A-2012-088

12/35-E
2012 04 19

UNCLASSIFIED –
See Handling Instructions

Integrated Terrorism Assessment Centre | Centre intégré d'évaluation du terrorisme

THREAT ASSESSMENT

CANADA: BIANNUAL UPDATE ON TERRORIST AND EXTREMIST THREATS

Objective

1. This biannual update provides an overview of terrorist and extremist threats to Canadians and Canadian interests at home and abroad. Since the last update (ITAC 11/82) was issued on 2011 08 31, the terrorist threat environment has not significantly changed. The intelligence cut-off date for this update is 2012 04 01.

- the most significant threat to Canadians and Canadian interests at home and abroad over the next six months continues to be posed by AQ-inspired terrorists. The threat against the West has diversified as the global jihad is increasingly being driven by violent home-grown extremists and AQ affiliates. Recent jihadist messaging and attack plotting indicate a move away from complex plots or, at minimum, augmenting these plots with smaller-scale attacks against a broader range of targets.

- much of Al Qaeda (AQ) Core's daily attention is now firmly focussed on survival, and that AQ Core is increasingly likely to rely on attacks undertaken by lone actors and AQ affiliates. These attacks, combined with a steady stream of AQ media propaganda, are designed to maintain AQ's position at the forefront of the global jihad movement.

- AQ affiliates Al Qaeda in the Arabian Peninsula (AQAP) and Al Shabaab (AS) continue to represent elevated terrorist threats. Recent jihadist messaging and attack plotting indicate a move away from complex plots or, at minimum, augmenting these plots with smaller-scale attacks against a broader range of targets.

- The threat implications of the "Arab Spring" in North Africa and the Middle East remain a concern, as terrorist groups attempt to take advantage of political unrest and replace current regimes with one sympathetic to an extremist alternative.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

- some Canadian and Western youth continue to be at risk of radicalization through their travel abroad in particular to Somalia, Yemen, Afghanistan and Pakistan. While some individuals may seek to fight in various 'jihads' abroad, others may seek to acquire training and fighting experience to return to Western countries and carry out terrorist attacks at home.

- terrorist attacks will continue to be aimed at targets

Assessment Note: This assessment primarily draws upon a body of unclassified information and media reporting. It strongly relies on historical incidents as indicators of future terrorist threats in the near to medium term.

Any use of the term jihad in this document should be interpreted as referring to violent action undertaken by extremist Islamists, primarily inspired by AQ's "single narrative", which states that Sunni Islam is under threat from the West and that it is the duty of all Muslims to take action, including violence, to defend the faith.

Canadian Connections

2. Fall 2011 marked the 10-year anniversary of the September 11, 2001, terrorist attacks, in which 24 Canadians died, reminding us that Canada is not immune to terrorism. More recently, in April 2011, a couple from Montreal were amongst the 17 dead after a suicide bombing at a popular tourist café in Marrakech, Morocco. Canadians, including Robert Fowler, Louis Guay, Amanda Lindhout and Colin Rutherford, have also been the victims of several high-profile kidnappings by terrorist groups since 2008.

3. At home, terrorism and extremism remain ongoing concerns, as demonstrated by various recent terrorism-related arrests and convictions. For example, Pakistani-Canadian Tahawwur Rana was convicted on 2011 06 09 in a Chicago court of providing material support to Pakistani-based terrorist group Lashkar-e-Tayyiba (LeT). Tahir Sharif, an Edmonton-based man of Kurdish descent, was arrested in January 2011 for alleged facilitation activities in support of AQ in Iraq. Sharif's hearing is set for May 2012 and he is facing extradition to the US for terrorism-related charges.

4. On 2011 03 29, Mohamed Hassan Hersi, a 25 year-old Somali-Canadian was arrested at Pearson Airport in Toronto on terrorism-related charges. It is alleged that he was leaving Canada to join Somalia-based Al-Shabaab (AS), a listed terrorist entity.

5. Three individuals, Hiva Mohammad Alizadeh, Misbahuddin Ahmed and Khurram Syed Sher were arrested in Ottawa and London, Ontario, on terrorism-related charges in August 2010. The pre-trial dates for Ahmed and Sher, accused of plotting terrorist attacks in Canada, are June 18 to

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

July 13, 2012. Alizadeh and Ahmed are also accused of possessing and making explosives for a terrorist group.

6. In December 2011, the Canada Revenue Agency (CRA) revoked the charitable status of the Canadian Foundation for Tamil Refugee Rehabilitation (CFTRR). The CRA found the CFTRR was funding organizations which the CRA believes operate as part of a support network for the Liberation Tigers of Tamil Eelam (LTTE), a listed terrorist entity in Canada.

7. It is also notable that in its *2011-2012 Reports on Plans and Priorities*, the Royal Canadian Mounted Police (RCMP) stated that it expected to either make arrests or disrupt at least six suspected terrorist and other national security threats in upcoming months.

CANADIAN TERRORIST-RELATED DEATHS

194 Canadians (36 civilians and 158 military members) have been killed by terrorists or while combatting terrorism since September 2001 (totals include Canada's Afghanistan Mission).

Canadian civilians killed:

- 2001: Twenty-four Canadians were killed in the September 11th attacks
- 2002: Two Canadians were killed in the Bali, Indonesia bombings
- 2003: Two Canadians were killed in the bombing of the UN headquarters in Baghdad, Iraq
- 2006: A Canadian diplomat was killed in an attack on a Canadian convoy in Afghanistan
- 2008: Two Canadians were killed in the Mumbai, India attacks
- 2008: In Afghanistan, the Taliban ambushed and killed two Canadian aid workers
- 2009: An explosion in Kandahar City, Afghanistan claimed the life a Canadian journalist
- 2011: In a café attack in Marrakech, Morocco, two Canadian residents were killed

Soldiers killed serving in Canada's Afghanistan mission

- 158 members of the Canadian Forces have been killed serving in the Afghanistan mission.

