Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

PUBLIC REPORT | 2011-2013

Canada

MESSAGE FROM THE DIRECTOR

The release of our Public Report is an important event for the Canadian Security Intelligence Service (CSIS), because it provides an opportunity for us to talk about who we are and about the security threats Canada faces.

It used to be the intelligence community would rarely – if ever – speak to those issues in a public forum. In today's world, however, it may be that the first line of defence in protecting national security is public awareness of the threat environment. Security is a collaborative effort between governments and citizens, and in that spirit we at CSIS see the value in transparency, to the extent such is possible. It is an axiom within intelligence services that successes are known only to us but failures are known to all. In between those two poles, there is much that can be shared.

In 2011-2013, the review period of this report, there was an exponential increase in public awareness of the cyber threat, a realization that if you open even one malicious e-mail hostile actors can steal your most sensitive information – and do so in a blink of an eye and from thousands of kilometres away. CSIS and its partners are mandated to protect Canada's security interests. Our job becomes immeasurably easier as ordinary Canadians learn to be more careful where they click.

The sophistication and determination of cyber-spies, some of whom are backed by foreign governments, will continue to grow. Individuals, corporations and nations that are unable to defend themselves will suffer economic and other consequences. Fortunately Canada is well-positioned to meet this very serious threat.

Despite the visibility attached to cybersecurity, in this Public Report we reveal that terrorism is still our greatest preoccupation. The goal of terrorists is not to steal secrets in the countries they target but to kill people. This remains an immediate danger to public safety.

In April 2013, two men, one in Toronto and one in Montreal, were charged with plotting to attack a passenger train. In announcing those arrests, our law enforcement colleagues alluded to links between the accused and Al-Qaeda elements abroad. In a globalized world of personal mobility and modern communications technology, violent people and violent ideologies have greater reach than ever before. Al-Qaeda and other groups continue to successfully recruit and mobilize terrorist operatives, and those same groups continue to identify Canada as an attractive target.

Terrorism is a multifaceted phenomenon, one that has evolved since the *CSIS Act* was conceived nearly 30 years ago. In the heyday of political terrorism, a terrorist's objective was more often than not to draw attention or support for a cause, rather than to maximize civilian casualties. Those were the days when violent groups issued demands and even gave advance warning. In executing the 9-11 attacks, by contrast, the hijackers made no demands and Al-Qaeda initially did not even claim responsibility. Similarly, the contemporary phenomenon of "lone actor" terrorism – manifested most horrifically in 2011 by Anders Breivik in Norway – seems to have as its objective the murder of as many people as possible.

Moreover, modern technologies have accelerated the speed with which threats develop. The time between the conception and execution of an attack can be very short. When it comes to counter-terrorism, CSIS operates in a higher risk environment than ever before, with no margin for error. The sad reality of Canadian citizens participating in terrorist activities is another aspect of the problem that is rightly drawing public attention. (See "A Canadian Concern", page 27)

That said, one of the most disturbing national security incidents of 2011-2013 was not terrorism. In January 2012, Sub-Lieutenant Jeffrey Paul Delisle was arrested in Halifax and charged with spying for a foreign government. He later pleaded guilty and received 20 years in prison.

The case was historic because it marked the first conviction under the *Security of Information Act* and served as a reminder that Canada is a highly attractive target for hostile intelligence agencies. There are as many, and arguably more, attempts to steal Canadian secrets today – economic, military, political – than at any time in our national history.

As with counter-terrorism, our counter-espionage units operate in a higher risk environment than ever before. In the age of thumb drives, a warehouse of documents can be stolen in the blink of an eye and then carried away in one's pocket. As CSIS has said before, we wish for a world where the methods by which Canadian interests are harmed were diminishing rather than expanding, but sadly that is not the world we know.

Recently, the open media carried reports of new nuclear testing in North Korea. Meanwhile, Iran's nuclear ambition continues to be a developing story with implications for international stability and security. Canada's security interests, at home and abroad, are directly affected by the illicit production of unspeakably destructive weapons. This is an ongoing concern, one we share with our allies and to which we have committed significant counter-proliferation expertise.

The 2011-2013 period was also significant for CSIS in that we contributed to the government's broader effort to achieve economic efficiencies. The public resources with which we are entrusted must be managed responsibly, and we undertook detailed reviews of all activities to ensure the benefits justify the expenses. The Service will continue to do its part to help reduce the federal deficit.

The professionalism of CSIS is reflected in the fusion of operational effectiveness and responsible administration. We appreciate the confidence the government invests in the Service, and it remains for us a privilege to protect Canadians and Canada's interests.

Michel Coulombe

TABLE OF CONTENTS

Message from the Interim Director 3

The Threat Environment 2011-2013 11
- **Terrorism** 11
- Terrorism at Home and Abroad 11
- Radicalization 12
- Al-Qaeda Core and Affiliates 13
- Somalia and Al Shabaab 14
- *AQAP, AQI and JN* 14
- *AQIM* 15
- Boko Haram and Ansaru 15
- Iran 15
- Hizballah 16
- Domestic and Multi-Issue Extremism 16
- Terrorist Financing and Financial Investigation 17

- **Espionage and Foreign Interference** 17
- Protecting Canadian Sovereignty 17
- Espionage Threats 18
- Foreign Interference 18

- **Cybersecurity and Critical Infrastructure Protection** 18

Weapons of Mass Destruction 20
- Chemical, Biological, Radiological, and Nuclear (CBRN) Weapons 20
  - *Iran* 21
  - *North Korea* 21
  - *Other CBRN Issues* 21

- **Looking Forward** 22

Portrait of a Terrorist Group: Al Shabaab 25
- *Fact box: A Canadian Concern* 27

The Rise of the Analyst 31
- Intelligence Analysis in a Changing World 31
- Responding to Changing Threats and Requirements 31
- A Core Group of Experts 32
- *Fact box: CSIS Analysts: Much More Than Writing* 33
- Working Within the Canadian Intelligence Community 33
- Supporting Foreign Partnerships 33

Security Screening Program **37**
Government Security Screening 37
Fact box: Government Screening Programs 38
Fact box: Screening in Action I 38
Immigration and Citizenship Screening 39
Fact box: Immigration and Citizenship Screening Programs 40
Fact box: Screening in Action II 40

At Home and Abroad **43**
Domestic Cooperation 43
Foreign Operations and International Cooperation 44
Fact box: Security Intelligence vs. Foreign Intelligence 46

An organization like no other **49**
Our People 49
Recruitment 50
Financial Resources 51

Review and Accountability **55**
The Minister of Public Safety 55
The Security Intelligence Review Committee (SIRC) 56
Fact box: The Inspector General (IG) 57
CSIS Internal Audit Branch/ Disclosure of Wrongdoing and Reprisal Protection 57
Access to Information and Privacy (ATIP) 58

Committed to Canadians 63
Community Engagement 63
Academic Outreach 64

Contact Us 68

Executive Organizational Chart 70

“IN TODAY’S COMPLEX WORLD, THREATS TO NATIONAL SECURITY ARE MULTI-FACETED AND CONSTANTLY EVOLVING.”

THE THREAT ENVIRONMENT 2011-2013

Canada, a multicultural and diverse nation with an abundance of natural resources, requires security to preserve the way of life enjoyed by those who live within its borders. In today's complex world, threats to national security are multi-faceted and constantly evolving. Under Canadian law, and specifically the *Canadian Security Intelligence Service (CSIS) Act*, the Service is required to investigate threats to the security of Canada. The following is a brief summary of the key threats to Canada between April 2011–April 2013.

Terrorism

Terrorism at home and abroad

The period between April 2011–April 2013 saw a considerable evolution in the domestic and international terrorist threat as well as a number of significant events. Within Canada, there were high-profile incidents of Canadians travelling abroad to engage in terrorist activities, as well as the notable arrests for an alleged terrorist plot to be carried out on Canadian soil. In the United States, terror attacks at the April 2013 Boston Marathon demonstrated the ongoing threat to the West from homegrown violent extremism.

Internationally, developments such as the death of Osama bin Laden in May 2011, Anwar Awlaki in September 2011, and other key leaders dealt significant blows to the Al-Qaeda (AQ) leadership. Despite these events, the threat from international terrorism remains significant. Terrorist movements in North and West Africa, Somalia, Iraq, Syria and elsewhere feature near daily violent attacks which kill numerous innocent civilians each year and destabilize regions, posing a threat to Canadian interests abroad. Other events, such as the July 2011 attacks in Norway carried out by the extremist Anders Breivik that killed 77 people, serve as a reminder that terrorism takes many forms and is not limited to unstable parts of the world.

In Canada, terrorism emanating from Al-Qaeda-inspired extremism remains a serious threat. Despite recent successful operations targeting Al-Qaeda Core, the Service continues to see support for AQ causes in Canada. Of particular significance is the above-mentioned investigation into an alleged Al-Qaeda-linked plot to attack a train in Southern Ontario, which led to the arrest of two individuals in April 2013.

It is important to note that although AQ-inspired extremism might at this moment in time represent the most visible terrorist threat to Canadian interests, historically terrorism in Canada has been committed in the name of a variety of ideologies.

There are at least three main ways in which terrorism threatens the safety and security of Canadians:

- First, terrorists continue to plot direct attacks against Canada and its allies at home and abroad with the aim of causing death and disruption;
- Second, terrorists seek to conduct activities on Canadian territory to support terrorism globally (such as fundraising to support attacks and militant groups);
- Third, terrorist supporters seek to radicalize individuals within Canada, some of whom may travel overseas for terrorist training or to engage in terrorism abroad. These individuals endanger their lives and pose a risk to the countries to which they have travelled. Further, should they return to Canada, it is uncertain to what ends these individuals may put their training. There is concern it may include attempting to radicalize others, or train individuals in terrorist methods.

CSIS works with its law enforcement partners and other government agencies in order to preserve the safety, security and way of life for all who live within our borders. Further, the Service is committed to supporting the Government of Canada's national counter-terrorism strategy, *Building Resilience Against Terrorism*, released in February 2012 and expanded upon in the *2013 Public Report on the Terrorist Threat to Canada*.

