"These accusations are, of course, categorically false in what they insinuate and grossly unfair,"** OMA President **Naeem Malik** said in a statement. "The OMA and Imam Metwally do not have any ties to terrorist organizations nor do they harbour any ideology in favour of terrorism or extremism." However, the statement does not at any point address what specifically is incorrect about the *Sun's* reporting and the OMA **did not respond to requests for clarification**. Their release concludes: **"No further statement will be issued, nor will we be available for contact by the media."**

International

United States / États-Unis

4- Appearing before the **Senate Armed Services Committee** Tuesday, **NSA director Michael Rogers,** reports *Reuters,* said the **American intelligence community** continues to be **"actively concerned"** about the possibility **foreign governments** may be attempting to **undermine** the **November elections** through **cyber-attacks**. Under questioning, however, Rogers said he **could not provide specifics** about the spy agencies' current assessment of the alleged hacking in a public setting and **declined to characterize the activity** as by a **foreign nation-state.**
5- According to the *Washington Free Beacon,* the **Office of the Director of National Intelligence declined** to conduct a **required assessment** of the **damage to national security** caused by **Hillary Clinton sending** and **receiving secrets** on a **private email server** while she was Secretary of State. DNI **James Clapper agreed with security officials** who argued against the need to carry out the damage assessment. Intelligence officials argued in internal discussions that since many details of the drone missile program targeting terrorists were disclosed in earlier leaks unrelated to Clinton's use of a personal email server, gauging the **damage done by her conduct** would be **difficult**, and possibly **unnecessary.**
6- The *Washington Post* reports the **Pentagon** and **intelligence community** are expected to **recommend soon** to **President Obama** that he **break up** the **joint leadership** of the **National Security Agency** and **U.S. Cyber Command** to create **two distinct forces** for **electronic espionage** and **cyber-warfare** but in an exchange with the Senate Armed Services Committee yesterday, **NSA** and **Cyber Command director Rogers** told chair **John McCain** that he still held the position that the current **"dual hat" relationship** between the two departments be **retained.**

United Kingdom / Royaume-Uni

7- Speaking to the *Guardian,* **Edward Snowden** called Prime Minister **Theresa May** "a sort of **Darth Vader** in the United Kingdom", argued the **disclosure** of the scale of **surveillance** by **American** and **British intelligence agencies** was not only **morally right** but had **left citizens better off** and predicted in the **"fullness of time"** he will **return** to the **United States.** Snowden's supporters and his American solicitor have embarked on a campaign for a **Presidential pardon** before Barack Obama leaves office in January but two U.S. officials disclosed to *Reuters* that's **unlikely.**
8- A **19-year-old** accused of planning to carry out a **mass-casualty terror attack on London landmarks**, including **Buckingham Palace** and **Oxford Street**, will make his next court appearance next week after being remanded yesterday. **Haroon Ali-Syed** from Hounslow in west London, allegedly attempted to **buy a bomb over the internet** as well as **guns** this year. (Moderate coverage / couverture modérée).
9- Two days after he resigned his seat in the House of Commons, **David Cameron** was **sharply criticized** by an **inquiry** by **parliament's Foreign Affairs Select Committee** which concluded the former Prime Minster, relying on **poor intelligence**, approved a **botched 2011 intervention in Libya** which toppled Muamar Gaddafi and, said the inquiry**, caused the rise of Islamic State in north Africa.** (Extensive coverage / vaste couverture).
10- **GCHQ** has started an ambitious plan to **create a national firewall** to **block malicious websites.** (Extensive coverage / vaste couverture).

Europe

11- Un **adolescent "qui s'était proposé pour une action terroriste" a été arrêté ce matin à Paris et placé en garde à vue**, a appris *l'Agence France Presse* de sources proches de l'enquête. Né en septembre 2001, le suspect, arrêté dans le XXe arrondissement dans le nord-est de la capitale, était "en lien avec le **jihadiste français Rachid Kassim**", déjà au coeur de plusieurs enquêtes dont celle sur un commando de femmes démantelé la semaine dernière. Samedi, un autre adolescent, âgé de 15 ans, également en lien avec ce jihadiste et soupçonné de pouvoir "passer à l'acte", avait été arrêté à Paris.

12- Selon *Ouest-France,* un **jeune homme de 26 ans, adopté, s'est converti lors d'un de ses passages en détention**. Il est **jugé pour avoir violé son assignation à résidence et consulté des sites djihadistes**. Il se fait appeler **Daoud Abdillahi Houssein. David Pagerie**, à l'état civil, comparaît ce mercredi devant le tribunal correctionnel d'Angers. La justice reproche à cet Angevin de 26 ans d'avoir violé son assignation à résidence. **En surfant sur la messagerie cryptée Telegram, celle des terroristes récemment passés à l'acte en France, il pourrait aussi avoir consulté des sites liés au terrorisme. Des vidéos d'exécution ont été retrouvées sur son téléphone mobile.**
13- D'après *Le Soir,* (Belgique), une **disposition oblige dorénavant les commerçants à signaler les clients suspects La Belgique veut encadrer la vente de produits pouvant servir à la fabrication d'explosifs.** Une incitation à la délation sur la base de critères peu précis. A partir du 19 septembre prochain, toute personne ayant eu connaissance de vols, de **disparitions ou de transactions suspectes de « précurseurs d'explosifs » est tenue, en vertu d'une loi portant exécution d'une norme européenne, de le signaler auprès de la police fédérale**. Certaines substances chimiques, le nitrate d'ammonium et le perchlorate de potassium, par exemple, peuvent en effet servir à la fabrication de charges explosives telles que celles utilisées lors des **attentats de Paris et de Bruxelles.**
14- **Angry** at **Austria's "anti-Turkish political stance"**, a **Turkish hacking collective** calling itself **'Aslan Neferler'**, allegedly attempted to **break into the systems** of the **National Bank of Austria.** *The Local* observed the **same group** was behind behind an **attempted cyber attack** at **Vienna airport** two weeks ago.
15- **Two Swedish officials** will be permitted to **enter Ecuador's Embassy** in **London** on **October 17** to **question Julian Assange** on sexual assault charges reports *The Local.*

Africa / Afrique

16- In May, when **Isis fighters** struck **within a mile** of where **500 metric tons** of **chemical-weapon precursor materials** were **stored** in a **remote desert region of Libya,** the incursion set off a hurried chain of events culminating in a **disarmament operation** involving the **United States, European countries** and the **United Nations** reports the *Washington Post.*
17- Selon *Espace Manager,* (Tunisie), le **nouvel ambassadeur de France à Tunis s'appelle Olivier Poivre d'Arvor.** Tout ce qu'on sait de lui c'est que Tunis sera son premier poste à l'étranger. Certains doutent de sa capacité à pouvoir diriger l'ambassade de France à Tunis. Ses premières déclarations leur donnent malheureusement raison. En effet, interrogé sur ses priorités à Tunis par la radio RTL, **Olivier Poivre d'Arvor a eu cette déclaration tout à fait surprenante. Selon lui, sa « mission principale », « c'est d'assurer la sécurité des Français qui se trouvent en Tunisie.**

Middle East / Moyen-Orient

18- The *Times of Israel* reports that **Israel's new spy satellite, the Ofek-11 reconnaissance satellite** launched on Tuesday evening may be malfunctioning, officials involved in the project said a few hours after launch, though they said they have been able to make contact with the craft.
19- The *Lebanon Daily Star* reports that a **new cease-fire in Syria** brought a full day with no combat deaths in the war between **President Bashar Assad** and his opponents, a monitoring body said, and efforts to deliver aid to besieged areas got cautiously underway.

Afghanistan/Pakistan

20- *TOLO News* reports that Badakhshan officials said on Tuesday that **Taliban has seized security forces' equipment and weapons** in the province and are now using these against government troops.

Australia, New Zealand / Australie, Nouvelle-Zélande

21- According to *ABC News*, court documents have revealed Australia's spy agency **ASIO** was **fed information about two Sydney men** who were plotting to carry out a terrorist attack on behalf of Islamic State. **Omar Al-Kutobi**, 25, and **Mohammad Kiad**, 27, were **under surveillance for about a month** when they were arrested and charged with preparing to carry out a terrorist attack in February 2015. Court documents reveal an informant tipped off the **Joint Counter-Terrorism Team (JCCT)** to the plot on February 10 and said the attack was imminent.
22- Counter-terrorism authorities **could be given greater access to intelligence on criminals, local police reports, medical data and welfare information to better identify potential terrorists.** The government is examining ways information that might help identify people with extremist tendencies **could be cross-checked with other data bases to home in on potential terrorists**. The work was announced by **Malcolm Turnbull** in July and spearheaded by then counter-terrorism co-ordinator **Greg Moriarty**, who since has become the Prime Minister's foreign policy adviser. Since then, work has focused on **examining the personality and behavioural traits** of terrorists or extremists with a view to identifying potential markers, *The Australian* has been told.

Asia / Asie

23- *The Hindu* reports that in an indicator that **India** is going ahead with its SAARC commitment ahead of the summit of the grouping in Islamabad, the **chief of India's Intelligence Bureau (IB)** will address the representatives of anti-terror forces of other member-countries of the South Asian Association for Regional Cooperation on September 22.
24- According to *Reuters*, U.S. Secretary of State **John Kerry** will meet with his Japanese and South Korean counterparts in New York on Sunday to **discuss responses to North Korea's latest nuclear test**, South Korea's foreign ministry said on Wednesday. The three countries are pushing for **tough new U.N. Security Council sanctions** on North Korea after the isolated country on Friday conducted its fifth and largest nuclear test. The blast was in defiance of U.N. sanctions that were tightened in March. China, the North's chief ally, **backed the March resolution but is more resistent to harsh new sanctions** this time after the United States and South Korea decided to deploy a sophisticated anti-missile system in the South, which China adamantly opposes. South Korea said Foreign Minister **Yun Byung-se** and his counterparts Kerry and Japanese Foreign Minister **Fumio Kishida** will meet during the annual U.N. General Assembly to discuss putting further pressure on North Korea.
25- The *Yonhap News Agency* reports that North Korea on Wednesday **protested the United States' flyover of two B-1B nuclear-capable strategic bombers** over South Korea, saying such **"reckless provocations"** should stop. The U.S. Air Force on Tuesday flew the B-1B Lancers over **Osan Air Base**, south of Seoul, as a warning to North Korea following its fifth nuclear test last week. The *North's Korean Central News Agency (KCNA)* blasted the exercise as a "military provocation" revealing Washington's intentions to mount a pre-emptive nuclear attack.

Americas / Amériques

Light coverage / couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Friday, September 16, 2016
le vendredi 16 septembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1-The sudden release of a **Canadian** held for **two years in China on suspicion of spying comes after a high-stakes campaign to secure his freedom, including an unusual and unannounced visit four months ago by the director of the Canadian Security Intelligence Service**, who met with **Chinese officials to try to persuade them that Kevin Garratt wasn't a spy**, the *Global & Mail* reports. On Thursday, a bearded Mr. Garratt landed in Vancouver and embraced his family, a free man. He had been accused by Chinese authorities of stealing military and defence research secrets and charged with espionage. The visit to China by CSIS director **Michel Coulombe, Canada's top spy, was one element of that effort, according to multiple sources with knowledge of the meeting**. When Mr. Garratt was indicted in January, China's state media said investigators had found evidence he had accepted tasks to gather intelligence for Canada. Mr. Coulombe met with **Geng Huichang, the minister in charge of China's powerful state security apparatus, to deliver the message in person that Mr. Garratt, a Pentecostal pastor, did not work for CSIS.**

2-*La Presse+* rapporte quà **chaque jour, au Canada, 1600 attaques de rançongiciels auraient lieu**. Mots de passe et dossiers confidentiels volés font régulièrement l'actualité, stimulant la recherche de nouvelles approches pour assurer la sécurité des réseaux. L'une d'elles, conçue à l'Université de Cambridge et imitant le système immunitaire humain à partir des mathématiques probabilistes, semble prometteuse. **Elle est proposée depuis 2013 par l'entreprise britannique Darktrace, qui a ouvert en avril dernier son bureau canadien, dirigé par l'ex-agent des services secrets David Masson.** Entrevue. Q D'abord, pourriez-vous vous présenter ? R **J'ai été membre du service de renseignement britannique, le MI5, pendant plus de 20 ans, puis j'ai travaillé au sein du Service canadien du renseignement de sécurité (SCRS) pendant quatre ans. Je m'occupais de cybersécurité et de sécurité nationale en général.** Je me suis ensuite joint à la compagnie Darktrace en janvier de cette année, après une invitation à établir un bureau ici, au Canada.

3-A group of **German artists** calling themselves **'Peng!'** have set up a **'Call A Spy'** hotline in which people can **contact an intelligence operative** through a **private network** that **masks the original source of the call.** Speaking to *Sputnik Deutschland,* 'Peng's!' **Ariel Fischer** said **"you can find most of the numbers on the internet,** some of them are from **professional organizations**, and some of them became known as the result of **intelligence leaks.** You just have to search. We have a lot of them, including for the **Canadian Security Intelligence Service**, NSA, CIA, FBI, BND and the BfV. There are also Italian and French intelligence services. We are also constantly searching for people who might be able to find new numbers so that we can bring 'Call a Spy' to different countries."

Canada

4-After a police raid on a **Toronto technology company**, Canada has agreed to share a massive stash of encrypted **BlackBerry** Ltd. messages with **Dutch police investigating an underworld conspiracy involving robberies, drug trafficking, attempted murder and assassinations.** But rather than simply hand over the messages, from 20,000 different users, an Ontario judge this week imposed restrictions designed to prevent a "fishing expedition" by police in the Netherlands

or any other country. **The 20,000 users**, writes the *National Post*, are said to include the **Dutch criminal suspects and their associates**, but also likely include many **innocent users of Ennetcom's service.**

International

United States / États-Unis

5-Calling **Edward Snowden** a **"criminal"**, the **House Intelligence Committee** dispatched a **bipartisan letter** to **President Obama** urging him **not to pardon** the exiled American. The letter, reports the *Washington Post,* emerged on the same day the **panel unanimously voted** to adopt a **classified report on Snowden** that, according to a three-page **unclassified summary**, portrays him as a **disgruntled employee** whose leak caused **"tremendous damage to national security."** Taking to Twitter this morning, **Snowden slammed** the committee, writing "their report is so **artlessly distorted** that it would be amusing if it weren't such a serious act of bad faith."

United Kingdom / Royaume-Uni

6-**Senior figures** at **GCHQ** are understood to be **concerned** the **government lacks a policy** to **assess** the **security risk of foreign investments**, reports *The Times of London,* after it was disclosed that **Hikvision**, a **company controlled by the Chinese government,** has **sold** more than a **million closed-circuit television cameras** and **recorders** to **British clients** who have installed them at sites including **airports, government buildings, sports stadiums** and the **London Underground.** The *Daily Telegraph* has learned **British intelligence** will, henceforth, be **consulted before foreign countries** are **allowed** to **sign major contracts** with **British companies.**

7-**Intelligence Services Commissioner Sir Mark Waller** has **criticized MI6** for **"serious failings"** in its response to allegations that **Michael Adebolajo**, one of the **killers of Lee Rigby,** had been **tortured by Kenyan authorities** following his **arrest** there in **2010.** Adebolajo was subsequently deported (Moderate coverage / couverture modérée).

Africa / Afrique

Middle East / Moyen-Orient

8-The *Jerusalem Post* reports that hundreds of Israelis killed in thousands of rocket attacks — that is the army's **Home Front Command's** estimation for what to expect in the event of a future all-out war, according to figures released ahead of a nationwide preparedness drill set for next week.

9-*The National (UAE)* reports that the fanatics of **ISIL** may be increasingly on the ropes in their Middle East stomping grounds, but in Indonesia there are fears that when those strongholds collapse they will scatter **battle-hardened extremists across South-east Asia.**

Afghanistan/Pakistan

10-The *International News* reports that the **United States** has lauded **Pakistan's progress towards combating terrorism** through recent military operations while insisting that a decisive policy shift was needed to overcome difficulties.

11-*Pajhwok Afghan News* reports that expressing concern over the **security situation in Afghanistan**, top American Senators on Thursday alleged that neighboring Pakistan continued to play a duplicitous role there.

Europe

12-**Turkish authorities detained four people** this morning as part of the investigation into a **potential threat** against **British and German diplomatic missions** in the country but found **no links** between the **suspects** and any **terrorist groups** reports the *Anadolu News Agency*. Earlier, **both embassies** announced they would be **closed today** for **unspecified security reasons.**
13-A study undertaken by **Norwegian intelligence**, reports *The Local,* has found that **88 per cent** of the **radicalized individuals in Norway** have an **ethnic background other than Norwegian** with more than 30 different nationalities represented. Additionally, **76 per cent** of the extremists have **Norwegian citizenship.** "The study confirms the pre-existing understanding of **extreme Islamism in Norway** as a **multi ethnic phenomenon**, characterized by **young men with low education, high crime rates** and a loose attachment to the labour market," the PST stated in the introduction to the study.
14-Selon *La Tribune de Genève,* la justice a prolongé de trois mois la détention préventive d'un jeune suisse. **Un Genevois soupçonné d'être en lien avec une organisation terroriste reste en prison, selon nos sources. Arrêté le 8 juin à l'aéroport de Zurich, en provenance de Turquie, A. a déjà passé trois mois en détention préventive.** « Le Tribunal des mesures de contrainte a, par décision du 8 septembre 2016 et faisant suite à la demande du Ministère public de la Confédération (MPC), prolongé la détention provisoire du prévenu pour une durée de trois mois», confirme le MPC, sans faire d'autres commentaires. Il est **reproché au jeune homme d'avoir enfreint la loi fédérale interdisant les groupes Al-Qaida, Etat islamique et les organisations apparentées.** Il est en outre prévenu de soutien, respectivement de participation à une organisation criminelle.

Australia, New Zealand / Australie, Nouvelle-Zélande

15-**Two Islamic State-inspired terrorists** who **planned to firebomb a Shi'ite** centre in **western Sydney with a homemade explosive claim they abandoned their planned attack when they saw someone nearby** because they "didn't want to hurt anyone", the *Australian* writes. **Omar al-Kutobi**, who along with **Mohammad Kiad** has pleaded guilty to planning a terror attack, said they planned to destroy the **Muhammadi Welfare Association of Australia's centre in Granville** but changed their mind when they saw a man inside.

Asia / Asie

16-China said Friday that a Canadian citizen it detained for two years over **spying allegations** was allowed to leave the country after a **local court issued a verdict in his case**, but it **refused to say what the verdict was or why he was detained at all. Kevin Garratt's** return to Canada was announced Thursday by Prime Minister **Justin Trudeau**, who said he had pressed Garratt's case with top Chinese officials. *Associated Press* reports that **Chinese state media** have previously reported that authorities found evidence that implicated Garratt in accepting tasks from **Canadian espionage agencies to gather intelligence in China**.
17-North Korea is ready to **"counter-attack"** in the face of **ongoing "provocation" from the United States**, its foreign minister said Thursday amid a spike in tension caused by Pyongyang's latest nuclear test. "The Korean people have indicated that we are ready to wage a counter-attack against provocation by enemies," Foreign Minister **Ri Yong-Ho** said at a meeting of the **Non-Aligned Movement in Venezuela**. The warning comes after two US supersonic bombers flew over South Korea on Tuesday in a show of force following North Korea's fifth and largest-ever nuclear test last week. Ri said the nuclear tests were needed to counter "threats" from Washington, reports the *Agence France Presse.*
18-The *Bangladesh Daily Star* reports that **Prime Minister Sheikh Hasina**, now in Montreal, will today hand over the "Friends of Liberation War Honour" award for late Pierre Elliot Trudeau to the latter's son, **Canadian PM Justin Trudeau.**
19-The *Times of India* reports that the world witnessed **11,774 terror attacks in 2015**, in which 28,328 people were killed and 35,320 injured. **India was the fourth worst-affected country**

after Iraq, Afghanistan and Pakistan, with 43% of 791 attacks in the country carried out by Naxalites.