Canada Confirmed as Key Terrorist Target

8. Canada's international profile as a potential terrorist target has been confirmed through an analysis of files captured during the 2011 05 02 raid on Usama bin Laden's (UBL) Abbottabad, Pakistan compound. Canada is specifically named in the files, along with the US, Britain, Israel, Germany and Spain, as targets for terror strikes. Canada remains a viable target of Islamist terrorism mainly because of its participation in Western military and political alliances, its involvement in Coalition forces in Afghanistan, its support for Israel and the United States, and its geographic proximity to the latter.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION
SECRET
RELEASED UNDER ACCESS TO INFORMATION ACT
DOCUMENT DISCLOSED UNDER THE ACCESS TO INFORMATION ACT
INFORMATION DISCLOSED UNDER THE ACCESS TO INFORMATION ACT
SECRET
PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Where Does the Threat Come From?

9. Over the past year, Canadians and Canadian interests have faced a more diverse and complex terrorist threat, both at home and abroad.

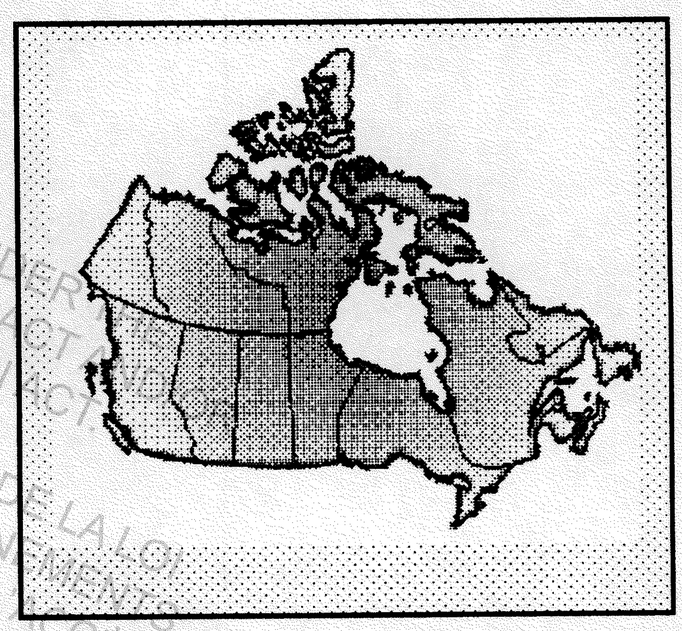
Terrorist threats to Canadians and Canadian interests emanate from four principal sources: AQ-inspired domestic extremists; AQ and its affiliates; other international terrorist groups; and issue-based domestic extremists.

Domestic AQ-Inspired Extremism: the Greatest Threat Within Canada

10. Domestic extremists who subscribe to the AQ ideology pose the most serious threat within Canada. Western Islamists – including converts to radical Islam

They understand Western culture, speak its languages and can move easily within its societies.

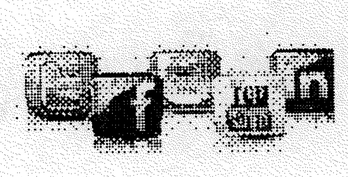
11. Motivated by ideas that Islam is threatened by Western policies and culture, these Islamists support the use of violence against their home or adopted countries. Some are attracted to jihad abroad, while others are radicalized or inspired by AQ ideology, but do not travel to fight abroad. Recent jihadist propaganda, such as AQAP's *Inspire* magazine, encourages adherents not to travel abroad and provides easy and simple guidelines on how to carry out opportunistic terrorist attacks at home. Previously disrupted plots demonstrate the existence of AQ-inspired extremists in Canada, the United States, Europe and elsewhere.



Role of the Internet

12. AQ and affiliated groups continue to pursue the radicalization, recruitment and training of Westerners, including Canadians, through increasingly accessible and sophisticated online propaganda. The growth of internet forums and the use of social media, as well as the professional quality of jihadist propaganda, have played a significant role in spreading the jihadist ideology on the Internet. The Internet allows jihadists to share ideas and sermons about violent jihad, as well as access professionally designed online teaching manuals on bomb-making and related terrorist tradecraft.

13. Interestingly, the presence of jihadi groups on social media sites has increased following the deaths of UBL and AQAP radical ideologue Anwar Al-Awlaki, as numerous video clips devoted to both AQ figures have been posted. Organizations "tweeting" on the social media site Twitter now include the Taliban, Al-Shabaab, Hizballah and others.



PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Prison Radicalization

14. Studies have identified that Islamist extremists have been further radicalized in prisons in countries such as Canada, the United States, Britain, France and Spain.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Globally, AQ Core, AQ Affiliates and Like-Minded Groups Remain the Primary Threat

15.

The primary threat remains Islamist terrorists, in particular AQ and its affiliates based in Afghanistan, Pakistan, the Middle East and Africa.

Al Qaeda (AQ) Core

16. AQ Core is under sustained counter-terrorism pressure in Pakistan from both Pakistani and US forces and much of AQ Core's daily attention is now firmly focussed on survival. The killing of AQ senior leader Usama bin Laden (UBL) by US Special Forces on 2011 05 02, as well as the deaths of general manager Atiyah abd al-Rahman, operational commander Ilyas Kashmiri and many other operatives, has seriously weakened AQ Core.

17. AQ Core still leads the global jihad movement by providing ideological cohesion, inspiration and direction to its affiliates, like-minded groups and individual extremists. In June 2011, AQ Core's senior leaders released a video emphasizing the importance of individual jihad in the West and in February 2012, AQ senior leader al-Zawahiri released a video message in support of the Syrian uprisings.