Radicalization

The radicalization of Canadians towards violent extremism continues to be a significant concern to Canadian national security. Essentially, radicalization is the process whereby individuals move from holding moderate, mainstream beliefs towards adopting extremist political or religious ideologies. Individuals who become radicalized may support or become involved in violent extremism. Activities can range from attack planning against Canadian targets, sending money or resources to support violent extremist groups, and/or influencing others (particularly youth) towards adopting radical ideologies. Radicalized individuals may also seek to travel abroad for terrorist training or to engage in fighting. Such individuals can pose very serious threats to the security of Canada. Not only are they now seasoned fighters who harness the ability to conduct attacks here, but they may also serve in influencing others.

The deaths of senior Al-Qaeda leaders, including Osama bin Laden, have not diminished the threat of international terrorism, a phenomenon that will continue to generate headlines in the coming year.

The participation of two young Canadians in an attack on an Algerian petroleum facility in January 2013 where up to 60 individuals died, as well as the widely-reported travel of two other young Canadians to North Africa, allegedly for extremist purposes, is indicative of this trend and highlights the challenge posed by the travel of radicalized individuals for terrorist purposes.

In order to generate a better understanding of the phenomenon, the Service conducts research on radicalization in Canada. CSIS has found that for those influenced by the AQ narrative, violent extremists have come from varied social and age levels, are spread widely across the educational spectrum and can appear fully integrated into society, making detection especially difficult.

Al-Qaeda Core and Affiliates

During 2011-2013, Al-Qaeda Core, based in Pakistan's tribal areas, experienced a series of major setbacks, including most importantly the death of its leader and founder, Osama bin Laden. This is in addition to the deaths or arrests of several other key AQ commanders and operatives, resulting from a potent and sustained counter-terrorism campaign led by the United States.

Moreover, AQ Core was caught off-guard by the political uprisings of the "Arab Spring", which largely rejected the Al-Qaeda narrative and message. During the period of this Report, AQ was initially absent and largely silent regarding the revolutions taking place. However, movements linked to AQ, or inspired by its narrative, have subsequently appeared in some Arab Spring countries. There is concern that the volatile security situation in some Arab countries as a result of the Arab Spring uprisings has now provided room for AQ and its affiliates to operate more freely.

Additionally, AQ Core has also been increasingly vocal about the Arab Spring. In early 2012, AQ leader Ayman al-Zawahiri released a video which called on jihadists in Syria and the wider region to join the fight against the Assad regime in Syria. In early April 2013, al-Zawahiri called upon all Muslims to unite in creed and actions, stating this is a "very crucial issue" for Muslims, especially as they enter a "new phase of empowerment and conquest" in the wake of the Arab Spring. These messages are typical of recent AQ releases which have adopted a more dogmatic stance: informing the revolutionaries of their duty to implement sharia law and seeking to situate geo-political events within a historical narrative shaped by AQ's worldview. Further, messages are evidence of al-Zawahiri's ongoing attempts to overcome leadership losses and operational weaknesses and reaffirm AQ's relevance and status as the vanguard of a global movement.

The Service assesses that AQ Core remains a dangerous terrorist group, which has thus far retained the intent to carry out spectacular attacks against the West and to influence individuals to do the same. The Service expects that AQ Core will remain based in the Afghan/Pakistan border tribal areas for the foreseeable future. This area is therefore likely to remain a significant source for terrorist activity that constitutes a threat to the security of Canada.

Somalia and Al Shabaab

Instability, terrorism, piracy and violence continue to plague the troubled African state of Somalia. The resulting problems which emanate from this region constitute significant threats to the security of Canada. In particular, the terrorist group Al Shabaab remains a substantial threat to regional security despite several setbacks it suffered between April 2011-April 2013, namely with the introduction of a Kenyan-led African Union force into Somalia. For example, in the spring of 2013, Al Shabaab was successful in launching several high-profile attacks in Mogadishu.

A number of Somali-Canadians have travelled to Somalia for terrorist training and to engage in violent jihad. Some of these individuals have reportedly been killed. In April 2013, a Canadian is reported to have taken part in the deadly attacks on Mogadishu's Benadir Courts which killed numerous individuals. For those who survive, there are concerns over the ends to which they may put their training. In October 2011 a Somali-American suicide bomber released an audiotape specifically calling upon "brothers and sisters" to engage in violent jihad in Canada. In April 2013, the Canadian government passed legislation which makes it illegal to leave Canada for the purpose of committing terrorism.

AQAP, AQI and JN

From 2011 until the summer of 2012, the Yemen-based Al-Qaeda in the Arabian Peninsula (AQAP) engaged in a short-term insurgency in the southern governorates of Abyan and Shabwah. While eventually forced to retreat, the group remains a significant terrorist threat focussed on carrying out attacks within Yemen and against the international community. Moreover, the group maintains the capacity and intent to carry out international plots when the opportunity presents itself. This was illustrated by the disruption of a second underwear plot by the Service's allied partners in May 2012, modeled on a similar failed plot by Umar Farouk Abdulmutallab in December 2009 which, had he been successful, might well have blown up a passenger jet enroute for Detroit over Canadian airspace.

AQAP's online magazine, *Inspire*, has continuously urged its audience to engage in lone-actor terrorism. A "Lone Mujahid Pocketbook", collecting advice and techniques from the 10 issues of *Inspire* Magazine, was published in March 2013.

Al-Qaeda in Iraq (AQI) remains a deadly force within Iraq although it lacks the support it would need amongst the general population to become a successful insurgency movement. Events in Syria, however, have provided AQI with new opportunities to challenge regional stability. AQI has provided support and operatives to Syria-based extremists and continued instability may eventually offer militant groups in Iraq increased freedom to operate in the region.

Jabhat al Nusra (JN) has emerged as an AQ node in Syria and one of the many groups fighting against President Bashar Al-Assad's regime. Recently, it openly pledged allegiance to AQ Core leader, Al Zawahiri. The threat posed by JN is complex. There is significant concern that extremism in Syria will result in a new generation of battle-hardened extremists who may seek to return to their home countries or export terrorism abroad.

AQIM

In North Africa, Al-Qaeda in the Islamic Maghreb (AQIM) continued to pursue a campaign of kidnapping and violence in the Sahel and North Africa, including the attack by an AQIM splinter group on an Algerian petroleum facility in January 2013 where up to 60 people died, and in which two suspected Canadian extremists participated. During 2011-2012, AQIM benefited from a Tuareg uprising in Northern Mali to increase its operational capacity, sanctuary and influence. AQIM has aligned itself with local extremist groups, and together they were able to effectively take control of most of Northern Mali. In light of growing concerns over the threat posed to regional stability with the consolidation of AQIM's territory, France militarily intervened in the country in December 2012, swiftly defeating the militants. Nevertheless, stability in the country will likely remain elusive for some time.

These developments have important implications for Canada as a number of Canadian businesses are based in Southern Mali and across the region, particularly in Nigeria. Additionally, Canada has a number of development projects in the Sahel region which may be at risk if the instability there continues.

Boko Haram and Ansaru

Within Nigeria, AQ-inspired Boko Haram and splinter group, Ansarul Muslimina Fi Biladis Sudan (Ansaru), engaged in a series of violent attacks in 2012, as well as several kidnappings against Western interests between December 2012 and February 2013. These violent actions demonstrate that Boko Haram and Ansaru pose a threat to Western interests in Nigeria. However, the February 2013 kidnapping of a French family by Boko Haram in Cameroon (allegedly in response to the French intervention in Mali) is a significant development as it represents a departure from past activities in Nigeria. Further, it suggests that these groups increasingly have the intent and the capacity to carry out operations outside of Nigeria.

Iran

Iran remains a leading counter-proliferation concern and state-sponsor of terrorism. Recently, a number of terrorist incidents have occurred or been foiled, all of which have been publically attributed to Iran's Islamic Revolutionary Guard Corps Qods Force (IRGC-QF) and/or Lebanese Hizballah.

In September 2012, the Government of Canada announced the closure of the Iranian Embassy and that it would designate the country as a sponsor of terrorism under the *Justice for Victims of Terrorism Act*.

Further, the Government of Canada listed the Islamic Revolutionary Guard Corps' Qods Force (IRGC-QF) as a terrorist entity under section 83.05 of the *Criminal Code* in December 2012.

Hizballah

Hizballah continues to be a major source of terrorism in the Middle East and has been listed as a terrorist entity in Canada since 2002. Hizballah has established networks in Lebanese Shia diaspora communities around the world, including Canada. The group has used these networks as mechanisms for fundraising, recruitment and logistical support. Notably, in 2013 Bulgarian authorities reported that a dual Lebanese-Canadian citizen had participated in the July 2012 Burgas Airport bombing linked to Hizballah. The Service is concerned that Hizballah may recruit and train other Canadian citizens to participate in similar plots.

During the period of review covered by this Report, Hizballah's main preoccupation was to maintain its influence over Lebanese political life while managing the fallout of the Syrian uprising. The improved quantity, lethality and sophistication of Hizballah's weapons systems have reinforced its dominance in the south of Lebanon and the Bekaa Valley, where the authority of the Lebanese Armed Forces is severely restricted. Hizballah maintains training camps, engages in weapons smuggling and also maintains an arsenal of thousands of rockets aimed at Israel.

Hizballah's increasing political role and military capabilities directly serve the geo-political interests of its Iranian and Syrian patrons. However, the uprising in Syria poses a significant logistical challenge to Hizballah, which is worried about the survival of President Assad's regime. Syria has served as a supply conduit for Hizballah and has been a facilitator of many of its activities. Further, Hizballah, Syria and Iran claim to act in unison as an "arc of resistance" against Israel, essentially, the raison d'être of the terrorist group. The fall of the Syrian regime would mean the loss to Hizballah of a key ally in the region. The Service assesses that Hizballah will continue to be a source of violence and disruption, posing a threat to Canadians and Canadian interests.

Domestic and Multi-Issue Extremism

Other forms of violence, motivated by ideology or political cause, also threaten Canadian national security. Domestic extremists in Canada are capable of orchestrating acts of serious violence. The 2010 firebombing of a Royal Bank branch in Ottawa, and the bombing of a military recruiting centre in Trois-Rivières, Quebec are just a few examples. Grievances harboured by those who oppose issues such as the perceived dehumanizing effects of capitalism are likely to continue and may trigger additional acts of serious violence.

Right-wing extremism has not been as significant a problem in Canada in recent years. Those who hold such extremist views have tended to be isolated and ineffective figures. However, the July 2011 bombing and shooting rampage in Norway, which killed 77 people, showed that

even a single individual can successfully execute mass-casualty terrorism.