Americas / Amériques
Light coverage / couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Wednesday, September 21 2016
le mercredi 21 septembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- China's security services have been **sending undercover agents into Canada on tourist visas to strong-arm expatriates to return home**, including some suspected of corruption and other criminal activities. The secret Chinese visits have raised concern among lawyers and prompted investigations by the **Canadian Security Intelligence Service** and the **RCMP**, even as the Trudeau government begins negotiations for an extradition treaty with China. According to an insider briefed on China's secret-agent operation, the Chi**nese moved to tactics that include threats and intimidation because they were were "ticked off" at Canada for "not being willing to send people back the instant they asked"** and for dragging its feet on an extradition treaty. "Nobody has been caught and nobody has been taken to court," the insider said. The revelation comes as Chinese Premier **Li Keqiang** arrives in Ottawa on Wednesday for talks with Prime Minister **Justin Trudeau**. The two leaders are expected to discuss the extradition treaty between China and Canada Toronto refugee and immigration lawyer Lorne Waldman told *The Globe and Mail* some of **his Chinese clients in Canada have received cellphone messages from Chinese security officials threatening them and their families if they do not return home.** One client suspected that people watching him "might be from the Chinese government," he said. Mr. Waldman said he has worked with at least six people sought by China as fugitives. In the past year, two of them and the family of a third have been approached by **CSIS agents** who **"asked them whether or not they had suffered harassment at the hands of those Chinese officials in Canada** … in relation to their return to China, or made any threats directed toward them." The most recent such meeting took place this summer when "**the officers told my clients that CSIS was investigating whether or not this type of harassment is occurring,"** he said.

Canada

2- The top-level Trudeau adviser overseeing a **possible extradition treaty with China** told the previous government that China's so-called ``**economic fugitives''** don't belong on Canadian soil, *The Canadian Press* has learned. Then-deputy minister **Daniel Jean** offered that advice in a 2015 briefing note to the former Conservative government prior to his appointment in May as Prime Minister Justin Trudeau's national security adviser. ``**Canada does not want to be seen as a safe haven for fugitives and it is in Canada's interest to have such persons removed,**'' said the note, obtained by *The Canadian Press* under the Access to Information Act. In his new role with the Liberal government, Jean was in Beijing last week for the start of a new ``high level dialogue'' between Canada and China on national security and the rule of law _ talks that include breaking ground on an extradition treaty.

3- *Le Journal de Montréal* rapporte **qu'Adil Charkaoui a affiché publiquement sa préférence pour le candidat à la direction du Parti québécois Alexandre Cloutier à cause de sa position modérée sur la question identitaire.** «Le Collectif québécois contre l'islamophobie n'a pas appuyé publiquement Alexandre Cloutier. Néanmoins, il nous apparaît clairement qu'Alexandre Cloutier demeure la voix la plus modérée au sein du PQ et surtout qu'il comporte au sein de son équipe bon nombre de conseillers maghrébins musulmans pratiquants, chose qui est tout à fait à son honneur», a lancé M. Charkaoui dans une vidéo publiée sur la page Facebook du Collectif

hier. **L'imam Charkaoui avait été propulsé dans la campagne péquiste vendredi par un message twitter de Jean-François Lisée, qui l'associait à Alexandre Cloutier.**
4- The race to create **new cryptographic standards** before super-fast quantum computers are built that can rip apart data protected by existing encryption methods isn't going fast enough, two senior Canadian officials have warned a security conference. "I think we are already behind," **Scott Jones**, deputy chief of IT security at the **Communications Security Establishment (CSE),** responsible for securing federal information systems, told the **fourth annual international workshop on quantum-safe cryptography** in Toronto on Monday. **Quantum computing** – or more accurately, computers that use quantum mechanics – is not a dream, Jones and others told the conference of business executives, crypto academics, IT companies and government officials. One prediction is there's a one in seven chance that by 2026 a quantum computer will exist that can break RSA-2048 encryption. It may take longer — or, if there's an advance, shorter. "Quantum represents a fundamental change and challenge to encryption for all of us," **Jones said, noting that encrypted transactions are the backbone of security and trust on the Internet**. His comments were backed by **David Sabourin**, CSE's manager of cryptographic security, who said that if the 2026 prediction is right "we're in trouble." Speaking on a panel of government experts, Sabourin noted the **U.S.-based National Institute of Standards and Technology (NIST)** will close its call for proposed new and more quantum-secure public key encryption algorithms next year, writes *IT World Canada*.

International

United States / États-Unis

5- In a rare public comment, the **CIA's top Russia analyst Peter Clement** said **Vladimir Putin** is **likely** to **run** for **re-election as president in 2018** and may impose **tougher authoritarian rule to curb unrest** over the slumping economy. Clement, reports *Reuters,* said he has seen some "indicators" of where Putin is likely taking Russia.including a recent news report of a possible **"major restructuring" of Russia's intelligence services**. "What I see there is the **potential tightening up of society,**" said the Agency analyst, adding that he thinks **Putin "genuinely, genuinely fears instability and disorder."**
6- Director of National Intelligence **James Clapper**, reports the *Associated Press,* has made it crystal clear that he is **opposed** to a **presidential pardon** for **Edward Snowden**. "I could understand what he did, if ... what he exposed was limited to domestic surveillance. ... But he exposed so much else that had absolutely nothing to do with domestic surveillance, where he has **damaged our capability against foreign threats.** He has taken away capabilities that were used to protect our troops in Afghanistan," Clapper said. "I don't think I could concur in offering him a pardon."
7- The State Department has placed **Jund al Aqsa**, an **al Qaeda front group in Syria,** on the **U.S. government's list** of **specially designated global terrorist organizations.** (Moderate coverage / couverture modérée).

United Kingdom / Royaume-Uni

8- Speaking in Washington, **MI6 director Alex Younger,** reports the *Daily Telegraph,* said the actions of **Edward Snowden undermined trust** between **intelligence agencies** and **technology companies** and been **"highly problematic"**.

Europe

9- Selon l'*Agence France-Presse,* la **garde à vue de huit hommes interpellés pour des vérifications dans l'enquête sur l'attentat qui a fait 86 morts à Nice le 14 juillet** a été prolongée, a-t-on appris de source proche du dossier. "On est toujours en vérifications. Pour le

moment on n'a pas de certitude. Les huit restent en garde à vue", a précisé cette source, en indiquant que la garde à vue pouvait durer jusqu'à vendredi après-midi mais qu'elle "pourrait se terminer plus vite pour certains".
10- A **German immigration official**, identified as **'TSP'**, has been **arrested** and **charged** with **espionage** for an **Indian secret service** for allegedly **spying on members** of the **Sikh religion** reports *The Local.* Working at an immigration office in the western region of Ostwestfalen, prosecutors allege the 58-year-old **accessed databases** to pass on information on **suspected extremist** and **opposition members** of the religious group.
11- *Süddeutsche Zeitung* has learned that **Russia** is the **prime suspect** behind the **hacking** of **several German political parties** over the summer. Security experts employed by the German government believe a foreign power initiated the attacks in order to **gain sensitive information that could influence next year's national election.** It was revealed that **politicians and employees of several parties** received **emails** on **August 15th** and **August 24th** which appeared to come from **NATO headquarters.** Within the email was a link which, if clicked on, would enable spying software to be downloaded onto the computer.

Africa / Afrique

12- The **hunt continues** for three engineers, including a **Canadian**, who were **kidnapped in Libya** near the Algerian border reports the *Associated Press.* **Hassan Osman Eissa** of the Ghat municipal council said the **abductors are known to local authorities** and have **carried out carjackings and robberies in the past.** Eissa stated local security forces are searching for them and raiding suspected hideouts. **Global Affairs Canada spokesman Michael O'Shaughnessy** said "we are aware of the troubling yet unconfirmed report of the abduction of a Canadian citizen in Libya. We are diligently pursuing all appropriate channels."
13- D'après *All Africa,* le **président du Sénat français, Gérard Larcher, a affirmé lundi à Paris qu'avec l'Algérie "nous pouvons trouver des réponses" au terrorisme.** "Avec l'Algérie, nous pouvons trouver des **réponses pour surmonter le terrorisme"**, a-t-il dit.

Middle East / Moyen-Orient

14- The *Fars News Agency* reports that Lieutenant Commander of the Islamic Revolution Guards Corps Navy General Alireza Tangsiri announced that his forces had detained **Canadian and Australian forces** before they captured the US and British marines for violating Iran's territorial waters in the **Persian Gulf** in the past.
15- *Now Lebanon* reports that **Nizar Zakka, a Lebanese citizen and U.S. permanent** resident detained for a year in Iran over **spying allegations** has been sentenced to 10 years in prison and a $4.2 million fine, his supporters said Tuesday, the latest move in a crackdown on those with foreign ties following last year's nuclear deal.

Afghanistan/Pakistan

16- *Khaama Press* reports that the **Afghan intelligence operatives foiled a deadly suicide attack plot** by arresting a suicide attack organizer along with a would-be bomber in southeastern Khost province.

Australia, New Zealand / Australie, Nouvelle-Zélande

17- The potential return of dozens of Australian children from Islamic State-controlled Syria and Iraq has prompted **state and federal authorities to workshop how they will reintegrate a generation of battle-scarred children back into community life,** *The Australian* has been told. With Western governments increasingly confident they have Islamic State in retreat, Australian authorities have begun war-gaming how to handle a potential influx of hardened jihadists driven out of Syria and northern Iraq. About **110 Australians are thought to be fighting in Syria and Iraq**. While the threat that returning foreign fighters pose to communities has long been known, a

new challenge emerging is how to deal with children who have been exposed to the violence of the Syrian war, perhaps for years on end.

Asia / Asie

18- The *Times of India* reports that the **UK, Canada and Australia** have issued advisories asking their citizens to avoid visiting five northeastern states, parts of Jammu & Kashmir and the India-Pakistan border.

19- Two **U.S. supersonic bombers flew over South Korea on Wednesday**, with one of them landing at an air base 40 km (25 miles) south of the capital, the second such flight since North Korea's Sept. 9 nuclear test. U.S. Forces Korea said the flight by a pair of B-1B Lancer strategic bombers based in Guam was a **show of force and of U.S. commitment to preserve the security of the peninsula and the region**. The United States, which has about 28,500 troops in South Korea, flew two B-1 bombers on Sept. 13 escorted by U.S. and South Korean fighter jets in a show of solidarity with Seoul. The South's *Yonhap news agency* said the aircraft flew over a U.S. live-fire training site in the Pocheon area bordering the North (moderate coverage / couverture modérée)

20- Premier **Li Keqiang** has told US President **Barack Obama** that Beijing supports closer cooperation in the **UN Security Council** and in enforcement efforts to halt **North Korea's nuclear programme**. This could be a **signal Beijing will support tougher sanctions on North Korea after its fifth nuclear test**, with China increasingly irked by Pyongyang's behaviour and its consequences - a decision by Seoul to deploy a US anti-missile system, reports the *South China Morning Post*.

Americas / Amériques

21- **Venezuela** has accused the **United States** of **spying** on the **Non-Aligned Movement summit** it recently hosted, saying Venezuelan fighter jets **intercepted a US surveillance plane** and forced it to turn back reports *Agence France-Presse*.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Monday, September 26 2016
le lundi 26 septembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- Canadians are being encouraged to ask more questions about the security of their electronic devices from an unlikely source: an executive at the country's electronic intelligence agency, reports the *Toronto Star*. **Scott Jones**, the deputy director of IT security at the **Communications Security Establishment**, said Canadians need to **start taking a greater interest in how their electronic devices protect personal information.** "We should be asking when we go and buy the stuff we have at home, **OK, tell me how it's being protected**," Jones said in an interview. **It may surprise some to hear an employee at CSE counselling Canadians to protect their private information**. The agency, which has largely operated in secret since its creation at the end of the Second World War, was thrust into the spotlight after U.S. whistleblower **Edward Snowden's** disclosures. While police and intelligence agencies argue about whether citizens should have access to strong encryption, the federal government, on the other hand, is trying to improve its own electronic defences. Known as "**Part B**" of CSE's mandate, cyber-defence operations require the **agency to work with a host of other federal departments to try and protect government information — including Canadians' personal information.** For **serious cyberattacks**, the response could include the **RCMP, CSIS, Public Safety, Shared Services Canada**, even **Global Affairs** and the **Privy Council Office**.

Canada

2- Ottawa has **confirmed that a Canadian is among three people taken hostage in Libya earlier this week**. In a statement Sunday, Global Affairs spokesman **Michael O'Shaughnessy** says the Canadian government is **"diligently pursuing all appropriate channels to obtain more information about this troubling incident."** He says the government will not comment further or release any information that may compromise efforts to secure the hostages' release or endanger the safety of Canadian citizens. The other two people taken hostage are Italians (moderate coverage / couverture modérée).

International

United States / États-Unis

3- According to an **internal law enforcement document** obtained by *BuzzFeed News,* the **Department of Homeland Security** has determined alleged bomber **Ahmad Khan Rahami** was **likely influenced by al Qaeda** and its **online magazine 'Inspire'** which contained **bomb-making instructions.** Each one of the explosive devices — allegedly planted by Rahami in Seaside Park, New Jersey, New York City, and a train station in Elizabeth, New Jersey — was **completely different from the others.**

United Kingdom / Royaume-Uni

4- Addressing the **Labour Party Conference** in Liverpool, leader **Jeremy Corbyn questioned** the need for **MI6** to **hire 1,000 new recruits** reports the *Daily Telegraph.*

Europe

5- Speaking to the Russian media the new SVR **director Sergey Naryshkin** said **"co-operation between the intelligence services** of **various countries** is **not only possible but necessary**" Naryshkin added that **Russian intelligence** is ready to **co-operate** with the **U.S., British** and **other Western security services.**
6- More than **65 per cent** of **Swiss voters** have backed **broadened surveillance powers** for the **country's intelligence services** reports the *BBC.* The law will permit the **Federal Intelligence Service** and other agencies to **put suspects under electronic surveillance** if authorized by a court, the defence ministry and the cabinet.
7- La **police espagnole a arrêté deux Marocains accusés de soutenir le groupe djihadiste Etat islamique (EI) et peut-être aussi de projeter un attentat en Europe**, a annoncé aujourd'hui le ministère espagnol de la Défense. L'un des **accusés avait voulu rejoindre l'EI en Syrie et s'était rendu à la frontière turco-syrienne pour y rencontrer un membre de l'organisation djihadiste,** afin de subir un entraînement avant de regagner l'Europe pour participer à un attentat, a précisé le ministère selon *Le Figaro avec Reuters.*
8- Les **défenseurs des droits de l'homme dénoncent des risques de torture. Pour la Chine, c'est une victoire. Paris a transféré un ressortissant chinois en fuite**, pour la première fois depuis l'entrée en vigueur, en juillet 2015, d'un **accord d'extradition avec la France.** Il s'agit d'un ancien officiel recherché dans le cadre de la campagne de grande ampleur menée par l'Etat-parti contre la corruption. **Chen Wenhua, né en 1952, est accusé par la Chine d'avoir détourné plus de 20 millions de yuans (2,7 millions d'euros) de fonds publics** indique *Le Monde.*

Africa / Afrique

9- Selon *Jeune Afrique,* le **chef du groupe jihadiste nigérian Boko Haram, Abubakar Shekau, a diffusé dans la nuit de samedi à dimanche une nouvelle vidéo dans laquelle il dit aller parfaitement bien,** fustigeant des déclarations de l'armée nigériane qui avait annoncé l'avoir grièvement blessé le mois dernier. « Vous avez dit sur les réseaux sociaux m'avoir blessé ou m'avoir tué, lance Shekau dans une vidéo d'une quarantaine de minutes, diffusée sur Youtube. Mais je suis heureux, en bonne santé et en sécurité. Je vais parfaitement bien. » **Il montre un calendrier islamique à la fin de son apparition, pointant du doigt une date qui correspond au 25 septembre 2016.**
10- The *Middle East Eye* reports a **leaked telephone conversation** involving **Major General Wael el-Safty** of **Egypt's General Intelligence Directorate** features **el-Safty** calling **Palestinian Authority President Mahmoud Abbas"stupid"** and his movement **Fatah "screwed."**

Middle East / Moyen-Orient

11- The *Saudi Press Agency* reports that **Canada** confirmed on Sunday it has become aware of a **citizen taken hostage in Libya** and is "diligently pursuing all appropriate channels to obtain more information."
12- The *Fars News Agency* reports that Governor General of Semnan Province Mohammad Reza Khabbaz announced that the **Iranian security forces** have recently captured a number of **ISIL agents** in his province.
13- The *Jerusalem Post* reports that Israel's military satellite program, the newest of which – **Ofek 11**, the newest and most advanced satellite is likely to soldier on in space, but with limited lifespan and ability to perform its **high-resolution spy duties**.

Afghanistan/Pakistan

14- The *Pakistan Dawn* reports that the former spokesperson for the **Tehrik-i-Taliban Pakistan (TTP), Azam Tariq**, has been reportedly killed in Afghanistan's Paktika province in air strikes carried out by Afghan and Nato forces.

Australia, New Zealand / Australie, Nouvelle-Zélande

15- On the back of the news on Friday that **IFM and Australian Super have lobbed an unsolicited approach for Ausgrid,** the big question for investment bankers is whether there is another opportunity to trump the domestically-funded $10 billion-plus offer. But the question remains as to what the latest situation means for **bankers who were recently in Canada to court prospective suitors for the asset**. The *Australian* writes that last year, **David Irvine,** a former director general of the **Australian Secret Intelligence Service — said to be highly vigilant on matters that may threaten national security — was appointed to FIRB.** The all-Australian offer comes as the risks surrounding Foreign Investment Review Board approval for **Chinese bidders and other foreign parties are perceived to be increasingly challenging.**

16- The *Australian Broadcasting Corporation* writes that **Australia's foreign spy agency** chief says **Islamic extremism in South-East Asia**, particularly in the southern **Philippines**, is a **growing national security concern**. Nick Warner, the head of the **Australian Secret Intelligence Service (ASIS),** is the only agency chief to have spoken publicly in its 60 years of operation. "In Australia's backyard in South-East Asia there are now ISIL affiliates — in Indonesia , in the southern Philippines," he told a panel discussion in Washington, using another term for the **Islamic State (IS) group**.

Asia / Asie

17- The *Bangladesh Sangbad Sangstha* reports that Law Minister Anisul Huq today said extradition of Father of the Nation Bangabandhu Sheikh Mujibur Rahman's convicted killer **Noor Chowdhury** was possible as discussion for his return was underway with **Canadian authorities**.

18- The PLA Air Force said on Sunday it had **conducted a drill involving long-range operations** over the **Western Pacific**, past the Miyako Strait, to test far-offshore combat and assault capabilities. **Shen Jinke**, a spokesman for the air force, said regular drills in the Western Pacific and patrols over the **East China Sea air defense identification zone were aimed at protecting China's sovereignty and national security**. According to a statement on the Ministry of National Defense's website, more than 40 aircraft including H-6K bombers, Su-30 fighters and aerial tankers of the **People's Liberation Army** completed exercises such as assaults on sea-surface targets and in-air refueling. The fleet also conducted a routine patrol in the East China Sea air defense identification zone, established in November 2013, writes the *China Daily*.

19- According to the *Global Times*, a man who claimed to be a member of the Islamic State (IS) jihadist group in an **attempt to increase his following on social media** has been detained by the police in South China's Guangdong Province, local media reported Saturday. The 25-year-old man surnamed Zhong will be detained by local police in Tangjia, Guangdong for five days for **"fabricating false facts and spreading rumors online"** in defiance of the Public Security Administration Punishments Law, said the Guangzhou-based news portal ycwb.com. Zhong was taken in for questioning by police after the city's department of public security on September 12 found that he had identified himself on the Tieba online forum as a member of IS, an Islamist group that has seized control of parts of Iraq and Syria and claimed responsibility for terror attacks around the world, said the report.