18. AQ Core has traditionally focussed on conducting high-profile, mass-casualty terrorist attacks against the West, with significant direction and expertise for these attacks provided by operational commanders in the Afghanistan-Pakistan theatre. However, AQ commanders in the Afghanistan-Pakistan region are no longer the primary drivers behind plots targeting the West. The threat against the West has diversified as the global jihad is increasingly being driven by violent home-grown extremists and AQ affiliates. Recent jihadist messaging and attack plotting indicate a move away from complex plots or, at minimum, augmenting these plots with smaller-scale attacks against a broader range of targets.

AQ in the Arabian Peninsula (AQAP)

19. Yemen-based AQAP is a capable and innovative group that has adopted a multi-pronged strategy, balancing local, regional, and international agendas. As such, the group is dedicated to mounting attacks both within Yemen, in neighbouring Saudi Arabia and Gulf states, and against the West. The group has attempted two attacks against Western aviation (the Christmas day "underwear bomber" in 2009, and the cargo printers plot in October 2010) and remains focussed on targeting the aviation sector.

20. In the fall of 2011, AQAP radical ideologue Anwar Awlaki was killed in a targeted air strike.

21. Since the spring of 2011, Yemen has been experiencing a serious political crisis

22. AQAP has successfully exploited the political instability and has taken and held new territory in Yemen.

Al Qaeda in the Islamic Maghreb (AQIM)

23.

Kidnapping foreigners for ransom is AQIM's most profitable activity, bringing in millions of dollars in revenue.

24. Before his death, UBL demanded that France withdraw its troops from Afghanistan in exchange for the release of four French hostages who were kidnapped in northern Niger in September 2010. Similarly, in January 2012, AQIM warned the French, British, Swedish and Dutch governments that any operation against them would result in the death of hostages.

25. AQIM is taking advantage of unrest to acquire weapons and expand its influence AQIM has also identified

Nigeria as a country of interest and has promised to assist and train Boko Haram, a Nigerian Islamist extremist group.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Al Qaeda in Iraq (AQI)

26. In 2004, Al Qaeda in Iraq (AQI) was founded by Jordanian Abu Mosab Zarqawi with the goal of conducting attacks in Iraq as a precursor to eventual international attacks aimed at advancing AQ's broader goal of establishing a global Islamist caliphate. AQI leaders remain faithful to this vision, conducting attacks throughout Iraq, including several sophisticated multiple Improvised Explosive Device attacks in Baghdad in late 2011, while indicating a sustained interest in activities outside Iraq's borders. Recent public statements continue to suggest an ongoing AQI focus on attack planning against Western countries. Further AQI propaganda issued in January 2012 declared victory over the US military in Iraq, stating, "we will come to you from all over...you will hear our footsteps on the ground," a possible reference to future attacks against the US.

Al Shabaab (AS)

27. In August 2011, AS withdrew its fighters from the Somali capital, Mogadishu. However, on 2011 10 04 AS dramatically reasserted itself into Mogadishu by carrying out the group's most deadly suicide-bombing ever. Over 100 were killed, the majority being young Somali students waiting in line to receive examination results from the Somali Education Ministry. In October and November 2011, Kenyan and Ethiopian forces moved into Somalia in pursuit of AS and to bring security to the areas of Somalia that border their respective countries. This military incursion caused AS to lose control over significant amounts of territory and the group vowed to respond. Grenade attacks conducted across Kenya in the fall of 2011 were believed to have been conducted by AS in retaliation for the Kenyan military operation in Somalia.

28. Western interests are believed to be priority targets for AS. It is notable that Canada was specifically identified as one of several countries targeted for attack in the martyrdom message of an American citizen and AS member who conducted a deadly suicide bombing in Somalia on 2011 10 30. Unclassified reporting indicates that approximately 20 Somali-Canadians are believed to have travelled to Somalia to engage in violent jihad as foreign fighters. On 2012 02 09, AS declared its affiliation with AQ. The combination of this declaration, along with the deteriorating AS situation in Somalia, raise concern that foreign fighters may disengage from Somalia to continue their violent jihad internationally, and potentially target their home countries, including Canada.

Boko Haram (BH)

29. Boko Haram (BH), a northern Nigerian extremist group, also known as Nigeria's "Taliban", gained notoriety in 2009 following a series of clashes with the government of Nigeria that led to the death of the group's leader. Meaning "western education is a sin" in the Hausa language, BH's goal is to establish an Islamic Caliphate throughout Nigeria. Nigeria has been identified by

AQ as a country of focus due to its large Muslim population and numerous Western, including Canadian, interests.

30. The majority of BH operations have been confined to northern Nigerian states and have targeted government, military, police and Christian entities. However, in December 2010, BH carried out a bomb attack outside its zone in the central Plateau State. In August 2011, BH further departed from its domestic targeting pattern when it bombed the UN headquarters in the Nigerian capital of Abuja, killing at least 24 people.

31. BH is not an official AQ affiliate but is closely associated with AQIM.

BH attacks have increased in frequency and sophistication since 2011 including fighting alongside AQIM in the Touareg rebellion in Mali,

instability in the Middle East and North Africa to increase their influence and mount operations.

Other International Terrorist Groups and Regions of Concern

32. While Canadian authorities have long focused on groups such as Hizballah and Liberation Tigers of Tamil Eelam (LTTE), new groups and regions of concern continue to develop as extremists take advantage of the ongoing political

Liberation Tigers of Tamil Eelam (LTTE)

33. LTTE continues fundraising activities within Canada, but at a reduced capacity. The Canadian government is actively working to reduce the possibility of further maritime migrant smuggling with potential links to the LTTE, as demonstrated by the 2011 06 14 arrests of four Sri Lankans on human smuggling charges. The individuals were crew members of the *MV Ocean Lady*, the vessel that arrived on Canada's west coast in 2009.