Terrorist Financing and Financial Investigation

Terrorist organizations require finances and resources to recruit and train members, to distribute propaganda and to carry out their attacks. Every dollar denied to terrorists makes these actions more difficult and thus less likely to happen.

The economics of terrorism are complex. Terrorist funding is often transnational, and may involve many different players using a variety of techniques in order to achieve their desired goals. In order to counter such activity, counter-terrorism authorities need to work together. CSIS enjoys excellent relationships with domestic partners such as the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), the Royal Canadian Mounted Police (RCMP), the Canada Revenue Agency (CRA) as well as international partners.

When terrorist groups emerge, Canada can formally declare them as such and list the group as a terrorist entity under the *Criminal Code* of Canada. Once designated as a terrorist entity, the group's assets in Canada are frozen and any financial and material support to such designated entities constitutes a criminal offence. By partnering with other agencies and institutions, CSIS helps to maintain the efficiency and integrity of Canada's financial system, while at the same time remaining vigilant against any forms of terrorist financing or support.

Hostile foreign intelligence services are very active in Canada, seeking to obtain our economic, political and military secrets.

Espionage and Foreign Interference

Protecting Canadian Sovereignty

While counter-terrorism remains a priority for the Service, during 2011-2013 CSIS continued to investigate and advise the government on other threats to the security of Canada, including espionage and foreign interference. An increasingly competitive global marketplace that has fostered evolving regional and transnational relationships has also resulted in a number of threats to Canadian economic and strategic interests and assets.

Espionage Threats

A number of foreign intelligence services continue to gather political, economic, and military information in Canada through clandestine means. The recent case of Sub-Lieutenant Jeffrey Paul Delisle, who plead guilty in October 2012 to spying for Russia and was later sentenced to 20 years in prison, is an example of such activity.

Canada's advanced industrial and technological capabilities, combined with expertise in a number of sectors, make this country an attractive target for foreign intelligence services. Several sectors of the Canadian economy have been of particular interest to foreign agencies, including: aerospace, biotechnology, chemicals, communications, information technology, mining and metallurgy, nuclear energy, oil and gas, as well as the environment. The covert exploitation of these sectors by foreign powers as a means to advance their economic and strategic interests may come at the expense of Canada's interests and objectives. Some ramifications of this activity include lost jobs, corporate and tax revenues, and a diminished competitive advantage.

Canada, with its economic wealth and advanced infrastructure, offers attractive prospects to foreign investors. Corporate acquisitions by some foreign entities can pose risks related to the vulnerability of critical infrastructure, control over strategic sectors, espionage and foreign interference activities, and transfer of technology. One risk relates to the consequences that may fall from foreign state control over strategic resources and their potential access to sensitive technology. CSIS assesses that national security concerns related to foreign investments in Canada will continue to materialize, owing to the prominent role of State Owned Enterprises in the economic strategies of some foreign governments.

Foreign Interference

Canada, as an open, multicultural society, has traditionally been vulnerable to foreign interference activities. When diaspora groups in Canada are subjected to clandestine and deceptive manipulation by a foreign power in order for it to garner support for its policies and values, these activities constitute a threat to the security of Canada. As boundaries between foreign state and non-state actors become increasingly blurred, it is particularly challenging for intelligence services to differentiate between legitimate and illegitimate activities. Foreign interference in Canadian society – as a residual aspect of global or regional political and social conflicts, or divergent strategic and economic objectives – will continue in the coming years.

Cybersecurity and Critical Infrastructure Protection

Although attacks may come from the virtual realm, their consequences are very real. Increasingly, individuals, groups or organizations with malicious intentions are able to attack Canada without actually having to set foot on Canadian soil. These hostile actors can include both state and non-state actors: foreign intelligence agencies, terrorists,

"hacktivists" or simply individuals acting alone. Moreover, these hostile actors have access to a growing range of cyber-attack tools and techniques. Attackers have employed carefully crafted e-mails, social networking services and other vehicles to acquire government, corporate or personal data.

As technologies evolve and become more complex, so too do the challenges of detecting and protecting against cyber-attacks. Foreign intelligence agencies use the Internet to conduct espionage operations, as this is a relatively low-cost and low-risk way to obtain classified, proprietary or other sensitive information. There have been a significant number of attacks against a variety of agencies at the federal, provincial and even municipal level. The Government of Canada, like those of other countries, witnesses serious attempts to penetrate its networks on a daily basis.

CSIS is also aware of a wide range of targeting against the private sector in Canada. The main targets are high-technology industries, including the telecommunications sector. However, the Service is also aware of attacks against the oil and gas industry and other elements of the natural resource sector, as well as universities involved in research and development. In addition to stealing intellectual property, state-sponsored attackers seek information which will give their domestic companies a competitive edge over Canadian firms.

Technological advances in data storage and retrieval have produced a vulnerability: Cyber attackers can steal in an instant a warehouse of sensitive information.

Of particular importance are the different types of cyber-operations that may occur. On the one hand there are politically-motivated hacker collectives that will attempt to hijack computer networks to spread mischief or propagate false information (such as the hoax Twitter report in April 2013 from a hacked news organization of an attack on the White House). More serious are cyber-operations which attempt to achieve some sort of "gain", normally in the form of acquiring information which may be valuable in negotiations or sensitive and proprietary information.

However, there have also been recent cases of cyber-operations which do not seek "gain" other than to delete data irrevocably, or target critical infrastructure such as energy grids, communication networks, and financial systems. For example, the 2012 cyber-attacks on Saudi Aramco which shut down 30,000 computers was reportedly aimed at shutting down oil and gas production. A few days later RasGas in Qatar was hit by a similar attack. Any attack on infrastructure targets in Canada could disrupt our way of life in very significant ways. The security of supervisory control and data acquisition (SCADA) systems, upon which the public and private sectors depend, is becoming increasingly important. Should cyber-operations, such as the ones carried out against Saudi Aramco and RasGas, be targeted against systems in Canada, the impact could be severe and affect any and all areas of critical infrastructure, including those which affect water supply, energy and utilities, manufacturing, Internet communications technology or even gravely affect institutions such as schools and hospitals. Given the borderless and instantaneous nature of cyber transactions, foreign actors may stage an operation against a Canadian target in a very short period of time.

Because the threat from cyber-espionage, cyber-sabotage and other cyber-operations are part of a broader economic threat to key sectors of Canadian society, the Service works closely with other government departments and international partners in order to remain abreast of the global threat. As outlined in the Government of Canada's *Cyber Security Strategy*, the Service analyzes and investigates domestic and international threats to the security of Canada, responding to the evolution in cyber-security technologies and practices.

Weapons of Mass Destruction

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

The proliferation of chemical, biological, radiological and nuclear (CBRN) weapons, commonly referred to as weapons of mass destruction (WMD), and their delivery vehicles constitutes a significant threat to the security of Canada, its allies and the international community. Regardless of whether proliferation is carried out by state or non-state actors, the pursuit of WMD increases global tensions and may even precipitate armed conflicts. Canada is a party to many international conventions and other arrangements designed to stem the proliferation of WMD, and CSIS works closely with both domestic and foreign partners to uphold the nation's commitment to this cause.

Canada is a leader in many high technology areas, some of which are applicable to WMD programs. As a result, foreign entities seeking to advance WMD programs have targeted Canada in an attempt to obtain Canadian technology, materials and expertise. CSIS investigates these attempts to procure WMD technology within and through Canada, and in turn advises the government as to the nature of these efforts. CSIS actively monitors the progress of foreign WMD programs, both in their own right – as possible threats to national or international security – and in order to determine what proliferators may be seeking to acquire.

Iran

Iran is widely believed to be seeking the capability to produce nuclear weapons. It has continued to advance a uranium enrichment program despite widespread international condemnation, successive UN Security Council resolutions demanding that it cease such activity, and the imposition of increasingly severe economic and financial sanctions in response to its failure to comply. A November 2011 report of the International Atomic Energy Agency (IAEA) detailed past Iranian research applicable to the development of nuclear weapons and warned that such work could be continuing. In 2011-2012, Iran had enough enriched uranium, which, if further enriched to weapons grade, could be used for five nuclear weapons. These developments have raised tensions and increased the likelihood of a regional conflict which could severely impact the safety of Canadians, Canadian interests as well as our allies in the region.

North Korea

The death of Kim Jung Il in December 2011 and the rise of his son, Kim Jung Un, to the leadership of North Korea created uncertainty as to the future of the impoverished but aggressive nation. North Korea has shown no serious inclination to "denuclearize" as called for by the international community. North Korea continues to actively pursue the development of nuclear weapons and maintains a uranium enrichment program that could further add to its arsenal. Further, it is believed that North Korea is actively developing a new road-mobile, intercontinental ballistic missile (ICBM) capable of reaching North America.

In February 2012, North Korea reached an agreement with the United States to suspend long-range missile tests and uranium enrichment and admit UN inspectors in exchange for food aid. However, the agreement fell through after North Korea's unsuccessful test of a long-range missile under the guise of a space-launch vehicle (SLV) in April 2012. In December 2012, North Korea began deploying the launch vehicles for its KN-08 intercontinental ballistic missile (ICBM), which is in the late stage of development. Significantly, in February 2013, North Korea for the third time tested a nuclear explosive device, provoking international outrage and new sanctions on the country.

There is concern as to how this aggressive and unpredictable country may use its nuclear weapon capability in the future. North Korea's increasingly bellicose rhetoric in the spring of 2013 may be accompanied by further provocative actions in the near-term.

Other CBRN Issues

In South Asia, a principal concern remains the nuclear arsenal of Pakistan and questions over the security of those weapons systems given the domestic instability in that country. Unrest in the Arab world has also raised fears about the security of chemical weapons (CW) stocks in some countries, notably Syria. The international community remains intensely concerned that Syria's large stockpile of CW might find its way into the hands of terrorists or be used by the regime against its own people.

A number of terrorist groups have sought the ability to use CBRN materials as weapons. Some groups such as AQ have pursued efforts to cause mass casualties with biological agents such as anthrax, or improvised nuclear explosive devices. While the technological hurdles are significant, the possibility that a terrorist group could acquire crude capabilities of this kind cannot be discounted. Even a relatively unsophisticated use of chemical, biological or radioactive material in small-scale attacks could have a disruptive economic and psychological impact that could far outweigh the actual casualties inflicted.