20- *The Hindu* reports that the **terror attack** at an Army camp in Kashmir's Uri district is only the latest in the long line of attacks on India's western border since the BJP led NDA government came to power. Since May 2014, there have been **23 fidayeen (suicide) attacks** along the Pakistan border, most of them in Jammu and Kashmir.

Americas / Amériques

21- **Ecuador** has expressed **optimism** that the **Julian Assange saga** is coming to an **end** reports *The Times of London.*

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Thursday, September 29 2016
le jeudi 29 septembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- Un **jeune Montréalais soupçonné d'être allé en Syrie et d'adhérer à des idéologies « extrémistes islamistes** » a **réussi à conserver son permis d'armes à feu** pendant des années et à s'acheter légalement des carabines semi-automatiques, alors qu'il **faisait l'objet d'une enquête antiterroriste de la GRC**, souligne *La Presse+* dans une **série de reportages**. Le dossier de **Samy Nefkha-Bahri** soulève de nombreuses questions sur les mesures de contrôle des armes à feu au Canada et sur la communication entre les corps policiers. Un des reportages souligne brièvement que : « **L'Équipe intégrée de la sécurité nationale pilotée par la GRC** mène les enquêtes liées au terrorisme. Le **Service canadien du renseignement de sécurité** (SCRS) ne fait pas d'enquêtes criminelles, mais collecte de l'information pour le gouvernement sur les menaces à la sécurité nationale. »

2- According to *The Canadian Press*, the NDP is calling on the Liberal government to **immediately rescind a directive that allows security agencies to use information that may have been obtained through torture**. The Liberals _ who opposed the ministerial directive while in opposition _ say it will be reviewed as part of a sweeping examination of national security policy. "The input of all Canadians, including all members of Parliament, is most welcome," said **Scott Bardsley**, a spokesman for Public Safety Minister **Ralph Goodale**. The New Democrats want the directive repealed now. Information obtained under torture is not reliable _ and therefore the practice does not ensure the safety of Canadians, NDP public safety critic **Matthew Dube** said Wednesday. The policy applies to the **Canadian Security Intelligence Service**, the **RCMP**, the **Canada Border Services Agency**, the **Communications Security Establishment** and **National Defence**.

Canada

3- At first glance, nothing stands out about the picture. A photograph like the thousands of others seen on social media, showing the prime minister smiling in the company of a voter. What's different is that the man posing beside **Justin Trudeau** is not just an average voter, notes a front-page *Toronto Star* report (written by *La Presse* reporters **Gabrielle Duchaine and Vincent Larouche**). He is the **subject of an RCMP investigation**, suspected of **having participated along with other Quebecers in the kidnapping of two American journalists in Syria in 2013**, an incident believed to have been orchestrated by the **al-Nusra Front**, a group linked to Al Qaeda. Despite this, he was able to get close enough to Trudeau for long enough to take a selfie with the prime minister. *La Presse* has chosen **not to name the suspect, because it is not possible at this stage in the investigation to confirm his level of involvement in events that occurred in Syria.** The young resident of a suburb south of Montreal has not been charged with any crime. He travelled to Turkey for several months in 2012 and 2013, but there is no proof that he crossed the border into Syria.

International

United States / États-Unis

4- Appearing on *CNN,* CIA director **John Brennan** said despite the government's best efforts, the **likelihood of terrorist activity** in the **United States is strong**. "So I think we have to assume **there's something here in the states,**" Brennan said. "We have to be **relentless** in terms of going after them." He added **"it's impossible to say"** whether **Isis** has **operatives or cells** in the **United States**, and he credited the "tremendous advances in **information sharing** and **interaction** between federal officials" in making it difficult for terrorists to operate in the country.
5- FBI director **James Comey** informed a congressional committee yesterday that **hackers** have attempted **more intrusions** into **voter registration databases** since those revealed this summer reports the *Washington Post.* Earlier in the week Homeland Security Secretary **Jeh Johnson** disclosed **18 states have asked for help** in **improving** their **election-systems cyber-security.**
6- **U.S. officials,** reports the *Wall Street Journal,* are **increasingly confident** that the hacker **'Guccifer 2.0'** is part of a **network of individuals** and **groups** kept at **arm's length by Russia** to **mask its involvement** in cyber intrusions such as the theft of thousands of Democratic Party documents. While the **hacker denies** working on behalf of the Russian government, U.S. officials and independent security experts say the syndicate is one of the most striking elements of what looks like an intensifying Russian campaign to target prominent U.S. athletes, party officials and military leaders.
7- *NBC News* reports the **hack** of more than a **half billion Yahoo email accounts** was **motivated by espionage,** not profit, according to an analysis by the **independent cyber-security firm InfoArmor** which contends that an **Eastern European state-sponsored actor** appears to have **ordered the massive hack** as part of a **coordinated effort** to infiltrate the **email accounts** of **U.S. military, diplomatic** and **political figures.**

United Kingdom / Royaume-Uni

Europe

8- De **nombreuses chaînes de télévisions auraient reçu ces derniers jours un courrier de la part du ministère de l'Intérieur leur demandant de différer de quelques minutes leurs émissions en direct afin d'assurer une éventuelle coupure en cas d'attaques terroristes,** rapportent nos confrères de Europe 1, citant la société de production Endemol. Une **information démentie** quelques minutes plus tard par le ministère de l'Intérieur selon *Le Figaro.*
9- D'après *Le Figaro et l'Agence France-Presse,* une **ressortissante allemande enlevée fin 2015 en Syrie et son bébé né lors de cette captivité ont été libérés hier**, a-t-on appris aujourd'hui auprès du gouvernement allemand, une libération confirmée par un groupe djihadiste. Ils ont été libérés hier "et sont entrés en Turquie", a indiqué à l'AFP une porte-parole du ministère allemande des Affaires étrangères.
10- The case of whether **Edward Snowden** can **travel to Norway** to accept an award **without fear** of **extradition** to the **United States** appears headed to the **Supreme Court** reports *The Local,* after an **Oslo Appeals Court upheld** a **lower court ruling** which **backed** the **Norwegian justice ministry's position** that **no guarantees on extradition** could be given before a request had been formally received.

Africa / Afrique

11- Selon *Liberté,* (Algérie), **six personnes, âgées entre 22 et 45 ans, activant dans un réseau de soutien aux terroristes, ont été écrouées, hier, par le juge d'instruction près le tribunal de Collo, en Algérie,** pour constitution d'un **réseau de soutien et de financement de groupes terroristes armés et propagande du terrorisme.**
12- **Amnesty International**, reports *The Times of London,* has accused the **Sudanese government** of using **chemical weapons to kill civilians** including babies and children, leaving hundreds of survivors with "horrific" symptoms. **Sudan's foreign minister, Ibrahim Ghandour,**

in a meeting with the *New York Times* editorial board on Tuesday, dismissed the allegations as **"nonsense."**

Middle East / Moyen-Orient

13- The *Gulf News* reports that Shaikh Abdullah Bin Zayed Al Nahyan, Minister of Foreign Affairs and International Cooperation, met on Tuesday with **Justin Trudeau, Prime Minister of Canada**. The meeting reviewed cooperation between the UAE and Canada and ways of boosting them, as well as ways to encourage investments.
14- The *Fars News Agency* reports that Secretary of Iran's Expediency Council (EC) Mohsen Rezayee disclosed that the country's **security forces have captured a number of ISIL terrorists** who plotted to carry out **suicide attacks** at the University of Tehran.

Afghanistan/Pakistan

15- *The International News* reports that **Pakistan's intelligence establishment** has got the information that **RAW** has been tasked by the Modi government to execute covert strikes against Pakistan that includes terrorist activity, targeting of ISI or MI offices and assassination of Hafiz Saeed and Masood Azhar.
16- *Pajhwok Afghan News* reports that the **National Directorate of Security (NDS)** on Wednesday claiming preventing 11 American power generators from being smuggled to Pakistan.

Australia, New Zealand / Australie, Nouvelle-Zélande

17- Some **110 Australians are fighting with terror group Islamic State** but the federal government expects a **much smaller number will seek to return home**, writes the *Australian Associated Press*. Justice Minister **Michael Keenan** said there was a good chance a significant number would be killed in fighting for Mosul and Raqqa, some dual nationals have lost their Australian citizenship while others won't want to return. "We will make sure that anybody who returns from the conflict zone doesn't pose a threat to the Australian community. **We are not going to allow them to threaten our safety**," he told reporters in Canberra on Thursday.

Asia / Asie

18- China **"means what it says"** when it says it will **consider countermeasures against the planned U.S. deployment of an advanced anti-missile system in South Korea,** the defense ministry said on Thursday. China, North Korea's neighbor and lone major ally, has repeatedly expressed anger at the United States and South Korea for their decision to **deploy the U.S. Terminal High Altitude Area Defence (THAAD)** system in the South to counter missile and nuclear threats from North Korea. The South Korean defense ministry said it would announce a new location for the system on Friday, after opposition from residents for the initial site choice, reports *Reuters*.
19- *The Hindu* reports that **India** has carried out **surgical strikes targeting "launch pads" for terrorists** across the Line of Control (LoC), the Army said on Thursday.

Americas / Amériques

20- **Peru's former spy chief Vladimiro Montesinos** has been sentenced to **22 years in jail,** reports the *Guardian* (UK), for the **forced 1993 disappearance** of **two students** and a **university professor**, whose bodies were burned in the basement of the country's intelligence agency.
21- With Colombians preparing to vote on the FARC peace pact on Sunday, **President Santos** has suggested **talks** with the **ELN** could start as early as **next week** if the rebels agree to **release hostages** reports *teleSUR*. For its part, the ELN announced it's **ready to talk** adds *Reuters*.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Friday, September 30, 2016
le vendredi 30 septembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1-The *Toronto Star Online* writes that the civilian watchdog committee that oversees **Canada's spy agency is giving a cautious thumbs-up to CSIS for its exercise of newly acquired anti-terror powers under Bill C-51,** the controversial law passed last year that the Liberal government says it will amend. **Pierre Blais**, chair of the **Security Intelligence Review Committee (SIRC),** said in an interview that **CSIS appears to have used in a responsible manner its warranted and unwarranted powers of threat disruption and information-sharing**. Under Bill C-51, passed by the previous Conservative government in 2015, the **Canadian Security Intelligence Service (CSIS)** was given wide-ranging ability to disrupt or reduce threats to Canada's national security, inside or outside Canada. **SIRC's recommendations are non-binding.** Yet **CSIS director Michel Coulombe** issued a written statement saying **CSIS is acting to strengthen its rules around such information gathering. (Moderate coverage/couverture modérée)**

2-The worries about a suspect in a **terror investigation** seen **posing for a selfie last year with the prime minister go far beyond the anxiety of how he got that close**. A joint *CBC News/Radio-Canada* investigation has learned that the man is one of at least four **Quebec men of interest to the RCMP for their alleged connection to the 2012 kidnappings of two Americans in Syria**. CBC has been in contact with two of the men, who are going about their lives in Quebec. **Sources have indicated that the other two may be overseas, possibly in Syria or Turkey. CBC has repeatedly asked CSIS and the RCMP about the travels and status of the men. Both agencies have declined to provide details.**

3-Un **journaliste américain kidnappé et torturé en Syrie en 2013 a été troublé hier en voyant un des suspects ciblés par la police dans son dossier prendre librement un égoportrait avec le premier ministre Justin Trudeau.** Troublé, mais pas surpris. **Matthew Schrier croit depuis longtemps que les autorités canadiennes ne prennent pas assez au sérieux les crimes dont il a été victime.** Surveillance des combattants à l'étranger Le ministère de la Sécurité publique soutient qu'il a les outils pour traiter des cas de Canadiens de retour au pays après avoir pris part à des activités de groupes terroristes. « Le gouvernement dispose d'un certain **nombre d'outils pour faire face aux combattants à l'étranger, dont la révocation de passeports, le Programme de protection des passagers et des accusations possibles. Comme l'a souligné le directeur du SCRS [Service canadien du renseignement de sécurité], le nombre total de Canadiens à l'étranger impliqués dans des activités liées à la menace [terroriste] est d'environ 180,** avec environ 60 présumés combattants qui sont retournés au Canada rapporte *La Presse+*.

Canada

4-In a **front-page report**, the *Toronto Star* points out that a **young Montreal man suspected of having gone to Syria and adhering to "extremist Islamist" ideologies** was able to keep his firearms licence for years and to legally purchase semi-automatic rifles while he was the subject of a terrorism investigation by the **RCMP**, a *La Presse* investigation has found.

International

United States / États-Unis

5-**U.S. intelligence officials** disclosed to *NBC News* there is now **"no doubt"** the **Russian government** is trying to **influence November's presidential election.** The American intelligence community has determined **Moscow** is **behind** the **leaks** of **Democratic National Committee emails to Wikileaks** and others — and that the goal is to **undermine confidence** in the November 8 ballot. *NBC* has also learned from a **Department of Homeland Security** source that there have been **hacking attempts** on the **election systems** of **more than 20 states**, far more than the two that have been publicly acknowledged.

6-*Yahoo News'* Michael Isikoff reports an analysis by the **Department** of the **Director of National Intelligence** says the **Russian government** is conducting a **wide-ranging** and **"opportunistic" campaign** to **expand** its **political influence** in **Europe** by deploying **internet "trolls** and other **cyber actors"** to **challenge pro-Western journalists** and **spread pro-Kremlin messages** in **social media forums.** According to the DNI report, **two state-owned media outlets *Sputnik*** and ***RT* promote Russia's political aims** with programming targeted to "activist" audiences including "far-right and far-left elements of European society." It adds that the *RT* channel gives "disproportionate coverage and airtime to the European Parliament's more extreme factions."

7-The **FBI** envisioned **infiltrating mosques** and **Muslim student associations** to look for **young Yemenis** to serve as **informants**, according to an internal presentation obtained by *The Intercept.*

8-A study by the **Justice Department's Inspector General's office** has concluded the **FBI's use** of the surveillance statute, **Section 215** of the **Patriot Act,** enabling it to **collect Americans' phone** and **email records,** has **declined** since details about the program were **leaked** by **Edward Snowden** in 2013 reports the *Washington Times.*

United Kingdom / Royaume-Uni

9-In conversation with the *BBC World Service,* **Firas Abi Ali, a senior analyst for IHS Country Risk,** predicted **Isis** will be **defeated militarily** by **late 2017.**

Africa / Afrique

10-**Algeria** announced yesterday its military **killed five armed Islamist militants** and **seized weapons, munitions** and **food supplies** in an ongoing operation in the **forests of Tazoult** in Batna province, east of Algiers reports *Reuters.*

Middle East / Moyen-Orient

11-The *Lebanon Daily Star* reports that **Montreal Mayor Denis Coderre** advocated for closer ties between **Lebanon and Canada** Thursday on the sidelines of an international mayors' conference.

12-The *Times of Israel* reports that the **Shin Bet** will be specifically responsible for providing personal protection to "more than 60 people from Israel and the rest of the world, including 20 presidents, 15 foreign ministers, five heads of state and VIPs from various countries that are coming to represent their nations at the funeral," the agency said.

13-*The National (UAE)* reports that one of the leading figures of **Al Qaeda in the Araban Peninsula (AQAP)** surrendered to Yemeni security forces on Thursday morning. Aden police spokesman Abdurrahman Al Naqeeb said **Taher Tammah** gave himself up to security forces in the southern province of Lahj.

Afghanistan/Pakistan

14-The *Pakistan Dawn* reports that an **Indian soldier has been captured by the Pakistan army,** while Indian soldiers have also been killed in the episode of firing across the Line of Control, it emerged Thursday.

15-*Pajhwok Afghan News* reports that the **Ministry of Defence (MoD)** on Thursday said yesterday's drone strike in the Achin district of eastern Nangarhar province was carried out on Islamic State or Daesh centres based on **intelligence information**.

Europe

16-Selon *Le Soir,* les **opérateurs européens sont contre un fichier d'enregistrement des voyageurs.** Le « passenger name record » belge incluant les trains internationaux devrait être évoqué en Commission Terrorisme à la mi-octobre. La Deutsche Bahn menacerait de supprimer des ICE vers la Belgique si ce texte est adopté. L'une des mesures prévues par le fédéral dans son programme de lutte contre le terrorisme est la **création d'un registre des passagers, pour confronter leurs noms à ceux qui se trouvent dans différentes bases de données de personnes recherchées**. Mais la particularité du projet belge est qu'il ne se limite pas aux seuls vols aériens, comme aux Etats-Unis. Le **ministre de l'Intérieur, Jan Jambon (N-VA) souhaite l'étendre aux trois autres modes de transports internationaux qui arrivent en Belgique : les bus, les bateaux et les trains**. Cette perspective fait réagir viscéralement les opérateurs ferroviaires européens.

17-D'après *l'Express,* **l'émission Quotidien, dont l'un des journalistes a pu consulter un procès-verbal de la sous-direction anti-terroriste, met en lumière des incohérences dans les versions officielles données par les autorités.** Course folle du camion, intervention des policiers, échange de tirs... Que s'est-il passé le soir du 14 juillet à Nice? Deux mois et demi après l'attentat sanglant sur la promenade des Anglais, de **nouvelles révélations viendraient contredire les versions avancées par les autorités après l'attaque.** C'est l'émission Quotidien qui, jeudi soir, a mis en lumière ces nouveaux éléments par la voix de **Azzeddine Ahmed-Chaouch.**

18-**Beate Zschäpe**, the **last known surviving member** of the **German neo-Nazi NSU,** accused of a spate of **racist murders** between 2000-2007, broke her silence in a Munich court on Thursday, personally speaking for the first time since the trial against her began in 2013 reports *Deutsche Welle.* In a short statement, 41-year-old Zschäpe told the court that as a young woman in eastern Germany in the aftermath of reunification, she **"indeed identified with nationalist ideology."** Today, however, she said: "I judge people not by their origin and political affiliation but by their behavior...**I regret my own misconduct."**

Australia, New Zealand / Australie, Nouvelle-Zélande

19-A **terrorism expert** says **jihadist fighters who are off the radar are the real risk to New Zealand**. *Radio New Zealand News* reports that a would-be Islamic State fighter, **Amin Mohamad**, was arrested in **2013 while boarding a plane at Brisbane airport bound for Turkey on a trip organised by an IS recruiter.** Because of time already served he will be released next year and will likely be deported to **New Zealand, where he has spent most of his life.**

Asia / Asie

20-The *Times of India* reports that in a stunning reprisal for the Uri terror attack that breached decades of self-imposed restraint, **India conducted "surgical strikes" on seven terrorist "launch pads"** across the Line of Control (LoC) in Pakistan-occupied Kashmir in the early hours of Thursday.

21-The White House **appears to want to stabilise ties with Beijing** in the final months of the Obama -administration, Chinese analysts said yesterday, after a weekend report **that Pentagon chiefs had been barred from publicly using "great power competition" in reference to military challenges from China**. According to the *South China Morning Post*, the analysts said the **US National Security Council's** reported gag order was another sign that Washington intended to ease its tension with Beijing over disputes in the South China Sea. Citing four sources

familiar with a classified directive, the *US' Navy Times*, a weekly publication for US naval personnel and their families, reported on Sunday that the NSC **ordered Pentagon leaders to strike out the phrase "great power competition" and find something less inflammatory**.

Americas / Amériques
Light coverage / couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Wednesday, October 19 2016
le mercredi 19 octobre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- *La Presse+* rapporte qu'un **motard en voie de devenir membre en règle des Hells Angels est au nombre des 800 débardeurs du Port de Montréa. Roger Bishop fils, 46 ans, est sorti de l'anonymat la semaine dernière** lorsqu'il a échangé quelques mots avec un journaliste venu couvrir une perquisition policière dans un centre de conditionnement physique du chemin de Chambly, à Longueuil. « En général, les personnes qui doivent avoir accès aux zones réglementées d'un port désigné au Canada doivent obtenir une habilitation de sécurité qui repose sur un programme rigoureux de vérification des antécédents par **le Service canadien du renseignement de sécurité (SCRS), par la Gendarmerie royale du Canada (GRC)** et, au besoin, par **Immigration, Réfugiés et Citoyenneté Canada », a** réagi Daniel Savoie, de Transports Canada.