Lashkar-e-Tayyiba (LeT)

34. Lashkar-e-Tayyiba (LeT) is a highly capable extremist organization which has been implicated in a number of terrorist strikes in India, including the November 2008 Mumbai attacks that killed over 160 people, including two Canadians.

35. The area of operations for LeT has traditionally been limited to South Asia. However, in 2009, LeT was implicated in a planned attack against the offices of a Danish newspaper responsible for publishing a cartoon depicting the prophet Mohammed. The Danish plot represents a rare foray into international attack operations and the organization is not known to

have carried out a successful operation outside of South Asia.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Abu Sayyaf Group (ASG)

36. Based in the Philippines, the Abu Sayyaf Group (ASG) has been actively involved in several kidnap-for-ransom operations. It has also bombed several religious sites as well as 'soft' targets such as restaurants and commuter buses. Travel advisories for Canada and the US specify that tourists should avoid all travel to the Sulu Archipelago and Mindanao in the Philippines. The Department of Foreign Affairs and International Trade (DFAIT) further advises caution in Manila, as terrorist groups tend to target tourist attractions, shopping malls and convention centres. The ASG is known to operate in concert with other terrorist groups in the Philippines, namely, the Moro Islamic Liberation Front, currently in peace negotiations with the Philippine government.

Tehrik-e-Taliban Pakistan (TTP)

37. Canada listed Tehrik-e-Taliban Pakistan (TTP) as a terrorist entity on July 5, 2011. The TTP aims to overthrow the Pakistani government, to create a Taliban-style Islamic emirate ruled by Shariah law, and to force NATO troops out of Afghanistan. The TTP has increasingly used suicide bombers, enabling the group to strike political, military, and law enforcement targets across Pakistan. The TTP also claims to have trained failed New York City Times Square bomber, Faisal Shahzad in Pakistan in 2009-10.

Hizballah

38. Hizballah has had a presence in Canada

Hizballah supporters conduct fundraising, procurement and intelligence activities in Canada, and are involved in organized crime, including fraud. Hizballah continues to threaten retaliation against Israeli interests worldwide for the killing of key individuals in the past two years.

39. The Arab Spring and the unpredictable nature of the current situation in the Middle East,

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Syria

40.

In

2011 10, Canada expanded sanctions against Syria by freezing Assad regime assets and prohibiting dealings on designated individuals and entities associated with the regime.

41. On 2012 01 23, a Syria-based jihadist group calling itself the Al Nusrah Front announced its formation in a video statement, claiming "we will be a firm shield and a striking hand to repel the attacks of this criminal Al Asad army..." The Al Nusrah Front has since utilized AQ-affiliated jihadist websites to claim credit for a series of attacks in Syria, including two bombings in Damascus on 2012 03 17 that killed 27 people and wounded more than 100.

Iran

42. Canadian Prime Minister Stephen Harper has said that Iran poses the "worlds most serious threat to international peace and security" because of its nuclear ambitions. On 2012 01 31, Canada expanded sanctions against Iran, freezing the assets of five entities and three individuals in response to proliferation activities undertaken by Iranian authorities.

43. Iran's support for terrorism is considered an important means of furthering its national interests and of exporting the "Islamic Revolution"; Iran has been linked to AQ, Hizballah, Hamas, TTP and other groups. On 2012 02 16, the US Treasury Department designated the Iranian Ministry of Intelligence and Security (MOIS) for its support to terrorist groups and its role in perpetrating human rights abuses. According to the Treasury, MOIS facilitated the movement of AQ operatives in Iran and provided weapons and money to AQI. The US has also designated Iran's Islamic Revolutionary Guard Corps- Qods Force (IRGC-QF) as a banned terrorist entity for its active role in terrorism, its involvement in Iran's nuclear and ballistic missile programs and its support for the Taliban in Afghanistan. In October 2011 the Qods Force was implicated in the plot to assassinate the Saudi Ambassador in Washington D.C. Two men, one of which is an alleged IRGC-QF member, were arrested and charged with conspiring to kill Adel Al-Jubeir while he dined at his favourite restaurant.

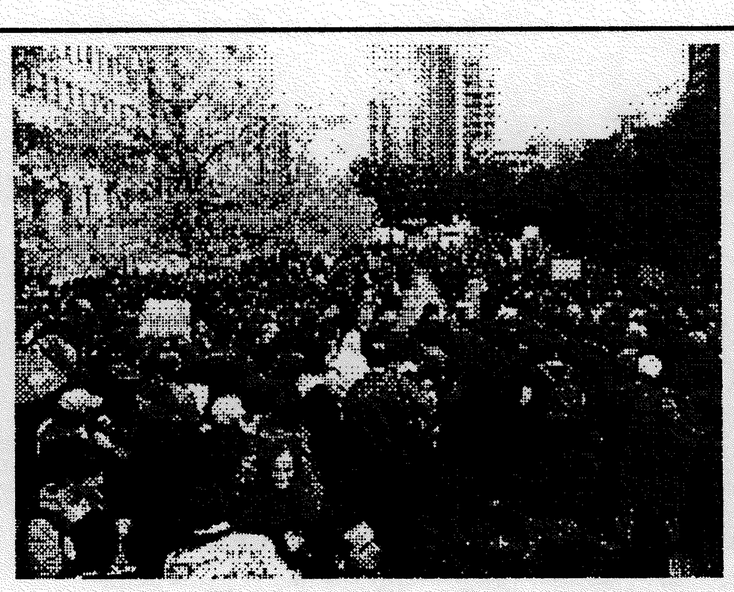
The Sinai

44. On 2011 08 18, attacks carried out by Sinai-based extremists near the Israeli city of Eilat left 8 Israelis killed and thirty-one injured. In August 2011, a proclamation announcing the alleged establishment of an AQ "Emirate of the Sinai Peninsula" appeared on AQ-affiliated websites but was quickly removed. However, in December 2011, another Sinai-based group calling itself *Ansar al-Jihad* issued an online manifesto announcing its formation and pledging allegiance to AQ.