Looking Forward

Canada is a relatively safe country with a harmonious society that has a strong sense of the fundamental values and freedoms embedded in our way of life. However, there are and will continue to be threats to our national security. Canadian interests are damaged by espionage activities through the loss of assets and leading-edge technology, the leaking of confidential government information or applications and the coercion and manipulation of ethno-cultural communities. Terrorism and radicalization threaten the loss of life at home and abroad. CSIS is committed to monitoring these threats and working with our domestic and international partners to ensure the safety and security of Canadians in an uncertain international environment.

> “THE RISE OF AL SHABAAB HAS BEEN QUICK AND THE GROUP CONTINUES TO TERRORIZE INNOCENT SOMALIS.”

PORTRAIT OF A TERRORIST GROUP: AL SHABAAB

Terrorism is a major threat to global security, and one of the geographic areas of greatest concern is the troubled African state of Somalia, the operating centre for the group Al Shabaab ("The Youth").

Al Shabaab initially operated as a militia affiliated with the Islamic Courts Union (ICU). In late 2006, after the ICU was defeated by a Western-backed Ethiopian military intervention, Al Shabaab evolved into its own distinct organization, controlling swathes of land in the southern and central parts of Somalia, including within the capital of Mogadishu. The group is committed to expelling all foreign presence from Somalia and transforming the country into an illiberal theocracy, governed by a radical interpretation of Islamic law.

Recently, Al Shabaab has suffered significant territorial losses and setbacks at the hands of African Union forces but the group continues to pose a threat. In February 2012, Al Shabaab announced that it had formally joined Al Qaeda (AQ). Subsequent reporting indicates that its members are actively fighting alongside Al Qaeda in the Arabian Peninsula in Yemen, and Al Shabaab has also been reported in having assisted Nigeria-based, Boko Haram – another terrorist organization.

The rise of Al Shabaab has been quick and the group continues to terrorize innocent Somalis. The attacks are brutal. In December 2009, Al Shabaab conducted a suicide attack on a medical school graduation ceremony at a hotel in Mogadishu, killing 21 people including a handful of government officials.

In July 2010, the group demonstrated its ability and willingness to attack outside Somalia when it carried out twin suicide bomb attacks in the Ugandan capital of Kampala. The attacks killed 76 people who had gathered to watch the FIFA World Cup final. Al Shabaab believes that watching sports on television is immoral.

In October 2011, suspected Al Shabaab militants kidnapped a French woman, Marie Dedieu, from a beachfront residence in Kenya. Though kidnapping is not a unique tactic, this incident was especially cruel. Ms. Dedieu was dependent on a wheelchair and medication. She died a few weeks later in captivity. In April 2013, Al Shabaab orchestrated a bloody attack on a courthouse in Mogadishu that made headlines around the world and showed that the group is still very much in business.

Al Shabaab has banned international aid agencies, including the UN and Red Cross, from operating in areas it controls. In November 2011, the group raided and seized control of several facilities preventing the distribution of much needed aid to Somalis.

Of particular concern is the success of Al Shabaab's recruitment campaign. The group's use of the Internet and new media such as Twitter, coupled with the promise of adventure and purpose, has enabled the group to attract recruits from around the world, including those from Somali diaspora communities. Since 2009, the group has been soliciting support from abroad by presenting its campaign in Somalia as a front in the global jihad.

Numerous young Canadians have been lured by this dangerous message and have travelled to Somalia for terrorist training, a disturbing phenomenon that has also been seen in the US and in other Western countries with a Somali diaspora. There have been reports that some of these individuals, including Canadians, have been killed as a result. In October 2011 an alleged Al Shabaab suicide bomber delivered a message specifically calling for attacks inside Canada, among other countries.

Groups such as Al Shabaab, AQ, and those affiliated with AQ continue to train terrorists and to encourage supporters around the world to carry out attacks against Western targets. The recruitment of Western citizens to participate in terrorist acts benefits these groups, because such operatives have easy access to Europe and North America.

These are all clear reasons why the Government of Canada listed Al Shabaab as a terrorist entity in March 2010. In fact, the group has been listed by many Western countries, including the US, the UK, Australia and others. But make no mistake, Al Shabaab doesn't just pose an isolated threat to security afar in its own geographic surroundings – the threat to Canada and Canadian interests is very real. Somali-Canadians are rightly worried about the influence and reach of this group, and the national security community – including CSIS – is committed to helping families and communities keep their children from pursuing a path that can have no good outcome.

Al Shabaab is not the only foreign terrorist movement that has attracted Canadian recruits. The phenomenon of young Canadians travelling abroad to participate in terrorist activities is a serious security concern, not least because these young people could return to Canada more deeply radicalized and with combat experience.

A CANADIAN CONCERN

CSIS HAS PUBLICLY EXPRESSED ALARM – WE DO SO AGAIN IN THIS REPORT – ABOUT THE INCREASING NUMBER OF CANADIAN CITIZENS OR RESIDENTS WHO LEAVE THE COUNTRY TO PARTICIPATE IN TERRORIST ACTIVITIES ABROAD. SOMETIMES THE QUESTION IS ASKED WHY CANADA SHOULD BE SO CONCERNED ABOUT THIS PHENOMENON, ESPECIALLY WHEN THE WOULD-BE TERRORISTS HAVE A GOOD CHANCE OF GETTING KILLED IN THEIR FOREIGN DESTINATION. IS IT NOT BETTER TO HAVE VIOLENT EXTREMISTS LEAVE CANADA RATHER THAN STAY?

THE ANSWER IS THAT NO COUNTRY CAN BECOME AN UNWITTING EXPORTER OF TERRORISM WITHOUT SUFFERING DAMAGE TO ITS INTERNATIONAL IMAGE AND RELATIONS. CANADA'S LEGAL OBLIGATIONS TO PROMOTE GLOBAL SECURITY NEED TO BE HONOURED, AND THAT MEANS ASSUMING RESPONSIBILITY FOR OUR OWN. A CANADIAN WHO TRAVELS TO COMMIT TERRORISM IS STILL VERY MUCH A CANADIAN "PROBLEM."

THERE IS ALSO THE SPECTRE THAT SUCH INDIVIDUALS WILL RETURN TO CANADA MORE DEEPLY RADICALIZED THAN WHEN THEY LEFT. MOST TROUBLING, IF THEY PARTICIPATE IN A FOREIGN CONFLICT OR TRAIN WITH A TERRORIST GROUP, THEY MIGHT RETURN WITH CERTAIN OPERATIONAL SKILLS THAT CAN BE DEPLOYED THEMSELVES OR TAUGHT TO FELLOW CANADIAN EXTREMISTS. EITHER WAY, THIS IS A SERIOUS SECURITY THREAT TO CANADA.

“THE CANADIAN SECURITY INTELLIGENCE SERVICE DOES MORE THAN DETECT THREATS TO OUR NATIONAL INTERESTS. WE ALSO SEEK TO UNDERSTAND THOSE THREATS, AND EVEN TO ANTICIPATE THEM BEFORE THEY MATERIALIZE.”

THE RISE OF THE ANALYST

Intelligence Analysis in a Changing World

The Canadian Security Intelligence Service does more than detect threats to our national interests. We also seek to understand those threats, and even to anticipate them before they materialize. That's where the role of the analyst comes in. The complexity of today's threat environment – and the speed at which it can change, owing to technology among other factors – requires an increasingly sophisticated response on our part.

The intelligence analyst surveys the crowded landscape of information, both classified and unclassified, and from that jungle of data he or she identifies the shape of things that policy-makers need to worry about. At more than any other point in our country's history, leaders are relying upon good intelligence analysis to help inform their decision-making process. In today's security context, insight is as valuable as information.

CSIS generates a number of intelligence products, ranging from raw ("non-assessed") intelligence to broader, strategic analysis of topical or regional-based threats.

The Integrated Terrorism Assessment Centre (ITAC), located within CSIS National Headquarters in Ottawa, produces threat assessments and tactical reports, frequently in response to threat incidents or fast-developing issues. ITAC is staffed by representatives from a number of federal government departments.

The Intelligence Assessments Branch (IAB) houses the core of the Service's analytical expertise. IAB provides timely and focused intelligence which meets the Government of Canada's stated priorities. Within the Service, IAB is responsible for prioritizing and integrating intelligence requirements. IAB analysts are leading subject-matter experts in their respective areas, from the radicalization process to the geopolitics of North Africa, and this expertise supports the front line operational work. That is to say, analysis is playing an increasingly important role in guiding our operations and intelligence collection.

Responding to Changing Threats and Requirements

In the course of an average day, any number of threat-related incidents around the world – many of which have a direct or indirect impact on Canada – will receive public attention and generate questions from political officials and other decision-makers. Intelligence agencies must be prepared to respond to those questions by delivering quick and concise analysis, all the while being mindful of the bigger and longer term picture as well.

At any given moment, CSIS is managing dozens of priority operations. In some cases, threats evolve day-to-day, while in others, steady patterns

of activity are monitored and noted. Whether it is an initial assessment following a terrorist attack or an analysis of recent trends in espionage, the Service has worked to improve its ability to deliver the right intelligence product to its government clients in a timely manner.

Raw intelligence reporting is disseminated in order to provide a snapshot of a threat-related issue. This is different from a *threat assessment*, which typically offers a synopsis of the immediate situation. Both raw intelligence reporting and threat assessments are designed to answer short-term questions. There is, however, a need for in-depth assessments that contextualize the issue and tell the reader why it is significant for Canada. These are *strategic intelligence assessments*, which draw upon CSIS reporting, foreign agency information and open-source material and serve to provide government officials with a holistic picture of the threat and its potential consequences for Canada. Strategic intelligence assessments not only answer questions about what happened yesterday but they also throw light on what might happen in the coming weeks or months – and what that might mean for Canada's national security. Strategic intelligence assessments play a key role in identifying emerging trends and, in some cases, linking those trends or actors to recent events in Canada or abroad.

CSIS produces other assessments as well, providing government clients with an analysis of the potential threats to a physical installation, facility, or organization. But the pressing demands of the immediate threat environment have not detracted from the Service's requirement to look down the road – even around the corner – so that we can better assess how regional or global events, organizational dynamics, and individual actors might have an impact on the security of Canada over the long term. While CSIS is not in the business of predicting the future, we recognize that embryonic trends in today's threat landscape may develop into dominant realities over the next year or decade, and it is imperative to identify and prepare for them.