Canada

2- Whistleblower. Hero. Traitor. Patriot. These words and more have been used to describe former cybersecurity contractor **Edward Snowden**, who in 2013 copied and distributed thousand of documents to reporters and whose stories of Western intelligence agencies — including Canada's **Communications Security Establishment (CSEC)** — shook the world, points out *IT World Canada.* This morning Snowden told the the annual **SecTor cyber security conference in Toronto** that Prime Minister **Justin Trudeau** want to amend the controversial **Bill C-51** anti-terrorism law and not repeal it because he "is afraid of being attacked for being soft on terrorism." Speaking by video from Russia, where he fled to avoid prosecution by U.S. authorities, **Snowden said the legislation, needs three fixes**: First, a judicial body should have oversight over federal intelligence agencies that has the power to prosecute authorities that have broken the law. Second, because intelligence agencies are trading personal information of citizens "like baseball cards" citizens should be told if the data sharing hasn't led to an arrest for criminal activity. And finally, what Snowden called the criminalization of speech through vague definitions of terrorism should be taken out of C -51.

3- Le **Canada est-il prêt à gérer un retour massif de djihadistes sur son territoire ?** Non, répondent des experts. Pourtant, une **éventuelle chute de Mossoul**, dernier fief du groupe armé État islamique (EI) en Irak, risque de pousser de jeunes Canadiens partis gonfler les rangs de l'EI à tenter de revenir au pays Indique *La Presse+*. « Avec ses pertes militaires quotidiennes ainsi que la perte éventuelle de la ville emblématique de Mossoul, la notoriété de Daech s'effrite, explique **Jocelyn Bélanger,** expert des questions de terrorisme et de radicalisation et professeur adjoint à l'Université de New York à Abou Dhabi.

4- A major investigation by **Winnipeg police** that recovered hundreds of thousands of dollars in stolen property has **raised national security concerns after blank passports were among the items officers found**, the *Winnipeg Free Press* reports. Tuesday, police announced **Project Heavy Metal** identified 20 suspects, including nine arrested in Manitoba, who are facing 140 charges related to a theft ring that operated across Western Canada.

International

United States / États-Unis

5- A survey commissioned by the **Center for Strategic and International Studies** involving **respondents** from **eight countries**. the **United States, France, Britain, Turkey, Egypt, China, India** and **Indonesia**, found that at least **three in four** polled said they **expect a terrorist attack** to **occur within the next year**. Additionally, reports the *Washington Post,* a majority in every country polled, including the United States, overwhelmingly approved all 21 options presented to them — among them, requiring identification cards for citizens and visitors; rigorous screening of immigrants; bans on incendiary religious speech; and monitoring of phone calls, emails and social media.

6- According to a study released by the **Brennan Center for Justice**, reports the *Washington Post,* the **Justice Department** has kept **classified** at least **74 opinions, memos and letters on national security issues,** including **interrogation, detention** and **surveillance**. Also still **classified** are between **25** and **30 significant opinions** issued between **2003** and **2013** by the **Foreign Intelligence Surveillance Court**. "This is an **extensive body of secret law,** which is fundamentally **incompatible with democratic self-governance,**" said **Elizabeth Goitein**, the **co-director** of the **Brennan Center's Liberty and National Security Program**. However, **Office of the Director of National Intelligence spokesman Brian Hale** countered that "in the last several years the government has engaged in an **unprecedented level of transparency regarding its intelligence collection authorities**". Hale said that the transparency includes releasing thousands of pages of documents related to foreign intelligence surveillance on U.S. soil and numerous FISC opinions, including five opinions this year.

7- Speaking at an event in Washington yesterday, NSA director **Michael Rogers**, reports *fed scoop.com.,* said by giving the **Department of Homeland Security rather than NSA**, the **lead** in **defending civilian government networks** and working with the private sector to **protect the nation's vital industries,** the U.S. had **"take[n] our best players off the field"**. Rogers said the decision "was **politically driven** and not policy driven. People were a little nervous about having NSA … dealing directly with them".

United Kingdom / Royaume-Uni

8- A nine month examination of the **government's counter-radicalization Prevent program** led the **Open Society Justice Initiative** to label it **badly flawed, potentially counterproductive** and a risk to the basic rights of young Muslims reports the *Guardian.*

Europe

9- D'après *L'Opinion,* **François Hollande révèle avoir ordonné l'exécution d'au moins quatre terroristes par la DGSE, tout en dévoilant des conversations qui mettent le Grec Tsipras en difficulté.** Services secrets et crise grecque : François Hollande hors limites.Soixante-dix pages du **livre «Un président ne devrait pas dire ça» de Gérard Davet et Fabrice Lhomme (Stock) sont consacrées à la diplomatie et au renseignement.**

10- **Turkish police** this morning **fatally shot** a **suspected Islamic State militant** who was believed to be planning a **suicide bomb attack in Ankara.** The *Associated Press* reports the man was killed in a raid on a ninth-floor apartment on the outskirts of the city after he ignored warnings to surrender and opened fire on police.

11- In **co-operation** with the **FBI, Czech authorities** this morning **arrested** an unidentified **Russian man** wanted in connection with **hacking attacks** on **targets** in the **United States** reports *Reuters.*

12- **EU Security Commissioner Julian King** has warned the **battle for Mosul** may lead to to the **return to Europe** of **violent Islamic State fighters** reports the *Daily Telegraph.* "This is a **very serious threat** and we must be prepared to face it" King said. He added that approximately **2,500 EU nationals** are currently **fighting alongside Isis** and that if even a handful return it would pose a "serious threat that we must prepare ourselves for."

13- Selon *Le Soir,* (Belgique), **quatre personnes ont été inculpées pour participation aux activités d'un groupe terroriste après 15 perquisitions menées mardi matin dans plusieurs villes du nord de la Belgique (Gand, Deinze, Anvers),** a annoncé le parquet fédéral. Parmi les inculpés, certains sont **« suspectés d'avoir voulu recruter des personnes pour qu'elles se rendent en Syrie en vue d'y rejoindre l'Etat islamique »,** souligne le parquet.

Africa / Afrique

14- Selon *All Africa,* les **brigades de lutte antiterroriste sont parvenues à dévoiler un groupe terroriste** qui aurait projeté un attentat contre une **personnalité politique importante,** occupant une haute responsabilité au sein de l'Etat, a annoncé, dimanche, le porte-parole officiel du Tribunal de première instance de **Tunis** et du Pôle judiciaire de lutte antiterroriste, **Sofiène Selliti.**
15- As the Nigerian government negotiates with Boko Haram for the release of 83 of the kidnapped Chibok schoolgirls, the *Associated Press* has been informed by **Pogu Bitrus** of the **Chibok Development Association** that as many as **one-third** of the **students remaining in captivity** appear to be **unwilling to leave their extremist abductors.** Meanwhile, the **government** is **denying** media reports that the **21 girls freed last week** were **exchanged** for **four Boko Haram prisoners.**

Middle East / Moyen-Orient

16- *Agence France-Presse* reports that an **Iranian-American businessman** and his 80-year-old father have been given 10 **years in prison for espionage,** Tehran's prosecutor said on Tuesday, prompting the US to demand their release.
17- *Al Jazeera* reports that **tens of thousands of allied forces** continued their advance on Mosul on Tuesday, but their offensive to retake **ISIL's last major stronghold** in Iraq was slowed down by explosives and booby traps they encountered along the way.

Afghanistan/Pakistan

18- The *Pakistan Dawn* reports that **Intelligence Bureau (IB) Director General Aftab Sultan,** while speaking in the Senate standing committee meeting on Tuesday, said a large number of terrorists arrested during the last three years had connections with and were working for the **Indian and Afghan intelligence agencies.**
19- Depending on the Taliban source, secret peace talks with the Afghan government were held in Qatar or they weren't but one Taliban official told *Reuters* that in any event, "like our previous meetings, it was a **waste of time** and resources, as we **could not achieve anything".**

Australia, New Zealand / Australie, Nouvelle-Zélande

20- **Reclaim Australia** says it has never condoned violence but national intelligence bosses say **radical anti-Islamic groups are a growing threat** to Australia's security. **ASIO** director-general **Duncan Lewis** said Reclaim Australia, in particular, **was of interest to intelligence agencies.** Authorities **charged a member of the right-wing group under federal terror laws for the first time in August for allegedly collecting or making documents to prepare for terrorist acts.** Mr Lewis said Reclaim Australia has **"offered violence"** in the past and expects they will continue to when they confront pro-Islamic groups. **"To the extent that there is a possibility of violence, or there is indeed violence being offered, that is of interest to us. That is business for ASIO,"** he told a Senate committee late on Tuesday night. But Reclaim Australia said it does not condone violence. **"Reclaim has never condoned violence and we never will. Reclaim has worked closely with police at past events to ensure public safety,"** a statement provided to the *Australian Associated Press* said.
21- Up to **70 children of Australians** have been **exposed to extremist groups in the battlefields of Syria or Iraq,** the country's security chief has revealed. **Duncan Lewis,** director-general of the **Australian Security Intelligence Organisation,** said these children either travelled to the

conflict zones with their Australian parents or were born there. He told a **Senate committee** late on Tuesday night that **ASIO is investigating around 190 people in Australia who are actively supporting groups like IS through recruiting, fundraising or wanting to join themselves,** reports the *Australian Associated Press.*

22- According to *The Australian*, the highest-ranking terrorist Australia has produced is now a -jihadi without a group, "**resigning**" to "**pursue a number of projects independently**". In a corporate-sounding statement released on his official **Twitter** and **Facebook** accounts, it is claimed former Sydney man **Mostafa Mahamed**, better known as **Abu Sulayman**, resigned from the al-Qa'ida-backed Syrian group **Jabhat Fateh al-Sham** this month. The "resignation" follows his group claiming to have severed ties to al-Qa'ida in July, and being heavily targeted by Russian and Syrian bombardments in the ravaged city of Aleppo.

Asia / Asie

23- In the three months since a band of **youths tortured and killed 20 hostages in a Dhaka restaurant, Bangladeshi intelligence officials say they're rooting out radicals and restoring security to the streets**, reports *Agence France-Presse.* The report points out that the The government continued to deny any IS role even after an August raid killed three suspected militants, including a **Canadian man of Bangladeshi origin** identified on an Islamic State website as the extremist Sunni group's representative in Bangladesh.

24- North Korea on Wednesday threatened to destroy Seoul and the South Korean presidential office if there is **any sign of pre-emptive strikes** by the **United States** and the South against Pyongyang. *Rodong Sinmun*, the North's main newspaper, said that the **country will strengthen its nuclear capabilities in quantity and quality in response to what it called its enemies' scheme for aggression**. "We have warned that South Korea will be engulfed in a sea of fire and the U.S. military units in the Pacific region and the mainland will be in chaos if the U.S. wages nuclear strikes against us," the newspaper said. "Our warning is not an empty word." North Korea has further ratcheted up war rhetoric since speculation has spawned that the U.S. may consider pre-emptive strikes against the North over Pyongyang's nuclear and missile programs, the *Yonhap News Agency* reports.

25- The *Times of India* reports that **Pakistan-based terror group Laskar-e-Taiba** has issued a warning to the Baramulla SHO for facilitating an operation on Monday in which at lease 44 have been arrested for **terror-related activities**.

Americas / Amériques

26- In the spirit of **neutrality** in the **U.S. presidential election, Ecuador** has **confirmed** it has **"temporarily" restricted access** to the **internet** within its **London Embassy, cutting off Julian Assange.** WikiLeaks has released emails and other material connected to the Clinton campaign. Ecuador's action, experts inside and outside the United States government said, is **not likely to slow the flow of leaked emails.** Those emails are routed through servers around the globe. (Extensive coverage / vaste couverture).

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Wednesday, October 19 2016
le mercredi 19 octobre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- *La Presse+* rapporte qu'un **motard en voie de devenir membre en règle des Hells Angels est au nombre des 800 débardeurs du Port de Montréa. Roger Bishop fils, 46 ans, est sorti de l'anonymat la semaine dernière** lorsqu'il a échangé quelques mots avec un journaliste venu couvrir une perquisition policière dans un centre de conditionnement physique du chemin de Chambly, à Longueuil. « En général, les personnes qui doivent avoir accès aux zones réglementées d'un port désigné au Canada doivent obtenir une habilitation de sécurité qui repose sur un programme rigoureux de vérification des antécédents par **le Service canadien du renseignement de sécurité (SCRS), par la Gendarmerie royale du Canada (GRC)** et, au besoin, par **Immigration, Réfugiés et Citoyenneté Canada », a** réagi Daniel Savoie, de Transports Canada.

Canada

2- Whistleblower. Hero. Traitor. Patriot. These words and more have been used to describe former cybersecurity contractor **Edward Snowden**, who in 2013 copied and distributed thousand of documents to reporters and whose stories of Western intelligence agencies — including Canada's **Communications Security Establishment (CSEC)** — shook the world, points out *IT World Canada.* This morning Snowden told the the annual **SecTor cyber security conference in Toronto** that Prime Minister **Justin Trudeau** want to amend the controversial **Bill C-51** anti-terrorism law and not repeal it because he "is afraid of being attacked for being soft on terrorism." Speaking by video from Russia, where he fled to avoid prosecution by U.S. authorities, **Snowden said the legislation, needs three fixes**: First, a judicial body should have oversight over federal intelligence agencies that has the power to prosecute authorities that have broken the law. Second, because intelligence agencies are trading personal information of citizens "like baseball cards" citizens should be told if the data sharing hasn't led to an arrest for criminal activity. And finally, what Snowden called the criminalization of speech through vague definitions of terrorism should be taken out of C -51.

3- Le **Canada est-il prêt à gérer un retour massif de djihadistes sur son territoire ?** Non, répondent des experts. Pourtant, une **éventuelle chute de Mossoul**, dernier fief du groupe armé État islamique (EI) en Irak, risque de pousser de jeunes Canadiens partis gonfler les rangs de l'EI à tenter de revenir au pays Indique *La Presse+*. « Avec ses pertes militaires quotidiennes ainsi que la perte éventuelle de la ville emblématique de Mossoul, la notoriété de Daech s'effrite, explique **Jocelyn Bélanger,** expert des questions de terrorisme et de radicalisation et professeur adjoint à l'Université de New York à Abou Dhabi.

4- A major investigation by **Winnipeg police** that recovered hundreds of thousands of dollars in stolen property has **raised national security concerns after blank passports were among the items officers found**, the *Winnipeg Free Press* reports. Tuesday, police announced **Project Heavy Metal** identified 20 suspects, including nine arrested in Manitoba, who are facing 140 charges related to a theft ring that operated across Western Canada.

International

United States / États-Unis

5- A survey commissioned by the **Center for Strategic and International Studies** involving **respondents** from **eight countries**. the **United States, France, Britain, Turkey, Egypt, China, India** and **Indonesia**, found that at least **three in four** polled said they **expect a terrorist attack** to **occur within the next year**. Additionally, reports the *Washington Post,* a majority in every country polled, including the United States, overwhelmingly approved all 21 options presented to them — among them, requiring identification cards for citizens and visitors; rigorous screening of immigrants; bans on incendiary religious speech; and monitoring of phone calls, emails and social media.

6- According to a study released by the **Brennan Center for Justice**, reports the *Washington Post,* the **Justice Department** has kept **classified** at least **74 opinions, memos and letters on national security issues,** including **interrogation, detention** and **surveillance**. Also still **classified** are between **25** and **30 significant opinions** issued between **2003** and **2013** by the **Foreign Intelligence Surveillance Court**. "This is an **extensive body of secret law,** which is fundamentally **incompatible with democratic self-governance,**" said **Elizabeth Goitein**, the **co-director** of the **Brennan Center's Liberty and National Security Program**. However, **Office of the Director of National Intelligence spokesman Brian Hale** countered that "in the last several years the government has engaged in an **unprecedented level of transparency regarding its intelligence collection authorities**". Hale said that the transparency includes releasing thousands of pages of documents related to foreign intelligence surveillance on U.S. soil and numerous FISC opinions, including five opinions this year.

7- Speaking at an event in Washington yesterday, NSA director **Michael Rogers**, reports *fed scoop.com.,* said by giving the **Department of Homeland Security rather than NSA**, the **lead** in **defending civilian government networks** and working with the private sector to **protect the nation's vital industries,** the U.S. had **"take[n] our best players off the field"**. Rogers said the decision "was **politically driven** and not policy driven. People were a little nervous about having NSA … dealing directly with them".

United Kingdom / Royaume-Uni

8- A nine month examination of the **government's counter-radicalization Prevent program** led the **Open Society Justice Initiative** to label it **badly flawed, potentially counterproductive** and a risk to the basic rights of young Muslims reports the *Guardian.*

Europe

9- D'après *L'Opinion,* **François Hollande révèle avoir ordonné l'exécution d'au moins quatre terroristes par la DGSE, tout en dévoilant des conversations qui mettent le Grec Tsipras en difficulté.** Services secrets et crise grecque : François Hollande hors limites.Soixante-dix pages du **livre «Un président ne devrait pas dire ça» de Gérard Davet et Fabrice Lhomme (Stock) sont consacrées à la diplomatie et au renseignement.**

10- **Turkish police** this morning **fatally shot** a **suspected Islamic State militant** who was believed to be planning a **suicide bomb attack in Ankara.** The *Associated Press* reports the man was killed in a raid on a ninth-floor apartment on the outskirts of the city after he ignored warnings to surrender and opened fire on police.

11- In **co-operation** with the **FBI, Czech authorities** this morning **arrested** an unidentified **Russian man** wanted in connection with **hacking attacks** on **targets** in the **United States** reports *Reuters.*

12- **EU Security Commissioner Julian King** has warned the **battle for Mosul** may lead to to the **return to Europe** of **violent Islamic State fighters** reports the *Daily Telegraph.* "This is a **very serious threat** and we must be prepared to face it" King said. He added that approximately **2,500 EU nationals** are currently **fighting alongside Isis** and that if even a handful return it would pose a "serious threat that we must prepare ourselves for."

13- Selon *Le Soir,* (Belgique), **quatre personnes ont été inculpées pour participation aux activités d'un groupe terroriste après 15 perquisitions menées mardi matin dans plusieurs villes du nord de la Belgique (Gand, Deinze, Anvers),** a annoncé le parquet fédéral. Parmi les inculpés, certains sont **« suspectés d'avoir voulu recruter des personnes pour qu'elles se rendent en Syrie en vue d'y rejoindre l'Etat islamique »,** souligne le parquet.

Africa / Afrique

14- Selon *All Africa,* les **brigades de lutte antiterroriste sont parvenues à dévoiler un groupe terroriste** qui aurait projeté un attentat contre une **personnalité politique importante,** occupant une haute responsabilité au sein de l'Etat, a annoncé, dimanche, le porte-parole officiel du Tribunal de première instance de **Tunis** et du Pôle judiciaire de lutte antiterroriste, **Sofiène Selliti.**
15- As the Nigerian government negotiates with Boko Haram for the release of 83 of the kidnapped Chibok schoolgirls, the *Associated Press* has been informed by **Pogu Bitrus** of the **Chibok Development Association** that as many as **one-third** of the **students remaining in captivity** appear to be **unwilling to leave their extremist abductors.** Meanwhile, the **government** is **denying** media reports that the **21 girls freed last week** were **exchanged** for **four Boko Haram prisoners.**

Middle East / Moyen-Orient

16- *Agence France-Presse* reports that an **Iranian-American businessman** and his 80-year-old father have been given 10 **years in prison for espionage,** Tehran's prosecutor said on Tuesday, prompting the US to demand their release.
17- *Al Jazeera* reports that **tens of thousands of allied forces** continued their advance on Mosul on Tuesday, but their offensive to retake **ISIL's last major stronghold** in Iraq was slowed down by explosives and booby traps they encountered along the way.