Domestic Issue-based Extremism: An Ongoing Security Concern

45. Domestic issue-based extremism, while a lesser threat, remains an ongoing security concern. A small number of domestic extremists continue to be associated with issue-based causes such as environmentalism, anti-capitalism, anti-globalization and far-right racism.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.



46. While protest activities in Canada are generally peaceful, a small number of issue-based extremists have targeted international events in Canada to engage in activities that have extended beyond lawful protest, as evidenced during the G8/G20 Summits in Ontario in late June 2010. These extremists continue to confront law enforcement and vandalize property by employing direct-action tactics (e.g. roadblocks, breach of security perimeters, assault against security personnel) in order to achieve their objectives.

47. The Freeman on the Land is a growing anti-government movement in Canada that includes adherents from both the left and the right wings of the political spectrum. At the core of the movement's beliefs is the idea that the government operates outside of its legal jurisdiction and therefore Freeman members do not recognize the authority of national, provincial, or municipal laws, policies or regulations. Freeman members now constitute a major policing problem in several provinces and have occasionally engaged in acts of violence against the police.

48. In November 2011, German authorities linked a series of race-related murders conducted between 2000 and 2006, as well as the 2007 killing of a German police officer, to a neo-Nazis terror cell. The cell had been operating in the eastern part of the country for over 10 years and appears to be part of a broader network.

In Canada, isolated cases of right-wing extremist violence against minority groups or properties have been reported

49. Aboriginal communities across Canada remain focussed on key issues such as sovereignty and outstanding land claims. At times more radical members of Aboriginal warrior societies advocate violence as a means of drawing attention to these issues.

Potential Targets of Terrorist Attacks: A Broadening Array

50. Disrupted and failed terrorist plots indicate that AQ and affiliated groups continue to focus on highly symbolic targets in attack planning against the United States, Israel and their Western allies. Wherever possible, AQ aims to attack targets which would generate worldwide media coverage.

The Olympic Games

51. The terrorist threat in the UK recent domestic counter-terrorism successes and the deaths of key AQ figures in the Afghanistan-Pakistan region.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTUE DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Critical Infrastructure

53. AQ has long prioritized attacks against Western financial, economic and business interests globally, as well as oil interests in the Middle East. Analysis of material extracted from the UBL compound in Abbottadad, Pakistan, revealed that UBL and his associates were very interested in mounting attacks on "infrastructure targets', specifically critical transportation infrastructure in large cities. The UBL compound information also emphasized that priority was placed on conducting attacks intended to bring Western "economies to their knees".

Transportation

54. The global transportation network continues to remain a prominent target for transnational terrorist organizations seeking to inflict civilian casualties. While mass-casualty attacks targeting the transportation sector have traditionally been associated with commercial aviation, reporting from the UBL compound indicates that AQ senior leadership was considering attacking rail infrastructure to commemorate the 10th anniversary of 9/11. Another notable example was the previous AQAP attempt to bomb a cargo flight in October 2010, while in February 2012, a jihadist poster in a web forum posted ideas on how to repeat the 9/11 attacks. These incidents demonstrate that transnational terrorist organizations remain committed to exploiting potential transportation security vulnerabilities to stage mass-casualty attacks against high-value transportation targets.

55. In addition to inflicting civilian mass casualties, attacks against the global transportation network may also be motivated by economic factors. As demonstrated by AQ's continued interest in attacking oil tankers, terrorist organizations are willing to directly attack the transportation sector for economic reasons if they believe damaging the global economy will advance their agenda.

Energy and Utilities

56. Canadian-based energy companies operate worldwide and have previously been targeted by Islamist extremists. AQ has reaffirmed its intention to target oil infrastructure on many occasions, and the group has indicated a particular interest in striking against those involved in exporting Middle Eastern oil resources to the West. employees and assets of

various Canadian-based energy companies continue to face a real threat from AQ and affiliated groups, such as AQAP and AQIM, in global regions of conflict and instability, including the Arabian Peninsula and North Africa.

Communications and Information Technology Infrastructure

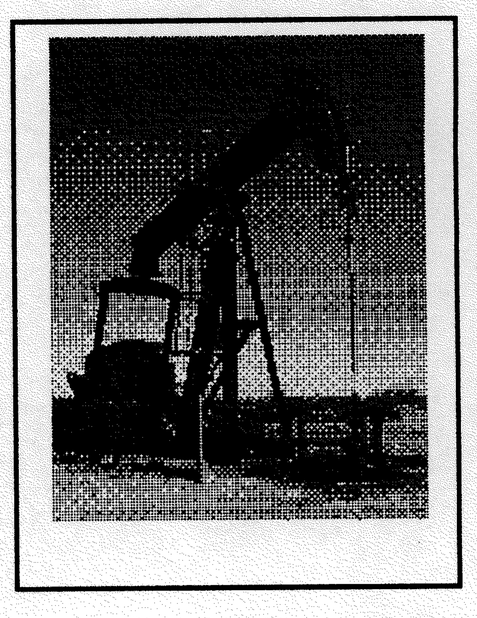
57. Terrorists and extremists continue to rely on computer networks to engage in operational support for terrorist activities, including communication, radicalization, recruitment, financing, training,

58. The threat of cyber attacks on critical infrastructure sectors is also a growing security concern, especially in the sectors of energy, finance, telecommunications and government sectors.