A Core Group of Experts

Effective intelligence analysis requires an integrated team approach – from the investigators who collect the information, to the analysts who make sense of the intelligence and, finally, to the individuals who ensure that the final product gets to the right people at the right time. More than ever, decision-makers are demanding high-quality intelligence analysis to identify trends or threats that have a direct impact on the security of Canada. They are increasingly recognizing the value of CSIS analysis to meet those objectives.

As with many other security and intelligence services, CSIS has worked to improve both the quality and timeliness of its analytical product for government clients. Quality-control is essential: the consequences of providing our government with inaccurate information or analysis could be severe. In recent years, we have attracted a number of subject-matter experts from the public and private sectors, with varying backgrounds and skill-sets. The tactical analysts and strategic analysts who form the core of the Service's analytical expertise are relied upon to produce analysis, identify intelligence gaps, and carry out a variety of other activities in support of the Service's mandate. This is no easy task. It requires in-depth knowledge of the subject, a thorough understanding of how to evaluate the intelligence, and a mastery of the various analytical tools used to produce intelligence assessments.

CSIS ANALYSTS: MUCH MORE THAN WRITING

CSIS ANALYSTS PERFORM A WIDE RANGE OF FUNCTIONS ABOVE AND BEYOND WRITING ASSESSMENT PRODUCTS. RECOGNIZED WITHIN OUR GOVERNMENT AS EXPERTS IN THEIR FIELDS, CSIS STRATEGIC ANALYSTS ARE BEING CALLED UPON INCREASINGLY TO BRIEF SENIOR DECISION-MAKERS AND OTHER LEVELS OF GOVERNMENT ON SPECIFIC ISSUES; DELIVER PRESENTATIONS TO THE PRIVATE SECTOR AND ACADEMIA; AND LIAISE WITH OTHER GOVERNMENT PERSONNEL ON A VARIETY OF ISSUES. ANALYSTS SERVE ANOTHER IMPORTANT ORGANIZATIONAL ROLE BY PROVIDING STRATEGIC INSIGHT, IDENTIFYING INTELLIGENCE GAPS, AND RENDERING OTHER FORMS OF SUPPORT TO OUR INTELLIGENCE OFFICERS IN THE FIELD AND TO CSIS SENIOR MANAGEMENT.

Working Within the Canadian Intelligence Community

The complexity of the threat environment and the volume of open-source and classified information have reinforced the need to develop inter-agency cooperation in Canada. Members of the Canadian intelligence community continue to work on ways to better coordinate their activities and provide the best product to decision-makers. CSIS analysts work closely with intelligence analysts from other Government of Canada departments, producing community assessments and participating regularly in discussions on issues identified as intelligence priorities. Decision-makers expect the intelligence community to produce comprehensive and coherent analysis. Collaboration and the sharing of best-practices across agencies have advanced this objective.

Supporting Foreign Partnerships

CSIS maintains robust intelligence partnerships with a number of foreign agencies around the world. While much of the business of inter-agency partnerships involves information-sharing on specific threats and targets, the exchange of intelligence analysis is playing an increasingly important role in the Service's international relationships. CSIS analytical products have a reputation for excellence among our foreign partners, and they have helped to facilitate collaboration with foreign agencies and multinational organizations on key threat-related issues. CSIS analysts – often acting as ambassadors of the Service – play the additionally important role of liaising with foreign agency partners on key strategic issues, briefing representatives of foreign agencies and international organizations, and carrying out other duties calling for subject-matter expertise.

> DURING 2011-2013, THE SECURITY SCREENING PROGRAM REMAINED ONE OF THE MOST VISIBLE OPERATIONAL ACTIVITIES UNDERTAKEN BY THE SERVICE.

SECURITY SCREENING PROGRAM

The CSIS Security Screening program plays a key role in defending Canada from the threats of terrorism and extremism, espionage, and the proliferation of weapons of mass destruction. The program prevents individuals who pose a threat to the security of Canada from entering or obtaining status in Canada or from obtaining access to sensitive sites, government assets or information.

In both 2011-2012 and 2012-2013, the Security Screening program remained one of the most visible operational activities undertaken by the Service. During those two years, CSIS received more than 870,000 Security Screening requests from a wide variety of government clients.

Government Security Screening

The Government Security Screening program conducts investigations and provides security assessments under the authority of sections 13 and 15 of the *CSIS Act*. These assessments form an integral part of the decision-making process required for the issuance of security and site access clearances required for employees of the Government of Canada, or for persons under contract to a federal government department requiring lawful access to classified government assets or information.

CSIS security assessments address national security concerns as defined in Section 2 of the *CSIS Act*, criteria set out in the federal Policy on Government Security (PGS), and requirements established by other clients under a variety of legislative authorities. Notwithstanding CSIS security assessments, however, the PGS gives these departments and institutions exclusive authority to grant or deny such clearances.

CSIS Government Security Screening also supports a variety of programs relating to sensitive sites such as: airports and marine facilities, the Parliamentary Precinct and nuclear power facilities. It also plays an integral role in providing assessments for the Free and Secure Trade (FAST) program which seeks to ease access for both American and Canadian-based commercial drivers across our shared border.

Finally, under reciprocal screening agreements, CSIS may provide security assessments to foreign governments and international organizations (such as NATO) concerning Canadians being considered for positions requiring classified access to information or sites in a foreign country. Canadian citizens, about whom information is being provided, must give their consent in advance and all screening arrangements with foreign entities are approved by the Minister of Public Safety after consultation with the Minister of Foreign Affairs.

Government Screening Programs

Requests received *	2010-2011	2011-2012	2012-2013
Federal Government Departments	54,400	58,800	51,200
Free and Secure Trade (FAST)	31,800	13,900	12,600
Transport Canada (Marine and Airport)	35,100	40,100	39,500
Parliamentary Precinct	1,400	1,200	970
Nuclear Facilities	12,500	11,200	7,000
Provinces	260	260	330
Site Access–Others	2,500	5,200	4,400
Special Events Accreditation	24,200	2,000	940
Foreign Screening	500	480	460

* Figures have been rounded.

SCREENING IN ACTION I

WHILE CONDUCTING A SECURITY SCREENING INVESTIGATION, CSIS LEARNED THAT AN INDIVIDUAL WITH ACCESS TO A SENSITIVE FACILITY WAS ENGAGED IN ACTIVITIES THAT POSED A THREAT TO THE SECURITY OF CANADA. THE INVESTIGATION REVEALED THAT THE SUBJECT CONCERNED WAS PROVIDING ASSISTANCE IN A CLANDESTINE MANNER TO A FOREIGN STATE ENGAGED IN FOREIGN INFLUENCE ACTIVITIES AS DEFINED BY SECTION 2(B) OF THE *CSIS ACT*. THE REQUESTING AGENCY ACCEPTED THE SERVICE'S ASSESSMENT AND SUBSEQUENTLY REMOVED THE INDIVIDUAL'S ACCESS.

Immigration and Citizenship Screening

CSIS's Immigration and Citizenship Screening Program is a key component of the Service's Security Screening program. As part of its mandate under the authority of sections 14 and 15 of the *CSIS Act*, CSIS conducts investigations in order to assist the Government of Canada in preventing non-Canadians who pose a threat to national security from entering or obtaining status in Canada. In carrying out this mandate, CSIS works closely with the Canada Border Services Agency (CBSA) and Citizenship and Immigration Canada (CIC) in order to provide security related advice. These CSIS activities are conducted in support of the *Immigration and Refugee Protection Act* (IRPA) and the *Citizenship Act*.

CSIS also works with Government of Canada partners in reviewing security aspects of the immigration system to ensure that the Service's security screening operations remain efficient and effective, and that its advice is relevant and timely. In an effort to meet increasing demands, CSIS continues to refine business processes and exploit new technologies, with the aim of finding efficiencies and eliminating redundancies.

In order to fulfill its mandate, CSIS conducts its immigration screening investigations both in Canada and abroad. The Immigration Screening Program is divided into the following business lines: applications for permanent residence from within Canada and abroad; applications for temporary resident visas; applications for Canadian citizenship; and refugee claims, both inland and abroad.

CSIS screening activities have helped many immigrants and refugees begin new lives in Canada.

Immigration and Citizenship Screening Programs

Requests received*	2010-2011	2011-2012	2012-2013
Permanent Residents Within and Outside Canada	79,600	83,200	76,200
Front End Screening**	17,400	18,300	12,400
Citizenship Applications	198,800	205,000	121,800
Visitors Visa Vetting	71,400	58,200	44,800

* Figures have been rounded.

** Individuals claiming refugee status in Canada or at ports of entry.

SCREENING IN ACTION II

IN JULY 2011, THE SERVICE RECEIVED FROM CITIZENSHIP AND IMMIGRATION CANADA (CIC) A TEMPORARY RESIDENT VISA (TRV) APPLICATION FROM AN INDIVIDUAL IN SOUTH EAST ASIA. AN INVESTIGATION OF THE APPLICANT UNDER SECTION 15 OF THE *CSIS ACT* REVEALED LINKS TO TERRORISM AND THE SERVICE ADVISED ACCORDINGLY. CIC EVENTUALLY DEEMED THE PERSON INADMISSIBLE TO CANADA UNDER SECTION 34(1)C OF THE *IMMIGRATION AND REFUGEE PROTECTION ACT* (IRPA) AS HAVING "ENGAGED IN TERRORISM".

> CANADA IS A GLOBAL ENTITY WITH INTERESTS AND EQUITIES AT RISK FROM TERRORISM, CRIMINALITY AND HOSTILE INTELLIGENCE AGENCIES.

AT HOME AND ABROAD

Domestic Cooperation

CSIS is a true national service, and, as such, its resources and personnel are geographically dispersed across Canada. The CSIS National Headquarters is located in Ottawa, with Regional Offices in Halifax, Montreal, Ottawa, Toronto, Edmonton and Burnaby. CSIS also has District Offices in St. John's, Fredericton, Quebec City, Niagara Falls, Windsor, Winnipeg, Regina and Calgary.

The geographic configuration allows the Service to closely liaise with its numerous federal, provincial and municipal partners on security issues of mutual interest.