Afghanistan/Pakistan

18- The *Pakistan Dawn* reports that **Intelligence Bureau (IB) Director General Aftab Sultan,** while speaking in the Senate standing committee meeting on Tuesday, said a large number of terrorists arrested during the last three years had connections with and were working for the **Indian and Afghan intelligence agencies.**
19- Depending on the Taliban source, secret peace talks with the Afghan government were held in Qatar or they weren't but one Taliban official told *Reuters* that in any event, "like our previous meetings, it was a **waste of time** and resources, as we **could not achieve anything".**

Australia, New Zealand / Australie, Nouvelle-Zélande

20- **Reclaim Australia** says it has never condoned violence but national intelligence bosses say **radical anti-Islamic groups are a growing threat** to Australia's security. **ASIO** director-general **Duncan Lewis** said Reclaim Australia, in particular, **was of interest to intelligence agencies.** Authorities **charged a member of the right-wing group under federal terror laws for the first time in August for allegedly collecting or making documents to prepare for terrorist acts.** Mr Lewis said Reclaim Australia has **"offered violence"** in the past and expects they will continue to when they confront pro-Islamic groups. **"To the extent that there is a possibility of violence, or there is indeed violence being offered, that is of interest to us. That is business for ASIO,"** he told a Senate committee late on Tuesday night. But Reclaim Australia said it does not condone violence. **"Reclaim has never condoned violence and we never will. Reclaim has worked closely with police at past events to ensure public safety,"** a statement provided to the *Australian Associated Press* said.
21- Up to **70 children of Australians** have been **exposed to extremist groups in the battlefields of Syria or Iraq,** the country's security chief has revealed. **Duncan Lewis,** director-general of the **Australian Security Intelligence Organisation,** said these children either travelled to the

conflict zones with their Australian parents or were born there. He told a **Senate committee** late on Tuesday night that **ASIO is investigating around 190 people in Australia who are actively supporting groups like IS through recruiting, fundraising or wanting to join themselves,** reports the *Australian Associated Press.*
22- According to *The Australian*, the highest-ranking terrorist Australia has produced is now a -jihadi without a group, "**resigning**" to "**pursue a number of projects independently**". In a corporate-sounding statement released on his official **Twitter** and **Facebook** accounts, it is claimed former Sydney man **Mostafa Mahamed**, better known as **Abu Sulayman**, resigned from the al-Qa'ida-backed Syrian group **Jabhat Fateh al-Sham** this month. The "resignation" follows his group claiming to have severed ties to al-Qa'ida in July, and being heavily targeted by Russian and Syrian bombardments in the ravaged city of Aleppo.

Asia / Asie

23- In the three months since a band of **youths tortured and killed 20 hostages in a Dhaka restaurant, Bangladeshi intelligence officials say they're rooting out radicals and restoring security to the streets**, reports *Agence France-Presse.* The report points out that the The government continued to deny any IS role even after an August raid killed three suspected militants, including a **Canadian man of Bangladeshi origin** identified on an Islamic State website as the extremist Sunni group's representative in Bangladesh.
24- North Korea on Wednesday threatened to destroy Seoul and the South Korean presidential office if there is **any sign of pre-emptive strikes** by the **United States** and the South against Pyongyang. *Rodong Sinmun*, the North's main newspaper, said that the **country will strengthen its nuclear capabilities in quantity and quality in response to what it called its enemies' scheme for aggression**. "We have warned that South Korea will be engulfed in a sea of fire and the U.S. military units in the Pacific region and the mainland will be in chaos if the U.S. wages nuclear strikes against us," the newspaper said. "Our warning is not an empty word." North Korea has further ratcheted up war rhetoric since speculation has spawned that the U.S. may consider pre-emptive strikes against the North over Pyongyang's nuclear and missile programs, the *Yonhap News Agency* reports.
25- The *Times of India* reports that **Pakistan-based terror group Laskar-e-Taiba** has issued a warning to the Baramulla SHO for facilitating an operation on Monday in which at lease 44 have been arrested for **terror-related activities**.

Americas / Amériques

26- In the spirit of **neutrality** in the **U.S. presidential election, Ecuador** has **confirmed** it has **"temporarily" restricted access** to the **internet** within its **London Embassy, cutting off Julian Assange.** WikiLeaks has released emails and other material connected to the Clinton campaign. Ecuador's action, experts inside and outside the United States government said, is **not likely to slow the flow of leaked emails.** Those emails are routed through servers around the globe. (Extensive coverage / vaste couverture).

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Thursday, October 20 2016
le jeudi 20 octobre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

Light coverage / couverture légère.

Canada

1- Le **rôle des grandes villes** ne se limite plus à entretenir les rues et à ramasser les ordures, mais aussi à **jouer un rôle diplomatique sur la scène internationale**, selon le maire **Denis Coderre**, souligne *La Prese+*. Critiqué à la suite d'un **récent voyage à Téhéran**, en Iran, le premier magistrat de Montréal s'est défendu en disant profiter de ses déplacements pour « passer des messages », sans préciser les messages qu'il avait passés ni à qui il l'avait fait. « Chaque fois que je me promène, que ce soit à Téhéran [en Iran], à Beyrouth [au Liban] ou à Jérusalem [en Israël] au mois de novembre, autant sur le plan du développement économique, du développement social que du développement durable, on passe des messages. Si on veut faire partie de ceux qui vont faire partie de la solution, on n'a pas à jouer la chaise vide non plus », a-t-il dit hier matin.

International

United States / États-Unis

2- *New York Times* reports that **National Security Agency contractor Hal Martin** had **in his possession top-secret NSA hacking tools** that two months ago were **offered for sale** on the **internet** but so far investigators have been **frustrated** in their attempt to **prove that Martin deliberately leaked** or **sold the hacking tools** or, alternatively, that someone hacked into his computer or otherwise took them without his knowledge. While they have found some forensic clues that he **might be the source,** the **evidence is not conclusive**. In interviews with the *Times,* officials described how the **Martin case** has **deeply shaken** the **secret world of intelligence**. They expressed **astonishment** that he managed to **take home** such a vast collection of classified material over **at least 16 years**, undetected by security officers at his workplaces, including the NSA, the Office of the Director of National Intelligence and Pentagon offices and they are **deeply concerned** that some of the mountain of material may, by whatever route, **have reached hackers** or **hostile intelligence services.**

3- Amid accusations that it scanned customer emails at the behest of the NSA or FBI, **Yahoo** has sent a **letter** to Director of National Intelligence **James Clapper demanding American intelligence reveal** how they **monitor online services.** (Extensive coverage / vaste couverture).

United Kingdom / Royaume-Uni

4- **Belgian jihadi 'Rashid'** told *The Independent's* Kim Sengupta that **Isis** is **"really afraid** of the **foreign spies who are among them"**, naming **British intelligence** as the **most successful infiltrator.**

5- The *Guardian* has learned the **Muslim Council of Britain** plans to establish **its own anti-radicalization program** in a direct challenge to the government's Prevent program.

6- **Paul Chichester,** the **director of operations** at **Britain's new National Cyber Security Center**, told an event in London that **hacking intrusions** were on their way to becoming **more**

"destructive, disruptive and **coercive"** reports the *Associated Press.* **"That will be our future,"** he said. Chichester was **seconded** by **Air Force Lt. Gen. James K. McLaughlin, deputy commander** at **U.S. Cyber Command,** who said **infrastructure-wrecking attacks** were being **seen "right now in the environment."**

Europe

7- **One police officer** was **killed** and **three wounded** Wednesday after a **man opened fire on them** during the serving of a warrant in the **Bavarian community of Georgensgmünd** reports *Deutsche Welle.* Authorities said the **49-year-old suspect,** who was slightly wounded in the altercation, is a **member** of the **far right "Reichsbürger" movement**, which translates as **"Citizens of the Reich." Berlin's state intelligence service** described the movement in a recent report as "an **extremely diverse range of small groups and individuals** who believe in an ideological mixture of **conspiracy theories, anti-Semitic and anti-democratic views,** and who have been **behaving increasingly aggressively** for some time."

8- Selon *Midi Libre,* le **CAT vient de décrypter le financement des attentats de Paris**. En ce mois d'octobre 2016, le centre d'analyse du terrorisme (CAT) vient de dévoiler son nouveau rapport sur le financement des attentats de Paris. Celui-ci **décrypte avec minutie la façon dont les terroristes se sont procuré des moyens financiers, pointe les failles dans le système qui leur ont permis de passer inaperçus et fait des propositions pour tenter d'améliorer les choses**. Cartes prépayées, commerce illicite, anonymat, fraude documentaire et manquements dans le partage d'informations sont notamment ciblés dans les problèmes à régler. Le tout est consultable sur le site internet du centre, où sont rendus publics tous les travaux.

9- **Investigators across Europe**, reports the *Wall Street Journal,* are **alarmed** by the **rise of militants** who they suspect have developed a way to **utilize chat apps** and other **social media tools** to **"remote control" attacks from far away**. That is blurring the lines between assaults carried out by militants trained in Islamic State territory and those by so-called lone wolves who authorities assumed were acting without the direction or support of terror groups. "What worries us is a new type of attacker who only appears to be acting alone," said **Hans-Georg Maassen, head of Germany's BfV**. "Such assailants are being steered virtually from abroad via instant messaging."

10- Selon *Le Soir,* (Belgique), un **nouveau dispositif de sécurité combinant technologie et contrôle humain sera bientôt mis en place à l'aéroport de Zaventem en Belgique**. Dernière trace des attentats du 22 mars (hormis la stèle commémorative qui a pris place à l'intérieur du bâtiment), les tentes plantées devant le hall des départs et destinées au pre-screening des passagers de l'aéroport de Zaventem vont prochainement disparaître.

Africa / Afrique

11- Selon *African Manager,* (Tunisie), **une cellule terroriste composée de quatre éléments a été démantelée** à la cité Khaled Ibn Al Walid, à Douara Hicher, gouvernorat de la Manouba, a annoncé, mercredi, le ministère de l'Intérieur de la Tunisie.

Middle East / Moyen-Orient

12- *The National (UAE)* reports that desperate to slow the advance of **Iraqi troops towards Mosul**, ISIL on Wednesday deployed **suicide bombers** and fired mortar shells a day after the Pentagon warned that trapped civilians were being used as human shields.

13- The *Jerusalem Post* reports that security forces have arrested an **Arab-Israeli couple** accused of joining the terrorist group Islamic State in Iraq, the **Shin Bet (Israel Security Agency)** announced Thursday.

14- *Naharnet Newsdesk* reports that **Russian warships** off the coast of Norway are carrying fighter-bombers that are likely to reinforce a final assault on the besieged Syrian city of Aleppo in two weeks, a senior NATO diplomat said Wednesday, citing **Western intelligence**.

Afghanistan/Pakistan

15- *Pajhwok Afghan News* reports that **two Americans were killed and another three were wounded** when a gunman in Afghan military uniform opened fire at a base in Kabul, the NATO-led coalition said on Wednesday.

Australia, New Zealand / Australie, Nouvelle-Zélande

16- The task of being an intelligence chief has become tougher with the rise of cyber threats and terrorism, according to the former head of the **Australian Security Intelligence Organisation, David Irvine**, who says he would like to see a **"much stronger" national cyber industry**. The *Sydney Morning Herald* reports that speaking during a rare interview in Canberra, Mr Irvine said "when you put cyber on top of [terrorism], it takes a bit of time off your sleep at night. The two issues have grown exponentially within a couple of decades and while the nature of the threats is the same, the vector has changed. **And cyber is a new and very potent vector."** Mr Irvine, who led Australia's overseas spy agency ASIS before he headed up ASIO, said he'd been "horrified" at the revelations of **Edward Snowden**, the subcontractor to the **National Security Agency** who exposed vast top- secret US government programs for monitoring global communications.
17- An **Australian living in Yemen was kidnapped** at the weekend, raising concerns he may have fallen into the hands of **Islamist militants**. The unnamed man was kidnapped near the capital, Sanaa, in an area believed to be under the control of **Houthi rebels**, a Shia insurgency that has taken control of tracts of the country. It is not clear who is holding the man, or why he was taken. Sources contacted by *The Australian* said while there was concern the man may have fallen into the hands of a terrorist group, it was just as likely his kidnapping was part of a criminal enterprise.

Asia / Asie

18- The *Times of India* reports that **Islamic State "operative" Subahani Haja Moideen's** account that he was allowed to leave IS-held territory due to a knee injury that ruled him out of active fighting is likely to be closely scrutinised by the National Investigation Agency that is looking at the possibility of his being tasked with setting up a **"sleeper cell"**.
19- According to the *Yonhap News Agendy*, South Korea's foreign ministry issued a **strong condemnation of North Korea's latest missile launch** on Thursday, which it said would only worsen the communist regime's isolation from the international community. The U.S. Strategic Command said N**orth Korea fired off what is presumed to be a mid-range Musudan missile from the northwestern city of Kusong**. The latest missile test-launch came less than a week after the regime unsuccessfully tested another Musudan missile on Oct. 15. The **Thursday launch came in defiance of warnings issued by the UNSC's press statement that was adopted right after the previous test-firing**, the foreign ministry said. It added, **"the latest provocation highlights North Korea's manic obsession with nuclear and missile development."**
20- The *South China Morning Post* is reporting that, a Hague ruling on the **South China Sea** was just a "piece of paper" and the case would "take the back seat" in talks with President **Xi Jinping** today, Philippine President **Rodrigo Duterte** said in Beijing yesterday. Officials said the two sides were expected to sign nearly 20 memoranda of understanding - mostly on economic cooperation - and shore up other **joint efforts against drugs and terrorism**. Duterte arrived in Beijing on Tuesday with a huge business delegation to pave the way for what he calls a new commercial alliance, amid deteriorating ties with long-time ally the United States.

Americas / Amériques

21- *NBC News* reports that **'quiet pressure; from** the **U.S. government** played a role in **Ecuador's decision** to **block** WikiLeaks founder **Julian Assange** from **using the internet** at Ecuador's London embassy. "It was a bit of an eviction notice," said a senior American intelligence official.
22- Stung by accusations that it **installed "back doors"** for the **American government** to **access customers' communications, Microsoft,** reports *Reuters,* has **opened a center in Brazil** where officials will be able to **inspect its programming code** in an attempt to **allay suspicions** in the region that its **software programs** are **vulnerable to spying.**

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Thursday, October 27, 2016
le jeudi 27 octobre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

Light coverage / couverture légère.

Canada

1-Foreseeing a possible "**flood of foreign fighters**" from **Syria**, the **RCMP** has circulated a strategy that **involves trying to understand the returning fighters' intentions and working with communities**, the *National Post* reports. The plan calls for monitoring the **social media activity of the returnees**, placing **them on the no-fly list** and asking **Passport Canada to revoke their travel documents and flag their future passport applications**. The RCMP has also compiled a list of indicators to ascertain the "future posture" of returning fighters that includes whether they are employed, married, "raising funds linked to a little-known charity" or "proselytizing." As an example of the dangers posed by returnees, an unreleased draft of **Public Safety Canada's 2016 annual threat report cited Hiva Alizadeh**, a **Canadian who attended a training camp in Afghanistan.**

2-La **Gendarmerie royale du Canada (GRC) a lancé un guide de prévention du terrorisme et de la radicalisation** menant à la violence, destiné aux parents, aux enseignants et aux proches des personnes à risque. Le guide, intitulé **«Guide de sensibilisation au terrorisme et à l'extrémisme violent»,** vise à les aider à mieux comprendre et à reconnaître le phénomène de la **radicalisation**. «Il n'existe aucun profil type du terroriste», prévient-on d'emblée. Mais pour identifier les personnes à risque, il énonce, entre autres choses, les signes avant-coureurs de radicalisation et ceux de la planification d'un attentat. Il discute également du rôle de l'internet et de la propagande rapporte *La Presse canadienne.*

3-D'après *La Presse+,* l'intensification des **combats contre le groupe armé État islamique dans la région de Mossoul, en Irak, pourrait avoir un impact au Canada** en mobilisant certains partisans du groupe, prévient la **Gendarmerie royale du Canada (GRC).** Celle-ci demande aux citoyens de demeurer «vigilants», tout en se gardant d'« être paranoïaques». «La ville va être libérée, des gens fuient, et ils vont aller quelque part. Sans être paranoïaques, on doit être conscients de cette menace», souligne la surintendante **Martine Fontaine,** responsable de la prévention au Québec pour le corps policier fédéral.

International

United States / États-Unis

4-According to a forthcoming report, now in draft form, to be issued by the **U.S.-China Economic and Security Review Commission** and viewed by the *Washington Free Beacon,* **Chinese spies** have **repeatedly infiltrated U.S. national security agencies,** including official email accounts, and **stole U.S. secrets on Pentagon war plans** for a future conflict with China. "The **United States** faces a **large and growing threat** to its **national security** from **Chinese intelligence collection operations,"** the draft report reads.

5-Speaking to the British edition of the *International Business Times,* **former NSA deputy-director John Inglis** said despite the controversy surrounding the Agency since the Snowden leaks, he's confident the **"NSA is in the right place** and I think **history will judge that it was in**

the right place" but conceding that "it will also judge that it **wasn't transparent enough** about what it was doing."

United Kingdom / Royaume-Uni

6-The **Home Office**, reports the *Guardian,* has disclosed that **six extremists** or **terror suspects** are now subject to **terror prevention and investigation measures** (Tpims) which include being **relocated** from their home towns or cities. **Five** of the six are **British.**
7-Testifying before the House of Lords EU Committee, senior **Metropolitan Police Assistant Deputy-Commissioner Helen Ball** said **access to information** in **Europe-wide security databases**, including the **European Arrest Warrant,** is **"mission critical"** in **fighting terrorism** reports *The Independent.*

Africa / Afrique

8-In an effort to **close an intelligence 'blind spot'** in **northern Africa**, the **United States**, reports the *Washington Post,* has secretly **expanded its global network of drone bases** in the region, deploying unmanned aircraft and U.S. military personnel to a facility in **Tunisia** to conduct **spy missions** in neighboring **Libya.**
9-A group **loyal** to **Islamic State** has **seized** the **small port town** of **Qandala** in **Somalia's** semi-autonomous **Puntland region,** the **first town** it has **taken** since emerging a year ago. *Reuters* reports the group is **led** by **Abdiqadir Mumin**, a **former al Shabaab commander.**
10-**Two American brothers** from **Michigan**, 32-year-old **Nathan Wells Lawwliss** and **Patrick Alan Lawwliss**, 31, have been **arrested in Tunisia** on suspicion of **involvement** with a **terrorist organization** reports the *Daily Beast* and the *New York Times.* Nathan has claimed on Facebook to be the Islamic Messiah and his site also features an Isis flag.
11-Selon *La Nouvelle Tribune,* (Maroc), sur la **liste noire de l'ONU des jihadistes les plus dangereux, le Français Kevin Guiavarch, soupçonné d'être un recruteur très actif du groupe EI, a quitté la Syrie pour rejoindre la Turquie où il est incarcéré.** Deux de ses quatre femmes, parties avec lui, **viennent d'être transférées en France et mises en examen. Kevin Guiavarch, 23 ans, avait rejoint la Syrie fin 2012, d'abord dans les rangs du Front Al-Nosra, la branche syrienne d'Al-Qaïda, avant d'intégrer l'organisation Etat Islamique (EI).**Outre ses activités de recruteur, il est aussi soupçonné d'avoir été directement impliqué aussi dans le **financement de l'organisation**. Le jeune homme, qui dit être « repenti », avait écrit aux autorités françaises disant qu'il voulait rentrer en France, puis avait traversé en juin la frontière turco-syrienne avec ses quatre compagnes françaises et leurs six enfants avant d'être interpellé en Turquie où il est écroué dans l'attente d'un procès.