Other Potential Targets

Commercial Interests

60. AQ and its affiliates have attacked various business interests, and hotel chains and luxury hotels catering to Westerners in Muslim countries continue to be targeted. Notable hotel attacks include the Intercontinental Hotel in Kabul, Afghanistan (2011), the Pearl Continental, Peshawar, Pakistan (2009), the Taj and Oberoi, Mumbai, India (2008), the J.W. Marriott, Jakarta, Indonesia (2007), and the Hyatt, Radisson and Days Inn, Amman, Jordan (2005).



61. Issue-based extremists also target commercial interests, especially companies that sponsor events or products singled out due to a grievance associated with an environmental or other special interest cause. A self-proclaimed anarchist group calling itself FFFC-Ottawa claimed responsibility for a firebombing at the Royal Bank of Canada (RBC) branch in Ottawa on 2010 05 18. In a message released following the incident, the group stated it targeted RBC because of its corporate sponsorship of the 2010 Vancouver Olympics and for being a major financier of Alberta's oil-sands project.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Western Economies and Terrorist Resourcing/Financing

62. Documents obtained in the May 2011 UBL compound raid revealed that one of the main priorities of UBL and AQ was to cause significant harm to the economy of the US and other Western countries. Many studies have concluded that major terrorist attacks have had a multi-billion dollar negative economic impact on many Western countries.

63. Conversely, terrorists require funds to facilitate their radicalization, recruitment, training and attack planning activities. While terrorists persistently find new means of obtaining and transferring funds to support their operations, traditional methods are also used. For example, terrorists continue to collect money for their activities through fundraising within local diaspora communities in developed countries (including through coercion and so-called diaspora "taxes"), seeking donations from rich or sympathetic governments, and through criminal activities such as fraud, drug trafficking, or kidnapping for ransom.

64. According to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) 2011 annual report, 103 cases of possible terrorist activity financing and threats to Canada's security were detected and shared with partners, compared to 73 cases in 2010. In December 2011, the charitable status of the Canadian Foundation for Tamil Refugee Rehabilitation (CFTRR) was revoked after CRA determined CFTRR was funding organizations believed to operate as part of the terrorist LTTE support network.

Terrorist Tactics

65. Tactics employed by terrorists vary widely, depending on the intent and capability of each threat actor, target vulnerabilities, situational opportunities and risks. Terrorist attacks can be planned over long periods by several individuals, be spontaneous acts by lone actors or any number of variations in between.

66.

AQ Core has traditionally focussed on high-profile mass-casualty terrorist attacks against the West,

67.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Favoured terrorist tactics include person and vehicle-borne improvised explosive devices (VBIEDs), armed assault using firearms, and attempted airline bombings. Multiple concurrent or sequential attacks using varied tactics provide greater impact as well as the possibility of targeting first responders reacting to the initial attack.

68. A number of small-arms attacks occurred in 2010 and 2011. In general, such attacks remain relatively rare in spite of the tactical advantages they offer to assailants. The November 2008 terrorist attacks in Mumbai, India, involved ten gunmen and multiple targets, lasting over two days and capturing global media attention. The Mumbai attacks demonstrate the potential lethality of well-planned coordinated attacks against soft targets using multiple tactics, including commercially available small arms.

***Chemical, Biological, Radiological and Nuclear* (CBRN)**

70. On 2011 10 27, Alaska resident and member of the Alaska Peacemaker Militia, Mary Morgan was apprehended by Canadian authorities at a Yukon-Alaska Canadian port of entry. Morgan was subsequently turned over to American authorities and indicted in the US on charges, including being a felon in possession of a firearm. According to US government court documents, at the time of her attempted border crossing, Morgan was had numerous documents, including background information downloaded from the internet on ricin, directions on how to build pipe bombs, make salt into an explosive, and a list of common household poisons and a reference to a "poisonous plants database" (which includes the castor plant from which ricin is derived). and the case remains before US courts.

HANDLING INSTRUCTIONS

This document is the property of the Integrated Terrorism Assessment Centre (ITAC). Prepared by ITAC, it is derived from various sources with information effective as of the date of publication. It is provided to your agency/department in confidence and may be further disseminated by your agency/department to those with the need to know. It must not be reused in any way, in whole or in part, without the consent of the originator. Any feedback should be directed via email to ITAC at or to ITAC Partnerships at

This document constitutes a record which may be subject to mandatory exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence may also be protected by the provisions of the *Canada Evidence Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with ITAC.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Canadian Security Intelligence Service

Intelligence Assessment

TOP SECRET/

CSIS IA 2011-12/83
2011 11 21

Cyber Threats and Security: An Overview

Summary

The Canadian public and private sectors are dependent on their computer-based systems and associated network connections (including those to the Internet), which contain vulnerabilities that can be compromised by those with the necessary knowledge, tools and techniques.

Stuxnet has been described as a watershed or a tipping point in the realm of cyber. The Stuxnet worm acts as a proof-of-concept, illustrating that attacks once thought to be hypothetically possible but improbable can be mounted against a target if necessary knowledge, resources and assets are dedicated to the operation.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Cyber tools provide insiders and other threat actors with the opportunity of removing information from targeted sites while making it difficult for security and intelligence organizations to attribute such action since threat actors can be located in one legal jurisdiction and operate out of one or more elsewhere.

Even though system vulnerabilities have been exploited by a variety of threat actors, the computer/network user is the weak point in the system. Users have been the target of social engineering operations
to compromise their computer and exploit the enterprise

New cyber attack tools and techniques will be developed in efforts to compromise Canadian public- and private-sector systems.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Head, IAB

CSIS_PUBLICATIONS / SCRS_ PUBLICATIONS

CAVEAT

This document is the property of the Canadian Security Intelligence Service and may constitute "special operational information" as defined in the Security of Information Act. It is loaned to your agency/department in confidence. The document must not be reclassified or disseminated, in whole or in part, without the consent of the originator.