Additionally, CSIS has several Airport District Offices, including those at Toronto's Pearson International Airport and at Vancouver's International Airport. These offices support aviation security, and assist CIC and CBSA on national security issues. The CSIS Airport District Offices also provide information to their respective CSIS Regional Offices and to CSIS Headquarters, and liaise with other federal government departments and agencies that have a presence within Canada's airports.

During 2011-2013, CSIS continued to share information on security issues with a wide variety of domestic partners. A key component of CSIS cooperation with its domestic partners remains the production and dissemination of intelligence reports and assessments such as those drafted by the Service's Intelligence Assessments Branch and Canada's Integrated Terrorism Assessment Centre, which is housed within CSIS headquarters.

One of CSIS's most important domestic partners is the Royal Canadian Mounted Police (RCMP). Because CSIS is a civilian agency without the powers of arrest, it will alert the RCMP to security threats that rise to the level of criminality, whereupon the RCMP can initiate their own investigation and lay charges if appropriate. CSIS collects intelligence whereas law inforcement–the RCMP–collect evidence for criminal prosecution.

In 2011-2012, CSIS and the RCMP continued to develop a series of protocols on information-sharing. There is a growing body of Canadian jurisprudence in this area, which the Department of Justice and the Public Prosecution Service of Canada have helped interpret for CSIS and the RCMP. The goal is to ensure that both organizations work together in a way that enhances the national security of Canada while at the same time respecting their respective legislative mandates.

To ensure that CSIS is in both practice and spirit a national service, intelligence officers get to live and work in different regions of the country during the course of their careers. One benefit of a CSIS career is the opportunity it provides to see Canada from coast-to-coast-to-coast.

Foreign Operations and International Cooperation

Over the past decade, world events have demonstrated that the threats of terrorism and espionage are not restricted by national borders. Many of the national security challenges facing Canada originate from or have a strong nexus to events, foreign governments, individuals and groups overseas.

Globalization has led to enhanced and more complex security threats from terrorism, other unlawful and violent extremist activity, espionage, weapons proliferation, illegal immigration, cyber-attacks and other acts targeting Canadians domestically and abroad. Canada's global presence in industry, diplomacy and as travellers of the world further compounds these threats and often results in its citizens and interests being targeted or threatened by terrorist groups and hostile foreign intelligence agencies.

The international dimension of terrorism manifested in Canada is continuously demonstrated by the fact that foreign terrorists continue to inspire and provide direction to individuals and groups in Canada. Some Canadians and residents of Canada have left the country to seek training in terrorist camps in Somalia, Pakistan and elsewhere in an attempt to support or conduct terrorist operations within Canada or abroad. Additionally, over the past several years, Canadians have been kidnapped in places such as Colombia, Iraq, Afghanistan, Somalia, Kenya, Pakistan, Niger, and Sudan. Numerous Canadian businesses, their workers and Canadian diplomats abroad have also been targeted or threatened.

The intent of the *CSIS Act* and, indeed, the expectations of Canadians, necessitates that CSIS is vigorously pursuing the collection of security intelligence wherever that intelligence can be obtained, be it in Canada or overseas. As a result, CSIS has enhanced and continues to maintain an international presence. In today's global environment, CSIS liaison and cooperation with its international partners remains a crucial component of our country's ability to effectively investigate, assess and counter threats to Canada and its interests.

CSIS has officers stationed in cities and capitals around the world. Their primary function is to collect and, where appropriate, share security intelligence information related to threats to Canada, its interests and its allies with partner agencies. CSIS officers stationed abroad also provide security screening support to Canada's Citizenship and Immigration (CIC) offices and to the security programs of the Department of Foreign Affairs, Trade and Development Canada (DFATD).

Occasionally, the Service is required to send Canada-based officers abroad to respond to certain extraordinary situations. For instance, CSIS efforts have provided assistance in the evacuations of Canadians from regions in turmoil. CSIS officers, at considerable personal risk, have been dispatched to unstable countries and dangerous situations around the globe. The training, expertise and commitment of CSIS personnel is well-known in the global intelligence community.

The intelligence collected by CSIS during 2011-2013 has assisted Canadian government agencies to restrict entry to Canada of

individuals who represent threats to Canadian security interests. CSIS's efforts have also cast light on the intentions and capabilities of terrorist groups and hostile intelligence agencies that seek to target Canadians, Canadian interests and the interests of our allies.

As of March 31, 2013, CSIS had more than 280 arrangements with foreign agencies or international organizations in some 150 countries and territories. This includes four new foreign arrangements approved during the 2012-2013 fiscal year by the Minister of Public Safety following consultation with the Minister of Foreign Affairs as required under Section 17 (1)(b) of the *CSIS Act*. Of those arrangements, some 60 were defined as 'Dormant' by CSIS (meaning there have been no exchanges for a period of one year or more). Additionally, CSIS continued to restrict contact with eleven foreign entities due to ongoing concerns over the reliability or human rights reputations of the agencies in question, while two arrangements remained in abeyance pending an assessment of the agency's future. Finally, one arrangement was terminated following the dissolution of the foreign agency.

For reasons of security and privacy, the Service does not publicly divulge details of the information it exchanges nor does it identify the foreign agencies in question. CSIS must protect its foreign arrangements in order to keep the relationships viable and secure. Foreign agencies expect that the information they provide to CSIS will remain confidential, just as the Service expects that any information it provides to foreign agencies will not be divulged or disseminated to a third party without the Service's prior consent.

Canada is a global entity with interests and equities at risk from terrorism, criminality and hostile intelligence agencies. The international mosaic which helps sustain Canada as a strong, healthy nation has, at times, revealed direct associations between international terrorist groups and Canadian-based citizens and residents. These represent national security concerns which require an international response, both in terms of information sharing and collection of intelligence outside of Canada. CSIS is positioned and committed to pursuing its mandate to collect security intelligence, in Canada or overseas, in support of protecting Canadians, Canadian interests and the interests of our international partners.

SECURITY INTELLIGENCE VS FOREIGN INTELLIGENCE

CSIS HAS A LEGAL MANDATE TO COLLECT BOTH "SECURITY" INTELLIGENCE AND "FOREIGN" INTELLIGENCE, THOUGH THE DISTINCTION BETWEEN THE TWO IS NOT WIDELY UNDERSTOOD.

SECURITY INTELLIGENCE REFERS TO INFORMATION ABOUT THREATS TO THE SECURITY OF CANADA, SUCH AS TERRORISM AND ESPIONAGE. THE MAJORITY OF RESOURCES AND ACTIVITIES AT CSIS FOCUS ON THE COLLECTION OF SECURITY INTELLIGENCE, AS OUTLINED IN SECTION 2 OF THE *CSIS ACT*. OUR LEGAL MANDATE DOES NOT IMPOSE GEOGRAPHIC LIMITATIONS ON WHERE WE CAN COLLECT SECURITY INTELLIGENCE. THREATS TO NATIONAL SECURITY CAN ORIGINATE ANYWHERE IN THE WORLD, AND THE SERVICE FOLLOWS THOSE THREATS. OUR PERSONNEL HAVE BEEN DEPLOYED TO MANY DESTINATIONS OUTSIDE CANADA FOR THIS PURPOSE.

FOREIGN INTELLIGENCE, ON THE OTHER HAND, IS INFORMATION ABOUT THE CAPABILITIES, INTENTIONS AND ACTIVITIES OF FOREIGN STATES OR ENTITIES. THIS TYPE OF INTELLIGENCE IS OFTEN COLLECTED TO ADVANCE OR PROTECT NATIONAL INTERESTS. CSIS CAN COLLECT FOREIGN INTELLIGENCE UNDER THE AUTHORITY OF SECTION 16 OF THE *CSIS ACT* BUT ONLY WITHIN CANADA AND WITH APPROVAL OF THE MINISTER OF PUBLIC SAFETY, BASED UPON A WRITTEN REQUEST BY EITHER THE MINISTER OF FOREIGN AFFAIRS OR THE MINISTER OF DEFENCE.

“CSIS IS RECOGNIZED AS AN EMPLOYER OF CHOICE, NOT JUST BECAUSE THE WORK IS INHERENTLY INTERESTING BUT BECAUSE WE HAVE A PROGRESSIVE WORKPLACE CULTURE.”

AN ORGANIZATION LIKE NO OTHER

Our People

The CSIS workforce is remarkably diverse, employing individuals in a variety of different settings. We have employees working as Intelligence Officers (IOs), Surveillants, Translators, Information Management Analysts and Administrative support to name a few. A complex organization such as CSIS requires an equally complex staffing regime.

At the beginning of the 2013 fiscal year, CSIS had more than 3,200 full time equivalents (FTEs) split evenly along the gender line. Collectively, our employees speak 107 languages. 75 per cent of our employees speak both official languages and 20 per cent have a good or excellent knowledge of a foreign language other than English or French. With respect to age demographics, four generations of workers can be found in our offices and the average age of our employees is 41.7 years.

CSIS is recognized as an employer of choice, not just because the work is inherently interesting but because we have a progressive workplace culture. For five years running, the organization has been named one of Canada's Top 100 Employers. The Service has also been named one of the National Capital Region Top Employers for six consecutive years and finally, for the fourth year in a row, we were selected as one of the Top Employers for Canadians over 40.

CSIS is a career employer. Employees of the Service are recognized for their skills, talents and contributions which is reflected in our ability to retain our top talent. For the fiscal year 2012-2013, we recorded a resignation rate of only 0.8 per cent. In fact, the resignation rate has hovered around the 1 per cent mark for the last ten years.

As a knowledge-based organization, CSIS continues to invest in ongoing learning for all employees. All employees benefit from an integrated corporate training and development regime called the Entry-to-Exit Training Framework (EET). As an extension to the EET Framework, Learning Paths for all occupational groups are accessible to all employees via the Service's Intranet. The Learning Paths have also been integrated with another HR initiative entitled "Career Navigator" which provides a one stop shop for employees to review the position profile, education criteria for any position in the Service. These tools assist employees to take control of their own career path.

E-learning is another critical element of the Service's new blended learning approach, which seeks to make the best possible use of various learning methods (e.g. videoconference, mentoring, instructor-led courses). ELITE, a new online learning tool, allows access to both

self-paced and live virtual online courses directly from an employee's corporate desktop. ELITE will supply internal courses designed by Training and Development and courses supplied by partner agencies and outside vendors. Access to ELITE will be 24/7.