Middle East / Moyen-Orient

12-*Press TV* reports that **Iran's elite Revolutionary Guards** said on Wednesday they had developed a **"suicide drone"** capable of delivering explosives to blow up targets at sea and on land.
13-*Now Lebanon* reports that a recently-formed group with ties to **ruling Kurdish authorities in northern Syria** has touted that it will soon launch attacks against Turkish forces backing **Free Syrian Army factions**.

Afghanistan/Pakistan

14-The *Pakistan Dawn* reports that Pakistan on Wednesday conveyed to the United States that **India's Research and Analysis Wing (RAW) and Afghanistan's National Directorate of Security (NDS)** are patronising terrorists groups to attack soft targets in the country.

15-*Pajhwok Afghan News* reports that **US forces** carried out precision strikes in eastern Kunar Province this week, targeting **Faruq al-Qatani and Bilal al-Utabi, Al-Qaeda's most senior leaders in Afghanistan**, the Pentagon said.

Europe

16-The **German** media reports that **four Ku Klux Klan cells** are **currently active** in the country.
17-Selon *Le Soir,* (Belgique), la **Belgique a sous-estimé l'intérêt de la lutte contre le financement du terrorisme. Au-delà des sommes en jeu, ces données financières auraient pu faire avancer bien des enquêtes.** Près d'un an après les attentats de Paris, l'Institut Egmont publie une évaluation des mesures préventives et répressives prises en matière de lutte contre le terrorisme depuis les attentats de Charlie Hebdo par sept experts issus du monde académique. Un **rapport assez sévère pour le gouvernement Michel** et dont Le Soir a pu prendre connaissance. L'un des volets du **rapport pointe l'inertie dont a fait preuve la Belgique en matière de lutte contre le financement du terrorisme** alors que « la quête de l'argent est vitale pour les terroristes », souligne **France Lemeunier**, coauteure du rapport.

Australia, New Zealand / Australie, Nouvelle-Zélande

18-**Australia's Reserve Bank** is fighting a **war against cyber security threats**, with potential hackers **testing the resilience of its systems every two seconds**, according to the central bank's technology chief. **Sarv Girn**, chief information officer at the RBA, told delegates at the Gartner Symposium on the Gold Coast that the central bank was withstanding a barrage of potential attacks, the *Australian* reveals.
19-The *Australian* writes that one of Southeast Asia's most notorious militants and a mastermind of the 2002 Bali bombing, **Hambali**, will remain behind bars in **Guantanamo Bay** after US - officials rejected his appeal for release, ruling he still posed a "**significant threat to the security of the United States**". Both **Indonesia** and **Malaysia** opposed Hambali's release. Malaysia warned he could still have strong influence over the remnants of **Jemaah Islamiah** — the terror group behind the Bali attack, which killed 202 people including **88 Australians** — and could even spur a resurgence of JI militancy in Malaysia.

Asia / Asie

20-The *BDNews24* reports that **Bangladesh has urged Canada to devise an 'effective mechanism'** to move forward with the deportation of Nur Chowdhury, the killer of its independence architect.
21-The *Times of India* reports that a **Pakistan High Commission official** has been asked to leave the country, as he was involved in **spying**, Delhi police said.
22-South Korea plans to **reopen talks on an intelligence-sharing pact with Japan** in more than four years, Seoul's Defense Ministry said Thursday, seeking to **boost security cooperation** amid a thaw following their settlement over the sex slavery issue. The envisioned General Security of Military Information Agreement will be the first ever bilateral military accord between the two countries, designed to fac**ilitate the exchange of intelligence and data on North Korea**, as well as search and rescue missions, reports *the Korea Herald.*
23-The government is stepping up efforts to recover billions of yuan in assets **illegally transferred overseas** by corrupt officials via **money laundering platforms** and underground banks. Statistics provided by the **Central Commission for Discipline Inspection**, the nation's top anti-graft watchdog, show that from 2014 to July, the police confiscated illicit assets sent overseas worth 7.62 billion yuan ($1.14 billion). Last month, during Premier **Li Keqiang's** official visit to **Canada**, the two countries signed a bilateral agreement to share illegally transferred assets, a move that is being seen as a milestone in China's program to recover misappropriated funds and assets. Similar agreements are now under negotiation with the United States, Australia and France, reports the *China Daily.*

Americas / Amériques

24-**Hundreds of thousands** of **Venezuelans** dressed in white and chanting **"This government will fall!"** poured onto the **streets of Caracas and other cities** on Wednesday to **demand** a **referendum** to **oust President Nicolás Maduro** reports the *New York Times*. The protests were sparked by a **ruling** by **Venezuela's Electoral Council** to **suspend the process** for **organizing a recall referendum.** "This is a **dangerous new phase,**" said **David Smilde,** a scholar of Venezuela at Tulane University and a senior fellow at the Washington Office on Latin America.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Thursday, November 3 2016
le jeudi 3 novembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- D'après *La Presse+,* alors que la SQ et la Ville de Montréal ont confirmé avoir mis des journalistes sous surveillance, la **GRC et le Service canadien du renseignement de sécurité (SCRS), les deux corps policiers fédéraux, ne veulent pas confirmer s'ils ont déjà adopté de telles pratiques, et le cas échéant à quelle fréquence. La GRC précise seulement que «les cas où des enquêtes de la GRC concernant des journalistes ont eu lieu sont extrêmement rares». Le commissaire de la GRC Bob Paulson a dit mercredi «ne pas être au courant que nous avons des enquêtes actives ou de la surveillance à l'égard de journalistes»**, mais la GRC n'a pas voulu confirmer si des journalistes ont été surveillés dans le cadre de ses enquêtes. Un cas de filature avait été rendu public il y a un an, celui du journaliste de La Presse **Joël-Denis Bellavance** qui a été pris en filature en 2007.
2- *Le Devoir* rapporte que le **ministre de la Sécurité publique ordonne une enquête administrative En lieu et place de l'" affaire Lagacé "**, il faudra désormais traiter du scandale de la surveillance des journalistes : la Sûreté du Québec a confirmé mercredi qu'elle avait, tout comme la police de Montréal, traqué des reporters au cours des dernières années dans le cadre d'une enquête, suscitant une nouvelle vague d'inquiétudes et de dénonciations dans l'univers des médias. **Fait inquiétant, ni la Gendarmerie royale du Canada ni le Service canadien du renseignement de sécurité (SCRS) n'ont voulu préciser si des journalistes avaient déjà été, ou se trouvent actuellement sous écoute électronique.**

Canada

3- *La Presse+* rapporte que le lanceur d'alerte américain prenait part à une vidéoconférence organisée par l'Université McGill, hier Les **Canadiens sont très mal protégés contre les pratiques de surveillance abusives, estime Edward Snowden, qui s'alarme des possibilités ouvertes aux services de renseignements d'ici et d'ailleurs par les nouvelles technologies de communication.** L'ex-sous-traitant de la National Security Agency (NSA), qui participait hier à une vidéoconférence organisée par l'Université McGill, a souligné que le **système de régulation des services de renseignement canadiens était probablement le plus « déficient en Occident** ». Il a déploré à ce titre que le gouvernement libéral de **Justin Trudeau tarde à réviser la Loi antiterroriste, dite loi C-51,** qui confère des pouvoirs accrus à ces mêmes services.

International

United States / États-Unis

4- **Current** and **former U.S. intelligence officials** are **predicting** a **months-long campaign** backed by the **Russian government** to **undermine** the **credibility** of the **presidential election** - through hacking, cyber attacks and disinformation campaigns - is **likely** to **peak** on **Tuesday,** when Americans head to the polls reports *Reuters.* **CIA director John Brennan declined** to **comment** on the Russian efforts but he said **Russian intelligence operatives** have a **long history** of **marrying traditional espionage** with **advances in technology**. More broadly, Brennan said the digital age creates enormous opportunities for espionage but it also creates vulnerabilities. **Former CIA director Leon Panetta** said **"don't underestimate what they can do or will do.**

We have to be prepared. In some ways, they are succeeding at disrupting our process. Until they pay a price, they will keep doing it."

United Kingdom / Royaume-Uni

5- The **British government will appeal** a decision by the **High Court** this morning that it **must have parliament's approval before starting** the **process** to **leave** the **European Union** reports the *BBC*. Prime Minister Theresa May had stated she intended to activate Article 50, formally notifying the EU of the UK's intention to leave, by the end of next March.

Europe

6- Selon *L'Obs,* l'enquête sur **l'ex-patron du renseignement révèle que Bernard Squarcini n'a jamais coupé les ponts avec son ancienne maison, tout en travaillant pour LVMH Juste avant d'être présenté aux juges,** Bernard Squarcini a tenté de s'expliquer. « Je suis parti contraint et forcé, a déclaré **l'ex-patron de la DCRI (le renseignement intérieur, devenu la DGSI en 2014). J'ai changé d'activité, mais j'ai gardé un état d'esprit identique** à celui qui m'accompagnait en ma qualité de haut fonctionnaire. » Une défense bien maladroite. Mis en examen fin septembre notamment pour « compromission » et « trafic d'influence », le « Squale » est justement soupçonné d'avoir continué, après son départ, en février 2013, à **se comporter comme un chef du renseignement au mépris de la loi**.

7- **Quatre mosquées de région parisienne ont été fermées par les autorités**. Dans un communiqué, le ministère de l'Intérieur précise que leur fermeture a été décidée sur "le fondement des dispositions de l'article 8 de la loi sur l'état d'urgence permettant la fermeture des lieux de culte au sein desquels sont tenus des **propos constituant une provocation à la haine ou à la violence ou une provocation à la commission d'actes de terrorisme ou faisant l'apologie de tels actes"**. Parmi ces établissements, figurent la mosquée Al-Islah de Villiers-sur-Marne, dans le Val-de-Marne. Fin août, une perquisition avait permis de découvrir qu'elle abritait une école coranique clandestine indique *Atlantico.*

8- Police in **Berlin** have arrested a **27-year-old** as yet unidentified **Syrian refugee** on suspicion of being a **member of Isis** and plotting an **attack** on **one** of the **city's airports** reports *Deutsche Welle.* The man, who has been living in Germany since 2015, was apprehended at his apartment. Authorities have until the end of today to bring the suspect before a judge for a decision on whether they can continue holding him.

9- In an **audio recording** released this morning, **Isis leader Abu Bakr al-Baghdadi** has commanded his followers to **attack Turkey** reports *Daily Sabah.*

10- Interviewed by broadcaster *RT,* **Julian Assange flatly denied** the **Russian government** is **WikiLeak's source** for the trove of **Clinton campaign emails.**

Africa / Afrique

11- D'après *Jeune Afrique,* le **Niger, cible de trois attaques terroristes en dix jours au mois d'octobre** se trouve sous les feux de la rampe et des **jihadistes venus du Nord-Mali**. La sitution au Nord-Mali s'est dégradée. Le Niger a demandé à ce que le **mandat de la Minusma soit plus offensif et permette de faire la guerre.**

Middle East / Moyen-Orient

12- *Agence France Presse* reports that Tehran's notorious former chief prosecutor **Saeed Mortazavi**, whose role in curbing dissent has been condemned by human rights groups for years, has been sentenced to 135 lashes on charges related to a corruption trial. The **Canadian government** accused Mortazavi of direct involvement in the death of **Zahra Kazemi, an Iranian-Canadian photo journalist**.

13- The *Jerusalem Post* reports that **Canadian Governor-General David Johnston**, who arrived in Israel on Tuesday with his wife, Sharon, told President Reuven Rivlin on Wednesday that he

would like to "reaffirm Canada's commitment to work with Israelis, Palestinians and other partners to **uphold the prospects of a two-state solution** and achieve a just and lasting peace."
14- *The National (UAE)* reports that **Iraq's elite counterterrorism troops** became the first Iraqi soldiers to set foot in the northern city since the army ignominiously abandoned Mosul to ISIL in June 2014.

Afghanistan/Pakistan

15- Two Indian diplomats in Islamabad have been caught spying for India's premier spy agency, **Research and Analysis Wing (RAW)**, and may be expelled, sources told *The Express Tribune* on Wednesday.

Australia, New Zealand / Australie, Nouvelle-Zélande

16- According to *ABC News*, Counter-terrorism police allege one **of two people arrested in Sydney raids this morning had links to a member of foreign fighter network**. A Sydney man accused of travelling to Syria to fight alongside Al-Qaeda affiliate **Jabhat al-Nusra** has alleged links to two other men who are also under the watch of counter terrorism police. State and federal police from the **Joint Counter Terrorism Team** have arrested **Mehmet Biber**, 24, and a **17-year old boy** on suspicion of **breaching foreign fighter laws**. Biber was arrested at Birrong this morning over allegations he travelled to Syria to fight alongside Jabhat al-Nusra in July 2013.
17- *Radio New Zealand News* is reporting that the **Inspector-General of Security and Intelligence** has **reviewed an urgent authorisation for warrantless surveillance** and has found **no "material concerns"**. The **SIS** used the **first ever authorisation to respond to a suspected terrorist act in the second half of last year, to carry out surveillance without a warrant for up to 24 hours**. In her annual report, the Inspector General, **Cheryl Gwyn**, says there **were no major problems with the authorisation**. She also says the **Government Communications Security Bureau** has 'self-reported' four completed investigations and seven other possible incidents of non-compliance. Ms Gwyn says none require immediate, urgent action, but all will be followed up.
18- Cabinet ministers have **been told to improve the cyber security of their departments** after it was found **inadequate safeguards risked government agencies** becoming the **"honey pots"** of **secret information** in **cyber espionage**. **Dan Tehan**, the minister assisting Prime Minister **Malcolm Turnbull** on cyber security, will tell his senior colleagues they need to appoint top bureaucrats to be responsible for cyber security after a study by the **Australian National University's National Security College** found **smaller government agencies** and **medium-sized business were the weakest link, or "honey pots"**, in Australia's cybersecurity defences because they are not vigilant enough about "low-level" threats like malware and denial of service attacks. This is despite a $230 million cyber security strategy introduced by Mr Turnbull in April. "This report clearly shows that, when it comes to government agencies, we've still got more work to do," Mr Tehan told *The Australian Financial Review*.

Asia / Asie

19- The *Times of India* reports that **Pakistan** on Wednesday pulled out six employees posted at its high commission in New Delhi, days after India declared one Pakistani official **persona non-grata for espionage activities**.
20- China's **draft cybersecurity law**, which stipulates that **foreign technology firms should store important business data and personal data related to their operation within China**, is aimed at effectively safeguarding State security as well as protecting people's privacy, an expert said. The comment came after *Reuters* reported that short-term rental company **Airbnb** told Chinese users that it will store their **personal data locally "as foreign tech companies operating in China respond to increasing regulatory pressure."** A spokesperson with the Airbnb China confirmed with the *Global Times* on Wednesday on condition of anonymity that its

parent company is moving Chinese mainland-based users' information including the guest bookings in China and Airbnb listings to local servers for greater localization.
21- According to the *China Daily*, China and Kyrgyzstan vowed on Wednesday to **fight terrorism, separatism and extremism through strengthened security cooperation** as Premier **Li Keqiang** paid his first visit to the Central Asian neighbor. In the capital, Bishkek, Li and Kyrgyz Prime Minister **Sooronbay Jeenbekov** signed a joint communique on bilateral cooperation in fields such as security, agriculture and production. The agreement is especially timely since the Chinese embassy in Kyrgyzstan was attacked by a suicide car bomber on the morning of Aug 30. The attack injured three embassy personnel.
22- *Indo-Asian News Service* reports that Kolkata born former Scotiabank's Vice Chairman **Sarabjit Singh Marwah** has become the first Sikh to be appointed to the **Canadian Senate**.

Americas / Amériques

Light coverage / couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Tuesday, November 22 2016
le mardi 22 novembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- La **menace de cyberattaques est de plus en plus présente et les Forces canadiennes veulent mieux y répondre**. *Radio-Canada* a appris qu'à partir de l'année prochaine, un **nouveau corps de métier totalement consacré à la cyberdéfense sera créé au sein de l'armée.** Le risque de cyberattaques a de nouveau été exposé au grand jour la semaine dernière. Même si l'origine du problème demeure inconnue, le site de recrutement des Forces canadiennes a été ciblé jeudi. **L'ancien directeur du Service canadien du renseignement de sécurité (SCRS) Richard Fadden y est favorable, mais croit qu'il faut avoir une discussion nationale sur le sujet** puisque, selon lui, mener des cyberattaques vient avec son lot de risques. Au Canada, il n'y a pas que la **Défense nationale qui est responsable d'assurer la cybersécurité. Le ministère de la Sécurité publique et des agences comme le Centre de la sécurité des télécommunications** ont aussi un rôle important à jouer.

2- Most of the government employees who have seen their **security clearances revoked** for bad behaviour since January 1 work at the **Canada Revenue Agency** and **agencies under the purview of Public Safety Canada** — including the **RCMP**, **Correctional Services Canada** and **CSIS**, *Ipolitics* reports. An order paper question filed by Conservative MP **Jim Eglinski** on October 3 asked the government to **provide a breakdown by department of all employees who have had their security clearances cancelled or revoked,** excluding retiring employees or employees whose terms of employment had ended. It also asked how many of those employees with revoked clearances were terminated as a result and what the reasons for the revocations were. Liberal MP **Kevin Lamoureux**, parliamentary secretary to the Leader of the Government in the House of Commons, submitted the response on November 18. It shows that **48 government employees had their security clearances revoked for bad behaviour,** not including those whose clearances were revoked or cancelled because of retirement or taking another job after receiving a clearance during the recruitment process. The **Canada Revenue Agency** saw the largest number of employees whose "reliability status" was either revoked (12 employees) or administratively cancelled (six employees). While **Public Safety Canada itself hasn't had to revoke or cancel the security clearances** of any department-specific employees, the same can't be said for several agencies that fall under its purview. **Two employees** at the **Canadian Security Intelligence Service (CSIS)** had their security clearances revoked and were terminated as a result. The documents tabled by the government don't give reasons for those revocations. "**For reasons of national security and to protect employee safety, CSIS does not disclose the reasons or rationales as to why security clearances were cancelled or revoked**," the documents say.

Canada

3- La **police de Montréal a lancé un avis de recherche concernant deux suspects après la découverte d'une cartouche de fusil pleine au consulat de France de la métropole québécoise, laissant craindre une menace potentielle à la sécurité**. «Le 18 octobre dernier, une munition d'arme à feu non utilisée a été retrouvée à l'intérieur du bâtiment du Consulat général de France», a indiqué le service de la police de Montréal (SPVM). Une cartouche de fusil de chasse

de calibre 12 aurait été laissée par deux suspects, a indiqué **Jean-Pierre Brabant, porte-parole au SPVM** indiquent *TVA Nouvelles avec l'Agence France-Presse.*

International

United States / États-Unis

4- Speaking to *McClatchy,* **former CIA director Leon Panetta** said **nominee Mike Pompeo** is a **"pretty good choice"** to lead the Agency. "I've had a chance to talk with him during hearings on the Hill," Panetta said. "He's someone who has **very good credentials** and **understands what intel is all about.** He knows what the Agency's responsibilities are. I believe he's interested in doing a good job." **New York congressman Pete King applauded** the selection of Pompeo because he believes the nominee will bring back **"realistic approaches"** like **waterboarding** which King supports.

5- **Four U.S. officials** who spoke to the *Daily Beast* said **fear is pervasive among Muslims** inside the halls of the Pentagon, the **CIA**, and the **Department of Homeland Security** in anticipation of a **Trump administration**. Already, the officials said, they are seeing colleagues who are **less willing to share their thoughts about national security.** They fear they will no longer be seen as an asset to confronting terrorism but rather suspect members of the government they serve.

6- **President-elect Trump** released a **video** on **YouTube** yesterday which dealt primarily with domestic issues reports the *New York Times.* **National security** was **not mentioned** other than Trump saying he would **ask his top military officials** for a **comprehensive plan** to **guard America's vital infrastructure** from **"cyber-attacks**, and all other form of attacks."