Canadian departments, agencies or organizations: This document constitutes a record which may be subject to mandatory exemption under the Access to Information Act or the Privacy Act. The information or intelligence may also be protected by the provisions of the Canada Evidence Act. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

Foreign agencies or organizations: This document is loaned to your agency/department in confidence, for internal use only. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator. If you are subject to freedom of information or other laws which do not allow you to protect this information from disclosure, notify CSIS immediately and return the document.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Introduction

1. We live in an era where almost every tool (automobiles, smart phones and other devices) used in daily life incorporates a computer, an Internet connection and some kind of wireless communication capability. Technological innovation has been the basis of Canada's economic development, prosperity and security, especially as the Canadian economy becomes increasingly knowledge-based. A number of actors have identified this reliance on technology as a vulnerability and have sought to exploit it. stealing our industrial secrets, our personal identities, and penetrating our critical infrastructure networks, actors undermine our continued economic prosperity and peace, order and good government.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

2. The Canadian public and private sectors depend on their computer-based systems and associated network connections (including those to the Internet) to conduct their day-to-day operations, and these systems and networks underpin all aspects of the national critical infrastructure (including water treatment, and hydro and nuclear power plants). Such networks

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

consist of four principal elements: hardware, software, the interconnection with communication and other networks, and the user. While computer-based networks provide greater functionality to daily operations within various sectors of activity, they contain vulnerabilities

3. The configuration of the devices, the default settings for their various capabilities, the speed with which they are brought to market, the bundling of functions within a single product are not necessarily created with security in mind. Even though these vulnerabilites have been exploited by a variety of threat actors

the computer/network user is the weak point in the system. In recent computer-related incidents, the user has been the target

to compromise their computer and exploit the enterprise where the person works

Vulnerabilities

4. The software and hardware that comprise computer-based networks normally possess some form of vulnerability. Many of these are known and their details can be found via the Internet. Threat actors use a variety of software applications to observe these networks for information relating to system configuration, and software and hardware components which comprise them, in order to develop the means to compromise specific systems, networks and users. Some of these efforts are automated, combining the probing – to see what systems and defences the target is running - and compromise function. While some of these efforts are opportunistic, looking for any vulnerable systems, others are more targeted, seeking to compromise the systems used by specific government departments/branches, businesses, and military and academic institutions.

5. Previously, system resources only could be used within the public or private-sector enterprise. Security was designed to protect the periphery of the enterprise to prevent access to

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

computer and other assets. Once these computer-based systems were networked and connected to the Internet, it became difficult to define what constituted an enterprise's periphery. Employees can conduct enterprise operations using desktops, laptops, smartphones, tablets and other handheld devices wherever they are located around the globe, and have the ability to move data from one device to another using a variety of removable media (thumb drives, discs, and in the memory of various handheld devices) and "cloud computing"2.

6. Early adopters acquire and use new products for reasons of functionality rather than with security in mind, creating new vulnerabilities within their enterprises. Threat actors no longer require direct access to a targeted system to effect a compromise. They can achieve remote access using a variety of tools and techniques. They can provide themselves with authorised access to the targeted system manipulate its operation, create backdoors into the system, use system resources to mount compromise efforts on other networks, and steal, erase or alter the information resident on or accessible via the system.

7. The system user is a weakpoint within an enterprise as he/she generally uses technology without understanding it. Their use of the technology determines the security of the enterprise,

The user possesses or has access to information and the networked nature of computer-based systems makes this data more accessible to threat actors.

8. At the level of the individual user (both at home and work), they can be a target for identity theft. The private sector is a target because of its proprietary information,

The public sector possesses information relating relating to political, social and economic issues, both domestically and abroad.

2 Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTUE DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Compromise/Exploit Tools

11. The focus of system security, stated simply, is to ensure access to the resources when required, integrity of the data available via the system, and the identity of the system's users. Threat actors use a variety of tools and techniques, which vary from the fairly simple to very complex, to compromise and exploit the systems they target. The capabilities of threat actors are defined by the extent of these resources and assets. The following outline some of the types of tools that are most noted in the media

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

16. Advisories issued by the UK and the US in 2005 outlined aspects of the crafting, sending, and impacts of these emails. The attack campaigns, gathered information about topics of interest to government departments and the private sector, and about employees within them. This information was used to craft the emails, target the recipient of the message, give the appearance that the originator was a person or organization known to the addressee (spoofing the sender), to have the recipient of the message open the email,

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

23. In October 2011, some anti-virus firms issued assessments of Duqu, a Stuxnet-like variant that uses a Word Document zero-day vulnerability to compromise systems. It has been detected in systems in France, the Netherlands, Switzerland, Ukraine, India, Iran, Sudan and Vietnam, and is suspected of compromises in Austria, Hungary, Indonesia and the UK. Duqu is a remote access Trojan that shares code with the Stuxnet malware

Some describe its infection of systems as a possible precursor of future attacks.

New Tools

24. Media reporting has raised awareness of the potential utility of research projects and presentations at hacker conferences,

In one instance, a project illustrated how an unmanned aerial vehicle (UAV) could be loaded with hardware and software that would allow the UAV to overfly and compromise/exploit wireless networks.

25. Furthermore, efforts will be made to compromise and exploit the capabilities of handheld devices such as smartphones and tablets, as more and more individuals adopt them for business and personal use. Given that these devices can contain personal and proprietary information, they will serve as a gateway into enterprises.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTUE DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Choice of Tools

26. Some of the attack tools and techniques that have been observed can be fairly simple,

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTUE DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Timing

28. The timing of attacks seems to fall into three categories: the normal day-to-day compromise and exploitation of systems found to be vulnerable through automated or directed operations online; more directed phishing and spear-phishing attacks against specific organizations/institutions

and those associated with special social and political events, and economic activities

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTUE DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTUE DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Special Events

29. Criminals and other threat actors have attempted to exploit systems associated with sporting events, and international expositions for personal gain

30. Demonstrations opposing some aspect of government social, economic or foreign policy are usually accompanied by some form of online activity.