In 2012, a new Talent Management (TM) Branch was established to support the development and maintenance of a high-performing workforce in the Service. Led by a director general, the new TM Branch supports the development of four key groups in the Service: 1) Executives, 2) Participants in the Leadership Development Program (LDP), 3) Managers and supervisors, and 4) Employees. A TM Framework was elaborated with a focus on talent analytics, onboarding, performance management, training and development, succession planning, and career management.

The Service remains committed to the principles of Public Service Renewal. This engagement stems from the belief that the best way to fulfill our mandate to protect national security is to create and nurture a respectful and innovative work environment where employee engagement is high and performance excellence is the norm.

Recruitment

With its reputation as an "employer of choice", coupled with enhanced recruiting activities and targeted ads over the past year, more potential applicants have begun to take notice of CSIS and its various career opportunities.

CSIS is committed to building an organization reflective of Canada's rich cultural mosaic and as such we continue to promote a better understanding of our role, mandate and career opportunities available. In 2011, CSIS welcomed a Proactive Aboriginal Recruiter whose main role is to reach out to Aboriginal, First Nation and Inuit communities throughout Canada. This is the first time in CSIS's history that we have assigned someone to proactively reach out and promote our careers in these communities.

Our microsite also saw some enhancements this year with **csiscareers.ca** replacing the former **intelligencematters.ca** as a means to simplify our web address and to further correlate with our brand messaging. This microsite is the main portal of information for potential applicants, who can also apply for CSIS positions online and we are committed to ensuring that it remains a relevant and useful resource for our potential applicants.

Our drive-to-web marketing strategy is effective and has attracted impressive traffic. The overall number of CSIS applicants applying online has more than quadrupled in 2012-2013 (52,126) compared to 2009-2010 (12,887). Also, from September 1, 2012 to March 30, 2013 csiscareers.ca received 537,557 unique visitors for a total of 798,182 visits, and more than 4 million page views.

CSIS continues to explore ways of building our brand and recruiting messaging using social media such as Facebook, LinkedIn, Twitter and YouTube. In September 2011, six recruiting videos were posted to YouTube. Reaction to the videos was extremely positive as by March

31, 2013 the videos had received more than 100,000 views. In 2012, CSIS posted an advertisement on LinkedIn to reach out to potential IT applicants. Our click-through rate was higher than industry standards as hundreds of applicants from LinkedIn applied for IT positions though csiscareers.ca.

Social media is a low cost alternative to reach our potential applicants and growing in popularity every year.

Financial Resources

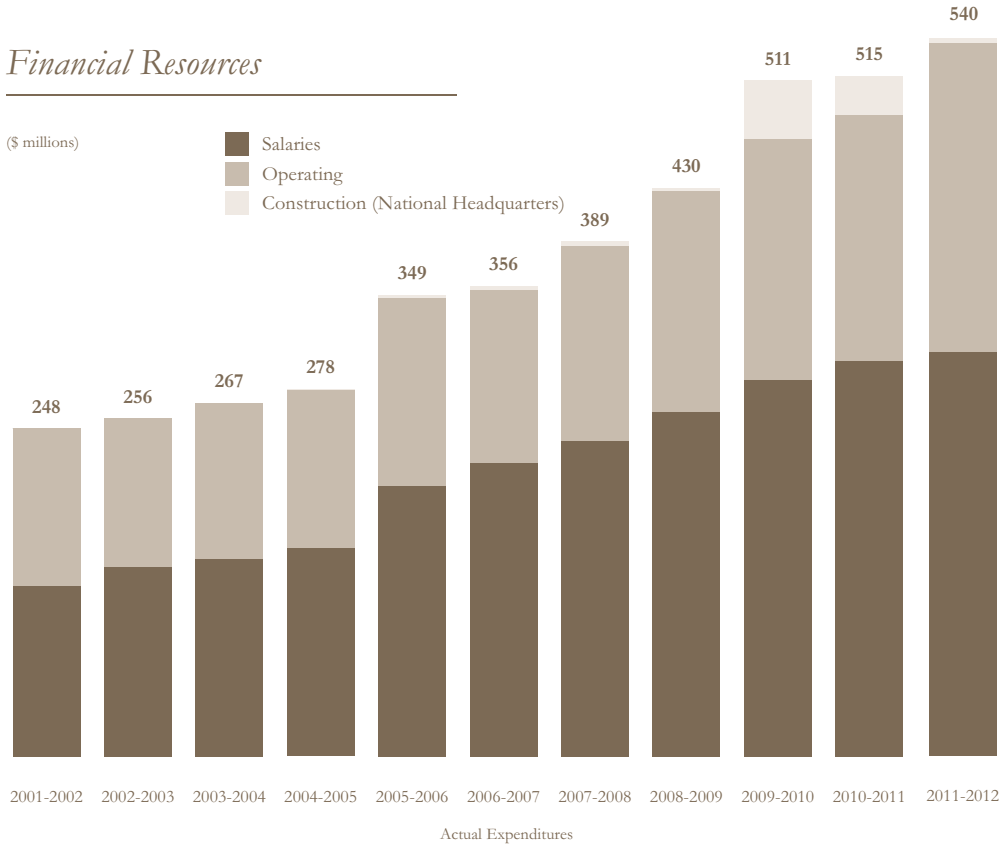
CSIS's final expenditures for 2011-2012, the last period for which figures are available, totalled $540 million.

The Service's financial resources increased from 2001-2002 to 2012-2013, partly as a result of new funding for public security and anti-terrorism initiatives allocated in the December 2001 Federal Budget. Funding was also provided to augment the Service's foreign collection capabilities, to administer Canada's Integrated Terrorism Assessment Centre, to help CSIS maintain its operational capacity both domestically and abroad, to expand its National Headquarters and to bolster existing capacities to combat terrorist financing. Furthermore, in 2010-2011, new funding was announced for CSIS to address its most acute program integrity needs.

The Service was subject to a stringent review process dedicated to ensuring that taxpayer dollars were being used as effectively and efficiently as possible. In 2009-2010, the Government of Canada had begun a strategic review process and the Service was required to rationalize operations and ensure alignment with organizational needs. This strategic review resulted in a $15 million budget reduction effective 2012-2013. Furthermore, as part of the Government's Deficit Reduction Action Plan (DRAP) announced in the 2012 Federal Budget, by 2014-2015 and ongoing the Service will reduce its budget by $24.5 million.

Construction costs shown are for the expansion of CSIS National Headquarters. Costs incurred from fiscal year 2002-2003 to 2006-2007 represent expenditures associated with the project definition stage. In 2007-2008 and 2008-2009, costs incurred were mainly attributable to the building's site preparation. The construction of Phase III began in the summer of 2009, with total expenditures of $4.9 million in 2011-2012. The building was officially opened by the Minister of Public Safety in October 2011.

Financial Resources



Actual Expenditures


“
THE SENSITIVE
NATURE OF THE
WORK UNDERTAKEN
BY THE CSIS
REQUIRES REVIEW.
”

REVIEW AND ACCOUNTABILITY

The *CSIS Act* did more than create Canada's civilian security intelligence agency. The Act also created and entrenched a regime of accountability so that the new agency, CSIS, would never engage in activities inconsistent with fundamental Canadian values.

The sensitive nature of the work undertaken by CSIS requires review. Service employees are accustomed to this close, ongoing scrutiny, and we believe it has helped the Service to become a global model of how an intelligence agency ought to function in a democratic system. CSIS continuously reviews and adapts its policies and practices, where required, in order to improve our operational effectiveness while ensuring that our activities continue to be carried out within our legislated mandate.

As with other federal agencies, the activities of CSIS are subject to review by the Federal Court, as well as by various officers of Parliament, including the Auditor General and the Privacy Commissioner. Again, the regular interaction between CSIS and these external bodies has helped the Service to become a more effective and professional organization.

The Minister of Public Safety

The CSIS Director is accountable to the Minister of Public Safety, who provides ministerial direction on the policies, operations and management of the Service.

Pursuant to section 6(2) of the *CSIS Act*, the Minister may issue to the Director written directions with respect to the Service. This can include direction on any matter, including intelligence collection priorities and/or restrictions, and on when and how the Service informs the Minister of its operations.

CSIS requires the approval of the Minister of Public Safety before entering into formal arrangements with domestic and foreign agency partners. These arrangements are governed under section 17(1)(a) and section 17(1)(b) of the *CSIS Act* and serve to ensure that the government's domestic and foreign policy interests and priorities are properly considered prior to the establishment of any formal intelligence sharing arrangement.

The Service also requires the approval of the Minister to file warrant applications with the Federal Court (section 21). This ensures appropriate ministerial accountability over the Service's more intrusive operational activities. Section 6(4) of the *CSIS Act* requires CSIS to report annually to the Minister on operational activities.

The Security Intelligence Review Committee (SIRC)

The Security Intelligence Review Committee (SIRC) is an independent, external review body which reports to the Parliament of Canada on Service operations.

SIRC and CSIS were both products of the same piece of legislation, the *CSIS Act,* and came into being at the same time in 1984. The *CSIS Act* was amended in 2012, repealing the Inspector General and transferring its responsibilities to SIRC, including accountability towards the Minister.

From the outset SIRC has always had access to all information held by the Service, with the exception of Cabinet confidences. In addition, SIRC meets with and interviews CSIS staff regularly, and formally questions CSIS witnesses in a quasi-judicial complaints process.

While CSIS is not required by law to adopt SIRC recommendations, they are carefully considered. The results of SIRC reviews and complaints are regularly discussed among members of the CSIS Executive and the Service has adopted most of SIRC's recommendations over the years.

The SIRC Annual Report, tabled in Parliament by the Minister, provides an unclassified overview of its various studies of CSIS issues that were conducted during the fiscal year, and of the results of its complaints investigations.

The Service's interactions with SIRC are primarily managed by the CSIS External Review and Liaison Unit. The unit coordinates the Service's response to requests or questions from SIRC, and acts as the primary point of contact regarding complaints against CSIS filed with SIRC under sections 41 and 42 of the *CSIS Act*.

THE INSPECTOR GENERAL (IG)

THE LEGISLATION THAT CREATED CSIS IN 1984 STIPULATED THAT THE SERVICE WOULD BE REVIEWED BY TWO BODIES: THE SIRC AND THE INSPECTOR GENERAL (IG).