7- The **Defence Department,** reports the *Washington Post,* has become the **first U.S. government agency** to launch a policy **enabling researchers** to **report bugs** or **flaws** they discover in its **websites without fear of prosecution.**

United Kingdom / Royaume-Uni

8- **Prime Minister Theresa May** is to **approve plans** for an **elite armed police force** to protect Britain's most **sensitive infrastructure** from a Paris-style terrorist attack reports *The Times of London.*

9- **Donald Trump** has publicly suggested a "very flattered" **Nigel Farage** be **Britain's ambassador** to the **United States** tweeting Farage would "do a great job!" In a terse response, **Downing Street replied** there is **"no vacancy"**. (Extensive coverage / vaste couverture).

Europe

10- *Le Monde* rapporte que la **CNCTR vient de mettre au jour un pan entier des interceptions, celles par voie hertzienne,** qui lui étaient jusqu'ici interdites d'accès C'est une ligne de front invisible pour le grand public, où se parle une langue indigeste. C'est pourtant là que se défendent les **frontières de l'Etat de droit. Après avoir subi quelques revers, la Commission de contrôle des techniques de renseignement (CNCTR) repart à l'offensive,** profitant de la censure, le 21 octobre, par le Conseil constitutionnel, de l'article du code de sécurité intérieure consacré à la surveillance des communications circulant par la voie hertzienne. Dans sa délibération, datée du 10 novembre, adressée au premier ministre, dont Le Monde a eu connaissance, la **CNCTR part à l'assaut d'un champ de surveillance des communications par les services de renseignement français** qui lui était jusque-là interdit.

11- The **U.S. State Department**, citing **"credible information"** that **Isis** and **al Qaeda** are **planning attacks** in **Europe** has issued an **advisory** warning **American travelers** to be cautious about attending **Holiday festivals, events** and **outdoor markets** reports *Newsweek.*

12- According to *Süddeutsche Zeitung*, the **Federal Court of Justice** has ruled **Edward**

Snowden must be **brought** to **Berlin** to **personally answer questions** posed by a **parliamentary committee investigating National Security Agency activities in Germany**. *The Local* points out the **government** has long argued that it could **not guarantee Snowden's safety** if he were to travel to Germany due to the fact he is wanted on charges of espionage and theft of government property in the U.S.
13- Le **ministère de l'intérieur a annoncé l'arrestation à Strasbourg et Marseille de sept personnes, soupçonnées d'avoir planifié des attaques terroristes en France**. C'est un important projet d'attentat, possiblement fait d'attaques simultanées, qui a été «déjoué» suite à une vague d'interpellations à Strasbourg et à Marseille, dans la nuit du samedi 19novembre au dimanche 20novembre. Le ministre de l'intérieur, **Bernard Cazeneuve, l'a annoncé lui-même, lundi 21novembre. Une série d'arrestations qui s'ajoute à d'autres et à la vingtaine d'attentats «déjoués» depuis le début de l'année, selon la place Beauvau, et vient rappeler que des cellules très structurées sont toujours dormantes, en France.** Paris et Marseille étaient visées révèle *Le Monde.*

Africa / Afrique

14- Selon *All Africa,* en Libye, le ministère de l'Intérieur annonce l'arrestation **d'une des épouses de Mokhtar Belmokhtar.** L'une des femmes du chef **du groupe jihadiste al-Mourabitoune,** de nationalité tunisienne, circulé dans une voiture dans la région de Syrte. Son nom vient d'être révélé, par **la Direction générale du comité libyen pour la lutte contre le terrorisme.**

Middle East / Moyen-Orient

15- **Ginella Massa**, who on Friday became the **first Canadian woman** donning the Islamic veil covering the hair known as hijab, told *Al Arabiya* that she hopes this will change "misconceptions" about Muslim women.
16- *The National (UAE)* reports that **Syrian regime forces advanced quickly** in rebel-held areas of Aleppo on Monday, pressing a new offensive in defiance of international concern over the fate of the city and its residents.

Afghanistan/Pakistan

17- *Pajhwok Afghan News* reports that **Pugwash, a Canada-based organization**, is holding a conference in Islamabad tomorrow to discuss Pakistan-Afghanistan relations besides the Afghan government-initiated peace process.

Australia, New Zealand / Australie, Nouvelle-Zélande

18- Authorities will **soon be able to impose control orders on children as young as 14** after controversial **counter-terrorism laws cleared parliament**, reports the *Australian Associated Press*. A bill that included a suite of measures passed the lower house on Tuesday after changes were made in the Senate earlier this month. Aside from reducing from 16 the age a person can be subject to a control order**, the legislation creates a new search, telecommunications interception and surveillance regime for those under the orders.**

Asia / Asie

19- The *Philippine Star* reports that **Abu Sayyaf bandits** are reportedly demanding P500 million in ransom for a German hostage. Sub-commander Alhabsi Misaya disclosed their demand through text messages when they released photographs of Juergen Kantner.
20- The *Press Trust of India* reports that the **NIA** carried out searches at 17 premises of controversial Islamic preacher Zakir Naik, his NGO and a few associates for the third consecutive day on Monday, even as it **blocked the website** of outlawed Islamic Research Foundation founded by him.

21- The **governments of South Korea and Japan** on Tuesday **separately endorsed a pact that allows the sharing of military intelligence** in response to the growing threat posed by North Korea's nuclear and missile programs. South Korea's Defense Ministry said the pact, known as the **General Security of Military Information Agreement**, will be signed at 10 a.m. Wednesday in Seoul. The complete text of the agreement will also be disclosed. According to South Korean government officials, Defense Minister **Han Min Koo** and Japanese Ambassador **Yasumasa Nagamine** will ink the deal at the Defense Ministry. **It will go into effect immediately as it does not require parliamentary ratification**. President Park **Geun Hye**, who is at the **center of an influence-peddling scandal**, was absent from Tuesday's Cabinet meeting where the endorsement was announced, but she endorsed it later in the day, *Kyodo News* reports.

Americas / Amériques

22- Colombian President **Juan Manuel Santos** has announced he is **cancer free** but will take medication and undergo one session of radiotherapy to eliminate any vestiges of a previous bout with the disease reports *Reuters.* **Santos**, who won the Nobel Peace Prize last month for his efforts to end the war, is expected to **sign a new peace document** with **FARC leader Rodrigo Londono** but the **timing** has **not yet been announced.**

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Friday, December 2, 2016
le vendredi 2 décembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

Light coverage / couverture légère.

Canada

1-Le meilleur endroit pour **recruter de jeunes Québécois prêts à partir faire le djihad en Syrie, c'est au centre islamique Assahaba du prédicateur Adil Charkaoui, croit le suspect de terrorisme Ismaël Habib,** dont le procès s'est amorcé cette semaine à Montréal. C'est du moins ce qu'il a confié en février à un agent d'infiltration de la GRC jouant le rôle du patron d'un groupe criminel de passeurs illégaux rapporte *La Presse.*

2-During a three-hour conversation with an undercover officer only days before he was arrested, **Ismael Habib admitted he was willing to do anything necessary to get to Syria and fight for the Islamic State**, the *Montreal Gazette* reprts. Testifying at Habib's trial on Thursday, the **RCMP officer said Habib told him he believed it was his duty to do so, that he lived to die and knew of other young people in Montreal who were ready to leave with him**. Habib was on **Passport Canada's watchlist** and **suspected of terrorist** activities as early as March 2013. He had tried to have a new passport made after his was seized following a trip to Turkey that same year.

International

United States / États-Unis

3-Calling him "the closest thing we have to Gen. George Patton," Donald Trump has nominated 66-year-old retired general **James Mattis** as his **Defence Secretary**. Mattis led the United States Central Command, which oversees military operations in the Middle East and Southwest Asia, from 2010 to 2013. His tour there was cut short by the Obama administration which believed he was **too hawkish on Iran.** But, reports the *New York Times,* his insistence that **Iran is the greatest threat to peace** in the Middle East, as well as his **acerbic criticism** of the **Obama administration's initial efforts** to **combat** the **Islamic State** in **Iraq** and **Syria,** made him an **attractive choice** for the incoming president. However, in some areas his **views differ from Trump**. For instance, he told the President-elect that **torture does not work** and that he believes **Trump's conciliatory statements** toward **Russia** are **ill informed.**

United Kingdom / Royaume-Uni

4-**Britain's independent reviewer of terrorism legislation David Anderson** said in his annual report that the **threat of terrorism remains 'severe',** expressing disquiet about the **ability** of **ports officers** to **defend against terrorist infiltration** due to **poor manifest information** reports *The Times of London.*

Africa / Afrique

5-According to the London-based *The New Arab,* the **Egyptian** and **Syrian governments** have been **co-operating** to send **Egyptian extremists** captured in the war-torn country **back home** to **face prosecution.**

6-Selon *Kapitalis,* (Tunisie), la **garde nationale a arrêté à Kairouan, un terroriste recherché et condamné par contumace à 20 ans de prison**. La police a intercepté **Mohamed Ali B. (36 ans) à son retour de Libye où il était en fuite** depuis plusieurs mois. **Il était membre du groupe terroriste tunisien Ansar Charia, avant de se rendre, en 2013, en Libye, où il s'est entraîné dans des camps de l'organisation terroriste l'Etat islamique (Daech)**. En rentrant en Tunisie, en 2014, il a participé à des attaques terroristes contre les forces sécuritaires, avant de fuir de nouveau en Libye.

Middle East / Moyen-Orient

7-*The National (UAE)* reports that in a **lightning offensive, Syrian government forces** have driven the rebels from about 40 per cent of their territory in eastern Aleppo over the past week.
8-*Al Jazeera* reports that an **English-language news website in Qatar** has raised the issue of **"censorship"** after it was blocked by the country's two Internet service providers simultaneously for reasons unknown.

Afghanistan/Pakistan

9-The *Pakistan Dawn* reports that the **US State Department** on Thursday congratulated Gen Qamar Javed Bajwa on his recent appointment as Chief of Army Staff and said the army chief should be given time to implement **counterterrorism efforts**.
10-*Pajhwok Afghan News* reports that Deputy Chief Executive Officer (CEO) Mohammad Mohaqqiq on Thursday said **Daesh or Islamic State (IS)'s main objective** was to disunite people and take them war against each other.

Europe

11-A report issued by **Europol** this morning warned that the **Islamic State** is **likely** to **carry out an attack** on the EU **member nations** in the **near future** having **"both the will and capability"** to strike at **both hard** and **soft targets**, though **soft targets** are the **strategic choice** given their capacity to frighten the public.
12-In a dispatch from Berlin, the *Daily Beast* identified the 51-year-old **BfV employee arrested** earlier this week on suspicion of preparing a **serious act of violence against** the **state** and an **attempted breach** of **government secrecy,** as **'Roque M'** He told his interrogator that he infiltrated the intelligence agency because it was **"Allah's will."** Indeed, 'M' claimed that there was a **bigger plan for infiltrating the BfV**—one that would continue without him, reportedly warning **"You may have me now, but the plan will go on."** The *Daily Mail* has published pictures of 'M' which shows tattoos of Che Guevara on his torso.
13-*Tass* reports the **FSB** warned on its website this morning that **"foreign special services** are preparing to carry out **massive cyber attacks** starting from December 5 aimed at **destabilizing Russia's financial system"**.
14-**Russia's new foreign policy concept** advocates a **readiness** to **develop ties with Canada** including on the issue of the **Arctic** reports *Sputnik.*
15-Selon *Le Figaro,* **face à la désormais connue « menace terroriste d'une ampleur inédite » que Bernard Cazeneuve juge lui-même « particulièrement complexe à détecter et à prévenir »** , tenaillé par l'ombre portée d'un plausible 11-Septembre à la française que se disputerait un État islamique en perte de vitesse et Al Qaida en quête de légitimité sur la scène terroriste, le **ministère de l'Intérieur s'évertue tant bien à harponner puis vitrifier les islamistes radicaux.** Dans le collimateur? Les **ressortissants étrangers ou les déchus de la nationalité française installés dans le pays pour prêcher la haine, se faire les zélateurs du djihad armé sur les réseaux sociaux ou encore les sergents recruteurs de Daech.**
16-D'après *Sud Ouest avec l'Agence France-Presse,* **l'Office européen de police alerte sur la probabilité de l'utilisation d'explosifs dans des voitures piégées par des terroristes du groupe Etat islamique en Europe.** C'est un mode opératoire maintes fois éprouvé par les

terroristes en Irak ou en Syrie. D'après Europol, l'Office européen de police, les réseaux terroristes tels que le groupe Etat islamique pourraient avoir recours à des voitures piégées pour atteindre leurs cibles en Europe. **"L'utilisation d'engins artisanaux, d'explosifs militaires ou achetés dans le commerce dans des voitures piégées n'a pas encore été employée par le groupe EI en Europe"**, selon un rapport publié à La Haye.

Australia, New Zealand / Australie, Nouvelle-Zélande

Light coverage / couverture légère.

Asia / Asie

17-*Reuters* reports that before **Tamim Ahmed Chowdhury** orchestrated Bangladesh's worst militant attack, he sought and won approval for it from the militant Islamic State (IS) group. A **Canadian of Bangladeshi origin**, he was told by his contact in the militant group, Abu Terek Mohammad Tajuddin Kausar, to target foreigners, according to a senior police official who has seen communications between the two men.

18-*The Manila Times* reports that the **Philippine National Police (PNP)** has placed the entire country under **"terror alert level 3"** following the foiled bomb attack by the Maute Group near the US Embassy.

19-US intelligence whistle-blower **Edward Snowden** has condemned the treatment of **asylum seekers in Hong Kong**, describing it as **"criminal"**. Snowden was sheltered by three groups of asylum seekers when he was in the city for about two weeks in 2013, after he had fled the United States. In an interview with **Canadian news outlet** *Ricochet Media*, he described the poverty, **"discrimination and repression"** suffered by such people in Hong Kong. The former **National Security Agency** contractor criticised the fact that asylum seekers were not allowed to work in the city, saying they were left "hungry and destitute" as they waited for their claims to be processed. When the former CIA contractor was in the city, he applied as an asylum seeker with the UN refugee agency. **"He was given several options and he thought it was in his best interest to leave Hong Kong," Robert Tibbo**, Snowden's lawyer in Hong Kong, told the *South China Morning Post*.

20-South Korea **blacklisted several top aides of North Korean leader Kim Jong-un** on Friday as part of a fresh set of its **unilateral sanctions** aimed at helping curb the defiant neighbor's nuclear and missile programs. According to the *Korea Herald*, the package is also designed to tighten Seoul's squeeze on Pyongyang's financial and maritime networks and reinforce export controls. The announcement followed two days after the **UN Security Council** approved a new resolution in response to Pyongyang's fifth nuclear test in September. **Japan also said Friday it had decided to toughen its own sanctions on the North Korea.**

Americas / Amériques

Light coverage / couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Wednesday, December 14 2016
le mercredi 14 décembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- Les **dirigeants du Service canadien du renseignement de sécurité (SRCS) font volte-face :** après s'être engagés devant un comité du Sénat le mois dernier **à préciser si des journalistes avaient fait l'objet d'une enquête de leur part dans le passé**, ils reviennent sur leur parole dans une réponse écrite qui a été envoyée au sénateur conservateur **Claude Carignan**. Dans leur réponse écrite, les dirigeants du SCRS justifient cette volte-face en affirmant qu'ils pourraient « compromettre l'intégrité des opérations » de l'organisation et « nuire à sa capacité d'exercer le mandat que le Parlement lui a confié » s'ils confirmaient que le SCRS avait déjà eu un journaliste dans sa ligne de mire dans le passé. « Ainsi, le SCRS est au regret de ne pas pouvoir confirmer si des journalistes ont fait l'objet d'une de ses enquêtes, et ce, même si son représentant s'était engagé à donner une réponse spécifique », affirme le SCRS dans sa réponse écrite, obtenue par *La Presse+*. Le journaliste **Joël-Denis Bellavance** rappelle que Durant son témoignage devant le Comité sénatorial permanent de la sécurité nationale et de la défense, le 28 novembre, le directeur adjoint aux opérations du SCRS, **Brian Rumig**, s'était pourtant engagé à préciser aux membres du comité le nombre de journalistes qui auraient été la cible de surveillance directe ou indirecte.

2- Canada's spy agency has backtracked on its promise to reveal to a Senate committee how many Canadian journalists it spied on in the past, citing operational security, reports the *Toronto Star*. The **Canadian Security Intelligence Service** said while it **"appreciates the importance of the question"** to Canadians and the Senate committee on national security and defence, **"we regret that we cannot confirm whether journalists have been the subject of any CSIS investigation."** Conservative Sen. **Claude Carignan** called it a **"bizarre response"** and a **"serious" breach of an undertaking to a parliamentary committee**. He suggested it **implies that surveillance of journalists is either still ongoing or has been recently suspended**. **"How can it harm operations if you don't have any operations ongoing?"** he said in an interview. The statement to the committee said **CSIS recognizes it "has a duty to fulfil its mandate in a manner that upholds Canadian law and values.** However, **we also have a duty to identify and advise government of threats to our national security, and exercise our authorities set out in law to fulfil this mandate.** Any individual engaged in threat-related activities may be subject to this kind of lawful investigation, irrespective of their profession. While CSIS can discuss elements of its relevant policy framework, **we cannot provide information regarding whether anyone may or may not have been the subject of investigation. To do so would compromise the integrity of our operations and jeopardize our ability to fulfil the mandate given CSIS by Parliament."**

Canada

3- According to the *National Post*, an **attack on a mosque in Chakwal, Pakistan**, has led to **calls for an investigation in Canada** over allegations a **Toronto-area man was part of a group** that vowed "**extreme measures**" against the place of worship. A mob of about 1,000 surrounded the mosque belonging to minority **Ahmadiyya Muslims**, according to Pakistani newspapers *The Nation and Dawn*, as well as social media posts, some showing video of the damage. The incident Monday reportedly came after locals filed a petition with police claiming "**infidels" were illegally occupying the building** and unless action was taken "**we will be forced to take**

extreme measures to liberate this mosque." One of the names near the top of the petition was **Haji Malik Rashid Ahmed**, whom Ahmadiyyas say is a **Canadian**. A news website run by the Ahmadiyya community reported he had spoken about the issue at mosques in the Chakwal area. The **Ahmadiyya Muslim Jama'at Canada**, which represents Canadian Ahmadiyya Muslims, raised the issue at a meeting with **Global Affairs Canada**, said **Asif Khan**, the organization's director of public relations.

International

United States / États-Unis

4- **Donald Trump's cabinet picks** and his **campaign rhetoric** have **industry experts** worried that his administration will **increase surveillance** on Americans and **gut** the **regulatory bodies** that **oversee cyber-security** reports *CNBC*. Of **particular concern** said **Corynne McSherry**, legal director at the **Electronic Frontier Foundation**, is **CIA nominee Mike Pompeo** who has **advocated routine mass collection** and use of "social data" from third parties. "The president-elect, his advisors and future Cabinet members appear to see more enemies lurking in the homeland than in Russia or other cyber superpowers," said **David Cowan,** an investor in cyber-security start-ups with **Bessemer Venture Partners**. "I fear that for the **first time,** the **federal government** really does **pose** a **'Big Brother' threat in cyberspace."**

United Kingdom / Royaume-Uni

5- An accusation in the House of Commons by **Labour MP Ben Bradshaw** that **Russian hackers "probably" swayed** the **referendum** in **favor** of **Brexit** was **dismissed** out of hand by **Downing Street** reports *Sky News*.

Europe

6- Three major German media outlets *Süddeutsche Zeitung* and broadcasters *NDR* and *WDR* have reported that **religious groups** from **Saudi Arabia, Kuwait** and **Qatar** have been **increasingly supporting Salafists** in **Germany**, raising **concerns** within both the **BfV** and **BND**. Currently, German intelligence estimates there are **10,000 Salafists** in the country and believe that refugees could also be drawn to the movement. Specifically named as **supporting organizations** are **Society of the Revival of Islamic Heritage** from **Kuwait**, the **Shaykh Eid Charity Foundation** from **Qatar** and the **Muslim World League** from **Saudi Arabia**. The **BND declined** to **confirm the accuracy** of the reports but **Sebastian Sons** of the **German Council on Foreign Relations** believes they're **credible** telling *Deutsche Welle* "it's well known that for decades Saudi Arabia has been launching missionary initiatives throughout the world, both by using private foundations and by sending clergymen abroad. Saudi Arabia wants to present itself as the leader of the Sunni Islamic world."