Regional Conflicts/Tensions

32. Every conflict or period of political tension is usually accompanied by some form of online campaign by one group targeting the other's online resources. In some cases, one or both sides have supporters who exploit vulnerable systems to alter Web page content to display a message that seeks to rationalize a particular political position or to achieve some political goal.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

37. Government officials in the UK believe computer-based systems provide new opportunities for states to engage in new arenas to target critical infrastructure and steal information from the public and private sectors.

These concerns are echoed in the US where it has been stated that the financial sector has been targeted and exploited,

US officials have voiced concerns regarding the activities of hacking collectives, such as Anonymous,

to exploit vulnerable Web servers, Web sites, computer networks

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Challenges

49.

some enterprises may not detect such intrusions into their systems or report them to the relevant authorities because of fears of loss of confidence among clients, partners and other users of their services. There is an ongoing contest between the development of attack tools and techniques by threat actors and counter measures by system administrators and defenders.

50. While there may be a variety of technical measures, and policies and procedures to secure IT systems, the weak point remains the system user. The questions that remain are: how to link security to the adoption of new technologies, how to incite users to be more secure in the use of technology,

Conclusion

51. The cyber threats posed by threat actors affect Canada's national and economic security. This has implications for its critical infrastructure, the operation of its public and private sectors, and its domestic and international interests.

53. Cyber tools provide insiders and other threat actors with the opportunity to remove information from targeted sites

Given the nature of the Internet and the existence of "mirror sites" (copies of the sites located on servers in other parts of the world), it is difficult to remove such data once it is posted. The same is true of the hurdles associated with trying to attribute the

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTUE DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

action when threat actors can be located in one jurisdiction and operate out of one or more elsewhere.

54. New cyber attack tools and techniques will be developed in efforts to compromise Canadian public and private-sector systems.

The cyber-related threat environment will evolve and become more complex, creating ever greater challenges for Canada within the context of national security.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTUE DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTUE DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Intelligence Assessment

TS

CSIS IA 2011-12/10
2011 04 18

The Global Overview: Weapons of Mass Destruction (WMD) and Proliferation Threats

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Summary

The most significant, urgent threats of weapons of mass destruction (WMD) proliferation today are the nuclear weapons programs of Iran, North Korea together with the ever-present danger of the malevolent use of chemical, biological, radiological or nuclear (CBRN) materials by terrorists worldwide.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

CSIS_PUBLICATIONS / SCRS_ PUBLICATIONS

CAVEAT

This document is the property of the Canadian Security Intelligence Service and may constitute "special operational information" as defined in the Security of Information Act. It is loaned to your agency/department in confidence. The document must not be reclassified or disseminated, in whole or in part, without the consent of the originator.

Canadian departments, agencies or organizations: This document constitutes a record which may be subject to mandatory exemption under the Access to Information Act or the Privacy Act. The information or intelligence may also be protected by the provisions of the Canada Evidence Act. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

Foreign agencies or organizations: This document is loaned to your agency/department in confidence, for internal use only. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator. If you are subject to freedom of information or other laws which do not allow you to protect this information from disclosure, notify CSIS immediately and return the document.

Introduction

1. The most significant, urgent threats of weapons of mass destruction (WMD) proliferation today are the nuclear weapons programs of Iran, North Korea

together with the ever-present danger of the malevolent use of chemical, biological, radiological and nuclear (CBRN) materials by terrorists worldwide. Any comprehensive survey of global WMD threats, however, must also include those states that serve as sources of technology and materials to other states of proliferation concern; those potential adversaries with the existing capacity to deliver devastating nuclear attacks on North America; those states that, although not worrisome by virtue of WMD programs of their own, have traditionally figured as key transhipment points for technology and materials destined for the WMD programs of others; and a handful of other states that are known or suspected to either possess or be seeking WMD. From a Canadian perspective, it is also important to know which countries may be seeking to use Canada for the acquisition of materials and technologies for a WMD program.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTUE DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

3. Iran. The fact that Iran has engaged in activities related to nuclear weaponization suggests that it is, at a minimum, seeking to acquire the capacity to produce such a weapon.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTUE DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

4. Following its ratification of the Chemical Weapons Convention (CWC) in 1997, Iran admitted to having had a past offensive CW program,

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTUE DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

5. Iran has the ballistic missile program

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTUE DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTUE DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

6. Syria. The Al-Kibar reactor bombed by Israel in 2007 09,

8. Syria has long maintained a substantial force of ballistic missiles,

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTUE DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

East Asia

19. North Korea. North Korea has twice tested a nuclear explosive device, demonstrating that it has a nuclear weapons capability,

After long denying that it had a parallel program of uranium enrichment, North Korea in late 2010 took the world by surprise by unveiling a relatively sophisticated centrifuge enrichment facility at its Yongbyon nuclear complex.

20. North Korea has a very active ballistic missile program,

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTUE DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

Cbrn Terrorism

29. A wide range of terrorist groups and individuals have historically shown an interest in the malicious use of CBRN materials and continue to do so. Nevertheless, the large-scale use of CB agents by Aum Shinri Kyo in Japan in the 1990s has not been followed by similar attacks elsewhere, as once feared. Al Qaeda (AQ) and a few other groups are believed to retain the aspiration for "strategic" CBRN attacks against Western targets, and have previously demonstrated (along with Aum) that it is possible to conceal the existence of substantial programs of this type.

Small-scale chemical and biological incidents continue to be reported in various conflict zones such as Afghanistan and Iraq,