7- **L'organisation djihadiste possède ses propres unités de renseignement.** Ce sont elles qui ont planifié les attentats menés en France et Belgique en 2015 et en 2016. Enquête sur un corps d'élite toujours menaçant. L'homme, encagoulé et revêtu d'un uniforme camouflé, parle un français sans accent. Derrière lui, dans un décor de ruines, un prisonnier bâillonné est attaché, les bras en croix. La vidéo, diffusée sur Internet le 26 novembre dernier, est censée avoir été tournée à Raqqa, la capitale « régionale » de l'organisation Etat islamique (Daech) en Syrie. **Le djihadiste, surnommé Abou Souleymane al-Firansi (« le Français »), donne une abjecte leçon de meurtre au couteau. Ce vademecum du terrorisme individuel peut être vu comme une réplique à un événement survenu en France, cinq jours plus tôt.** Le 21 novembre, les policiers de la **Direction générale de la sécurité intérieure (DGSI)** ont démantelé une cellule djihadiste qui prévoyait de commettre des tueries dans Paris et en Ile-de- France, le 1er décembre rapporte *L'Express*.

8- Selon *La Dépêche du Midi,* **trois individus, suspectés de vouloir partir faire le jihad en Syrie ont été interpellés très tôt hier matin dans une cité toulousaine par une unité de la Direction générale de sécurité intérieure (DGSI).** Leur interpellation s'est déroulée dans le cadre d'une commission rogatoire délivrée par un magistrat parisien. On ignorait hier soir ce que les perquisitions réalisées dans la foulée de ces arrestations ont permis de découvrir.

Africa / Afrique

9- Through its conduit the *Amaq News Agency,* **Isis** has **claimed responsibility** for Sunday's **suicide bombing** at **Cairo's** main **Coptic cathedral** which **killed 25 people** and wounded four dozen more. **Isis identified** its bomber as **Abu Abdallah al-Masri** which *Reuters* points out is **not** who the **Egyptian government named** as the **perpetrator**. Its culprit is **Mahmoud Shafik Mohammed Mostafa.**

Middle East / Moyen-Orient

10- *Haaretz* reports that **Israel** is undergoing a revolution in identity security in **biometrics** as other countries such as the United States, Australia, **Canada** and soon Britain have passports that include biometric data based on facial data.
11- A **deal** to **evacuate rebel fighters** and **civilians** from **eastern Aleppo** appears to have **stalled** this morning with **heavy shelling** reported in the Syrian city. The *BBC* reports the **breakdown** of the deal, brokered by Russia and Turkey, is being attributed to **demands** from the **Syrian government.** (Extensive coverage / vaste couverture).
12- The *Times of Israel* reports that the **Islamic State** terrorist group accused Israel of conducting **multiple airstrikes** against it in the northern Sinai Peninsula.
13- *Asharq Al-Awsat* reports that **Yemeni security forces** seized a commercial truck carrying **spy drones** on its way to the Houthi rebels, according to a Yemeni military official.
14- The *Fars News Agency* reports that **Iran's President Hassan Rouhani** ordered scientists on Tuesday to start **developing systems for nuclear-powered boats**, in reaction to what he called the United States' violation of a global atomic deal.

Afghanistan/Pakistan

15- *Pajhwok Afghan News* reports that **leading political and jihadi leaders** gathered in Kabul on Tuesday to discuss a peace resolution suggested by Pugwash, an official said. **Pugwash, a Canada-based organisation**, arranges conferences and seminars to seek solution to conflicts in various parts of the world.
16- The *Pakistan Dawn* reports that **Pakistan Navy's special 'Task Force-88' (TF-88)** was established Tuesday for maritime security of Gwadar port and protection of associated sea lanes against both **conventional and non-traditional threats**.

Australia, New Zealand / Australie, Nouvelle-Zélande

17- The US State Department has defended its role in the **Nauru and Manus Island refugee resettlement** deal with Australian Prime Minister **Malcolm Turnbull** and described its **security vetting procedures as "thorough".** It has also **outlined how it will attempt to facilitate the deal** without taking it through the minefield of the US congress. US Senate Judiciary Committee chairman **Charles Grassley** and House of Representatives Judiciary Committee chairman **Bob Goodlatte** have publicly questioned in recent weeks the **State Department** and **Department of Homeland Security's** decision to **keep the deal classified and not consult with congress.** The State Department hit back, **outlining its stance in a letter**, obtained by the *Australian Associated Press,* to Mr Grassley. "The **USRAP continues to implement thorough security vetting procedures for refugees of all nationalities**, and the **United States will not accept any refugees for resettlement,** under this arrangement or otherwise, unless they **pass all required security vetting.**"

18- The New Zealand government **rejected on Tuesday a proposal for industries to police new money-laundering rules themselves,** and will **instead leave one government department in charge of supervising thousands more businesses**. The **Department of Internal Affairs (DIA)** would scrutinize the new professions covered by the rules, including lawyers, real estate agents, accountants and car dealers, according to a proposal released by the **Ministry of Justice** on Tuesday. The new rules will be introduced next year, reports *Reuters*. The **government has come under pressure to tackle money laundering** since the release in April of the **Panama Papers**, which showed how **offshore companies often use New Zealand trusts as a way to create a secretive un-taxed vehicle in the South Pacific nation**. The Ministry of Justice said **"self-regulating bodies"** had **no experience in tackling money-laundering and the financing of terrorism.**

Asia / Asie

19- *Trend News Agency* reports that more than 500 employees of the **Azerbaijani State Security Service** have been dismissed within one year's time frame, **Madat Guliyev**, lieutenant-general, head of the service, told reporters in Baku.

20- The Chinese foreign ministry said on Monday a **Chinese State Councilor** met a **senior adviser** of US President-elect **Donald Trump** as part of **China's efforts to establish connections with Trump**. State Councilor **Yang Jiechi** met **Michael Flynn**, Trump's choice for **national security adviser**, during a recent stopover in New York on his way to Latin America, **Geng Shuang**, a spokesperson for Chinese foreign ministry, told a daily briefing on Monday. The two sides exchanged views on China-US relations and major issues of common interest, said Geng, without mentioning when exactly they met. This is China's attempt to build connections with Trump's team, and paves the way for the next meeting, **Wu Xinbo**, director of the Center for American Studies at Fudan University told the *Global Times* on Tuesday, who declined to say whether the next meeting will involve other top officials from both sides.

21- The *Times of India* reports that **India** is getting ready to test its **Agni-V intercontinental ballistic missile (ICBM)** in its final operational configuration from Wheeler Island off Odisha after two years.

Americas / Amériques

22- The Rupert Murdoch owned website *Heat Street* reported earlier this week that **senior Russian intelligence officers** from **Cuba visited** the **head** of **Ecuadorean intelligence** in Quito, **days before Edward Snowden pilfered classified NSA files.** This, concluded *Heat Street,* 'strongly suggests' that **both Ecuador** and **Russia 'knew in advance'** of Snowden's intentions.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

World News Overview
Aperçu des nouvelles mondiales

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

Thursday, December 15 2016
le jeudi 15 décembre 2016
07:00 / 7h00

CSIS in the News/Le SCRS dans les nouvelles

1- The federal government secretly gave **RCMP security officials the authority to tap telephone calls without court oversight during the Cold War,** newly unearthed archival documents show. According to *The Canadian Press*, the surveillance program, codenamed "**Picnic**," began as an emergency effort during the **Korean War**, but **federal agencies collaborated with telephone companies in 1954** to continue the wiretaps, says **Dennis Molinaro**, who teaches history at Ontario's Trent University. Molinaro's research indicates the RCMP security branch was listening in on the embassies of East Bloc countries, "**certain unfriendly organizations**" and individuals suspected of disloyalty. It has **long been known the Mounties kept an eye on a wide array of people and organizations - from church and gay rights groups to Quebec separatists and Communists - in the name of national security**, amassing hundreds of thousands of dossiers. Mountie scandals in the 1970s led to a royal commission, the **demise of the RCMP security service** and **creation in 1984** of the civilian **Canadian Security Intelligence Service**. Molinaro believes the documentation he has uncovered with the help of tenacious staff at **Library and Archives Canada** helps flesh out **how the RCMP surveillance of Canadians took place** and implicates federal politicians and bureaucrats in making it happen.

Canada

2- A British Columbia man has been **arrested on a terrorism peace bond**, officials said Wednesday, marking the 19th time since last year police have used the **legal tool against suspected extremists**. **Khalid Ahmed Ibrahim** was to appear in provincial court in New Westminster, B.C. on Dec. 20. Police told the court on Dec. 8 there were **reasonable grounds Ibrahim "may" commit a terrorism offense.** He has also been charged with **uttering threats**, court staff said. The threatening charge dates to July 19 and was to return to court Dec. 21. No further details about Ibrahim or the allegations were available. Peace bonds are not a criminal charge but rather impose conditions on the conduct of those subjected to them. Frequently suspects cannot travel, use the Internet or associate with other known extremists for one year. Police have been **increasingly using peace bonds in terrorism cases in an attempt to cut suspected extremists off from ISIL and al-Qaida online propaganda** and prevent them from leaving Canada to join terror groups, writes the *National Post*.

3- Selon *Le Point,* **l'espionnage informatique est l'arme fatale du renseignement, et les Français ne sont pas en reste.** Nous sommes en juin 2012. **Edward Snowden est pour une année encore l'un de ces bons petits soldats de l'ombre, tapi dans une base secrète de la NSA** à Hawaii. A Paris, **Nicolas Sarkozy termine son mandat, quand le chef des services informatiques de l'Elysée, un homme de la DGSE, s'inquiète. Les services de renseignement canadiens En 2009, le Centre de la sécurité des télécommunications du Canada (CSEC) découvre une vaste opération de cyberespionnage baptisée Snowglobe et l'utilisation de Babar, un programme malicieux (maliciel). Le CSEC soupçonne les services secrets français.**

International

United States / États-Unis

4- In conversation with *Sputnik,* the **president** of the Washington-based **Global Policy Institute Paolo von Schirach** said an **intelligence sharing fissure** between **Canada** and the **United States** over a **change in policy** under Donald Trump regarding **torture** is potentially a **"very big deal"** and **"probably damage U.S. security"**.

5- *Bloomberg* reports that **more than 150,000 U.S. government** and **military employees** are among the **victims** of **Yahoo's newly disclosed 2013 data breach** which impacted **one billion accounts worldwide.** The government accounts belong to current and former White House staff, U.S. congressmen and their aides, **FBI agents, officials** at the **National Security Agency**, the **Central Intelligence Agency**, the **Office of the Director of National Intelligence**, and each branch of the U.S. military. The list includes an **FBI division chief** and multiple **special agents** working around the U.S.; current and former diplomats in Pakistan, Syria and South Africa; **a network administrator** at **NSA's Fort Meade headquarters**; the **chief** of an **Air Force intelligence group**; and a **human resources manager** for the **CIA.**

6- **Senior U.S. intelligence officials** have disclosed to *NBC News* that the **intelligence community now believes** with **"a high level of confidence"** that **Vladimir Putin** became **personally involved** in a **covert Russian campaign** to **interfere** in **November's presidential election.** Two senior officials with direct access to the information say **new intelligence** shows that **Putin personally directed** how **hacked material from Democrats was leaked and otherwise used.** The **intelligence** came from **diplomatic sources** and **spies working for U.S. allies. Putin's objectives** were **multifaceted,** a high-level intelligence source said. What **began** as a **"vendetta" against Hillary Clinton** morphed into an effort to **show corruption in American politics** and to **"split off key American allies** by creating the image that **[other countries] couldn't depend** on the **U.S.** to be a **credible global leader** anymore". However, the *Town Hall* website reports that **FBI director James Comey phoned** President-elect **Donald Trump** and told him there was **no credible evidence** to suggest **Russian meddling**. Furthermore, Comey is reported to have informed Trump that **DNI James Clapper agreed** with the **FBI's assessment. CIA director John Brennan did not.**

7- According to **Army records** obtained by the *Washington Post* under the Freedom of Information Act, a **secret U.S. military investigation** in **2010** determined that **Michael Flynn**, the retired Army general tapped to serve as **national security adviser** in the Trump White House, **"inappropriately shared" classified information** with **foreign military officers in Afghanistan.** Although Flynn **lacked authorization** to share the classified material, he was **not disciplined** or **reprimanded** after the **investigation** concluded that he **did not act "knowingly"** and that "there was **no actual** or **potential damage** to **national security** as a result". The *Post* reports **former U.S. officials** familiar with the matter said that **Flynn was accused** of **telling allies** about the **activities** of **other agencies** in **Afghanistan,** including the **CIA.**

8- The **Shadow Brokers**—a **hacker** or group of **hackers** that **stole computer exploits** from the **National Security Agency**—has been quiet for some time but, reports *Vice Magazine's* 'Motherboard', a **newly uncovered website**, which includes a **file apparently signed** with the **Shadow Brokers' cryptographic key**, suggests the group is **trying to sell hacking tools directly** to **buyers one by one,** and a cache of files appears to include **more information on specific exploits.**

United Kingdom / Royaume-Uni

9- Speaking at Royal United Services Institute, **Chief of Defence Staff Sir Stuart Peach** warned **Islamic State** militants are **"moving in migrant flows, hiding in plain sight"** reports *Sky News.*

Europe

10- C'est une idée qui tourne dans les milieux politiques de droite et d'extrême droite depuis plusieurs mois et que le candidat François Fillon a faite sienne. La proposition de loi de **François-Noël Buffet invite à élargir « la notion d'intelligence avec une puissance étrangère pour y inclure l'intelligence avec une organisation terroriste** » et propose de créer « un délit d'allégeance à une organisation prônant la commission d'actes portant atteinte à des ressortissants français ou aux intérêts fondamentaux de la nation française » . La première permet de doper le quantum des peines en matière d'infraction terroriste pour le porter à trente ans. Une telle disposition pourrait être plus efficace dans la lutte contre le terrorisme que « l'association de malfaiteur » rapporte *Le Figaro.*

11- The **Russian government** and the **FSB** announced this morning that planned **terror attacks in Moscow, Crimea** and the **Rostov region** have been **foiled** and the alleged perpetrators arrested reports *Tass* and the *Associated Press.*

Africa / Afrique

12- Selon *Le Journal du Mali,* le **chef d'Al-Mourabitoune, Mokhtar Belmokhtar ne serait pas décédé dans la frappe aérienne menée par la France dans le sud-ouest de la Libye.** C'est ce que l'on a appris des aveux d'un infirmier nigérien, qui aurait soigné le chef djihadiste. Selon, les **services de renseignements algériens** qui collaborent avec les services nigériens, Mokhtar Belmokhtar se serait pas mort dans la frappe aérienne menée par la France en novembre dernier.

13- **Egypt hanged prominent Islamist fighter Adel Habara** this morning days after a top court rejected his final appeal and in defiance of **militant threats** to **ignite "a volcano of jihad"** across the country reports *Reuters.* Habara, 40, was **sentenced to death** in 2014 for **killing 25 army conscripts** in Northern Sinai in August 2013.

Middle East / Moyen-Orient

14- *The National (UAE)* reports that a **deal to evacuate fighters and civilians** trapped in east **Aleppo's** last remaining rebel-held pockets was suspended on Wednesday – just hours after the agreement was hatched.

15- *Haaretz* reports that the **Civil Service Commission** has launched an investigation into suspicions that **Mossad head Yossi Cohen** received free tickets to a concert worth thousands of shekels from Australian billionaire James Packer.

Afghanistan/Pakistan

16- The *Pakistan Dawn* reports that **Pakistan** on Wednesday successfully tested an improved version of the **medium-range and subsonic Babur cruise missile** to bolster the country's deterrence capabilities.

Australia, New Zealand / Australie, Nouvelle-Zélande

17- A report by a group **monitoring coalition air strikes in Iraq and Syria** has given Australia **low marks** for **transparency and accountability**. The UK-based **Airwars organisation** says Australia remains one of the **least transparent members** of the international military coalition, **consistently refusing to disclose almost any information about air strikes by RAAF aircraft or acknowledge any incidents that may have produced civilian casualties**. According to the *Australian Associated Press*, Airwars collates data on air strikes from official reporting and on civilian casualties from media and other reports. It said the US-led coalition, comprising aircraft from 13 countries, had conducted about 14,200 strikes in the first two years of the campaign against the Islamic State group. US aircraft conducted the majority of strikes in Syria and Iraq. Airwars ranked **Canada the most transparent of coalition members**, followed by the UK, US and France.

18- Australian warplanes in Iraq and Syria are **increasingly hitting Islamic State's logistics and finance networks as changes to the rules of engagement** and Australia's war crimes **legislation allows the RAAF to expand the list of targets**. *The Australian* understands **RAAF planes** have been working at a higher tempo in the past few months as the coalition pounds Islamic State targets in Mosul ahead of the final assault to retake the Iraqi city. As calls mount for a humanitarian intervention in Aleppo, which has been decimated by a Russia-backed campaign by Syrian government forces to retake the city, coalition planes are helping Iraqi forces on Mosul.

Asia / Asie

19- Canadian officials visited North Korea and met with **Canadian detainee Hyeon Soo Lim**, who was **sentenced to life in prison** last year over what Pyongyang described as **anti-state activities**, the North's state media said Thursday. A Canadian government delegation led by **Sarah Taylor**, director general for **North Asia and Oceania for Global Affairs Canada**, arrived in North Korea on Tuesday for a three-day visit to discuss Lim's case and other issues, Pyongyang's *Korean Central News Agency* said. The agency said the Canadian officials met Lim, but provided no further details. Lim, a **Christian pastor**, was convicted by Pyongyang's Supreme Court for **trying to use religion to destroy the North Korean system** and helping U.S. and South Korean authorities lure and abduct North Korean citizens. North Korea is often accused of using foreign detainees as a way to win concessions from other countries. The country is locked in a standoff with the international community over its expanding nuclear weapons and missiles program. North Korea is also holding at least **two Americans for alleged espionage, subversion and other charges**. Korean-American **Kim Tong Chol** is serving a 10-year prison term with hard labor, while University of Virginia undergraduate **Otto Warmbier** has received 15 years, reports the *Associated Press*.

20- Foreign organisations including **social and environmental advocacy groups fear they could inadvertently break broadly defined new rules that take effect in China next month**, with some even shutting up shop to avoid such pitfalls. Chinese President **Xi Jinping's** administration has made **sweeping changes to Chinese law** in the name of **boosting national security**, including a **controversial cybersecurity law** passed last month and another **targeting foreign non-governmental organisations (NGO)**, slated for Jan. 1. China says the **NGO law**, which **grants broad powers to police to question NGO workers, monitor their finances and regulate their work**, is necessary to regulate an unruly sector and that only those operating illegally have anything to fear. Western governments say the law, which was passed in April, **treats groups as criminals and would severely limit their ability to operate in China.** Foreign NGO employees in China have told *Reuters* that many groups still do not know whether they will be able to register with the authorities in time as key information about the process has not been published.

21- The *Press Trust of India* reports that **India's requests for extradition of 110 fugitives** are at various stages of execution in various countries, government said today. **Canada** is one country with which India has inked the treaty till date.

22- The *Philippine Star* reports that **China** appears to have constructed **point-defense capabilities** at each of its outposts in seven of the Manila-claimed islands on the Spratly (Kalayaan) Islands in the **South China Sea**.

Americas / Amériques

Light coverage / couverture légère.

For more in-depth coverage of today's news, please consult the daily news summary which is published at 8 a.m.
Pour une couverture plus détaillée des nouvelles du jour, veuillez consulter le sommaire des nouvelles, publié à 8 heures.

BLANK PAGE / PAGE BLANCHE