IN JUNE 2012, THE OFFICE OF THE INSPECTOR GENERAL WAS ELIMINATED AS PART OF THE GOVERNMENT'S DEFICIT REDUCTION ACTION PLAN (DRAP) ANNOUNCED IN THE 2012 FEDERAL BUDGET. THE MOVE ENTRENCHED THE RESPONSIBILITY FOR REVIEWING CSIS OPERATIONS INTO ONE ORGANIZATION – SIRC. THIS CONSOLIDATION WAS AIMED AT STREAMLINING OPERATIONS. FUNCTIONS AND RESOURCES OF THE IG'S WERE ACCORDINGLY TRANSFERRED TO SIRC. IN PARTICULAR, THE IG MONITORED CSIS FOR COMPLIANCE WITH OPERATIONAL POLICES AND ISSUED A YEARLY, CLASSIFIED CERTIFICATE TO THE MINISTER. THIS CERTIFICATE SERVED TO INDICATE THE DEGREE OF SATISFACTION WITH THE DIRECTOR'S ANNUAL REPORT ON CSIS ACTIVITIES PROVIDED TO THE MINISTER OF PUBLIC SAFETY UNDER SECTION 33 OF THE *CSIS ACT*. THIS UNIQUE FUNCTION HAS BEEN RETAINED AND RESPONSIBILITY FOR THE ISSUANCE OF THE CERTIFICATE WAS TRANSFERRED TO SIRC, NOW UNDER SECTION 6(4).

TO ENSURE A COMPARABLE DEGREE OF ACCOUNTABILITY AS IN THE PREVIOUS SYSTEM, SIRC, WHICH REPORTS TO PARLIAMENT, WILL NOW PROVIDE THE MINISTER OF PUBLIC SAFETY WITH THE REPORTS OF ALL REVIEWS OF CSIS ACTIVITIES THAT IT UNDERTAKES. IT WILL ALSO NOW BRIEF THE MINISTER AT LEAST ONCE A YEAR ON THESE ACTIVITIES THUS STRENGTHENING THE MINISTER'S KNOWLEDGE OF CSIS ACTIVITIES AND ENHANCING THE ABILITY TO RESPOND AT AN EARLY STAGE TO ANY CONCERNS ABOUT HOW CSIS CONDUCTS ITS BUSINESS.

CSIS Internal Audit Branch / Disclosure of Wrongdoing and Reprisal Protection

The Internal Audit (IA) Branch is led by the Chief Audit Executive (CAE), who reports to the CSIS Director and to the CSIS External Audit Committee (AC). The CAE provides assurance services to the Director, Senior Management and the AC, as well as independent, objective advice and guidance on the Service's risk management practices, control framework, and governance processes. The CAE is also the Senior Officer for Disclosure of Wrongdoing.

In 2010-2011, an external, independent assessment concluded that the internal audit function was in general conformance with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing and the Code of Ethics. The assessment also concluded that the audit function was in general conformance with the Treasury Board Policy on Internal Audit Suite and the Internal Auditing Standards for the Government of Canada.

The AC continued to bring about improvements to the delivery of assurance services by examining CSIS' performance in the areas of risk management controls and governance processes relating to both operational activities and administrative services. By maintaining high standards in relation to its review function in particular following-up on the implementation of management action plans derived from audit recommendations the AC supports and enhances the independence of the audit function.

IA's efforts and performance were also recognized by the Treasury Board Secretariat in context of the Management Accountability Framework by rating the audit function as "Strong" in 2011-2012 and 2012-2013.

In the capacity of Senior Officer for Disclosure of Wrongdoing, the CAE is responsible for administering the Internal Disclosure of Wrongdoing and Reprisal Protection Policy. The Policy provides a confidential mechanism for employees to come forward if they believe that serious wrongdoing has taken place. It also provides protection against reprisal when employees come forward, and ensures a fair and objective process for those against whom allegations are made. This effort to establish an effective internal disclosure process has met with success and has the support of senior managers.

Over the years, CSIS has demonstrated that it is a responsive and nimble organization that listens to advice from a variety of sources and implements change accordingly. In its role as assurance provider, IA supports the Service in implementing change by maintaining professional services that contribute to improving corporate risk management, control and governance processes.

Access to Information and Privacy (ATIP)

The mandate of the Access to Information and Privacy (ATIP) Unit is to fulfill the Service's obligations under the *Access to Information Act* and the *Privacy Act*. The Service's Chief, ATIP is entrusted with the delegated authority from the Minister of Public Safety Canada to exercise and perform the duties of the Minister as head of the institution.

Although CSIS is the custodian of state secrets, we will declassify documents to the extent we can in order to provide them to scholars, journalists and others who make official requests under *Access to Information Act*.

As the custodian of expertise related to the Service's obligations under the *Access to Information Act* and the *Privacy Act*, the ATIP Unit processes all requests made under the relevant legislation and responds to informal requests for information. In doing so, the unit must balance the need for transparency and accountability in government institutions while ensuring the protection of the Service's most sensitive information and assets.

In addition, the ATIP Unit directs all activities within the Service relating to the administration, application and promotion of both Acts. It provides advice to senior management on the implementation

of the Acts and prepares reports to Parliament, Treasury Board Secretariat (TBS) and senior management.

In 2011-2012, the ATIP Unit conducted a number of awareness sessions for all new employees, as well as for a number of managers and specialized groups. The objective of the sessions was to provide participants with an overview of both the *Access to Information Act* and the *Privacy Act* and to promote a better understanding of their obligations under these Acts.

In addition to enhancing awareness internally, the Service's ATIP Unit participates in intergovernmental activities as well. In February 2012, the unit delivered a briefing session at a Departmental Security Officers (DSO) conference hosted by CSIS. An estimated 58 DSO's from other federal institutions and 100 Service employees were in attendance.

During the last two fiscal years, the CSIS ATIP Unit received a total of 465 requests under the *Privacy Act* and 717 requests under the *Access to Information Act*. The Service's on-time completion rate was more than 99 per cent and CSIS received a 'Strong' rating from TBS in all three Management Assessment Framework lines of evidence related to the administration of the Acts. The Information Commissioner's special report tabled to Parliament on May 31, 2012 also recognized the Service's outstanding achievement.


“
CSIS’S DESIRE TO DEVELOP A CAPACITY FOR COMMUNITY ENGAGEMENT IS CONSISTENT WITH THIS OPEN APPROACH.
”

COMMITTED TO CANADIANS

Community Engagement

The work of intelligence services, even in democratic systems, is often cloaked in mystery and misunderstood by ordinary citizens. The entertainment industry in particular specializes in images of "spies" operating according to their own rules and with little accountability. The more prosaic truth however, at least at CSIS, is that we are not a secret organization and have no desire to be one. While true that we deal in secrets – or, better put, in classified information – we recognize that Canadians expect transparency from their institutions.

Indeed, in February 2012 the Government of Canada released its first counter-terrorism strategy, *Building Resilience Against Terrorism*, a document that highlights the importance of openness between citizens and their government in the ongoing, shared effort to counter violent extremism. CSIS's desire to develop a capacity for community engagement is consistent with this open approach. Canadian citizens have a strong interest in issues of national security, and where possible the Service is trying to promote an informed public conversation.

To this end, CSIS has continued to be an enthusiastic partner of the Cross-Cultural Roundtable on Security (CCRS), a Public Safety Canada-led initiative that seeks to demystify the security apparatus. The CCRS brings together security officials from several government agencies and departments and introduces them to members of ethno-cultural groups across Canada.

Over the past two years, CSIS personnel have participated in a variety of outreach meetings, some of them formal affairs around boardroom tables and some of them more casual "town-hall" style gatherings. We continue to meet personally – one-on-one, in some cases – with community representatives who have an interest in getting to know us and our mandate. The aim is to have an honest and useful dialogue, and indeed that has been our experience.

These initiatives provide the Service an opportunity to explain that our mandate is to protect all Canadians, including minority and immigrant communities. This is especially important given that some in these communities may fear the security apparatus based on experiences in their countries of origin. Canadians are entitled to know how we at CSIS conduct our business and the parameters within which we operate. Through our communications activities, the Service seeks to assure all Canadians that we see them as partners and allies.

CSIS itself is a remarkably diverse organization, becoming more so every year. The multicultural character of Canada is profoundly reflected in our workforce, something that would perhaps not be widely known or appreciated were it not for our participation in public outreach.

Community engagement is still relatively new to the Service, but the exercise is proving to be a positive one. As the custodian of national security expertise, we believe there is value in our assuming, where appropriate, an educational role, one that brings benefits to ourselves and, more importantly, to the communities we serve.

Academic Outreach

CSIS launched its Academic Outreach Program in September 2008. The purpose of the program is to promote a dialogue with experts from a variety of disciplines and cultural backgrounds working in universities, think tanks and other research institutions in Canada and abroad.

This program affords CSIS access to leading thinkers who can provide unique insights into a range of issues that have an immediate and long-term impact on Canada's security environment. It may happen that some of our academic partners hold ideas or promote findings that conflict with our own views and experience, but that is one of the reasons we initiated the program. We believe there can be value in having informed observers challenge our thinking and approaches. The program helps the Service focus its intelligence collection efforts and improve its analytical capacity.

The exchange runs in both directions. A more interactive relationship with the academic community allows the Service to share some of its own expertise and interests, which in turn can help scholars – political scientists, economists, historians, cybersecurity experts, psychologists – to identify new avenues of research.

Academic Outreach (AO) hosted three conferences during 2011-2013 that brought together multi-disciplinary groups of experts from several countries. The first conference was entitled "Competing Visions of the State: Political and Security Trends in the Arab World and the Middle East" and was designed to identify the implications of the Arab Uprisings for the region and the West. The second conference, entitled "Informing (In)stability: The Security Implications of a Shifting News and Media Environment", focused on the tremendous changes information technology has introduced to the media world and their consequences for government and other social actors. The third conference, "The Security Dimensions of an Influential China", examined the security implications of the evolution of China as a burgeoning superpower.

The international conferences, however, represent only one component of the AO program. We have also hosted a number of in-depth briefings on other topics of interest. For instance, one examined advances in Iran's nuclear program. The speaker had conducted extensive research on the technical aspects of the question as well as the intentions of the Iranian leadership. Another briefing designed to bolster our analytic capacity involved discussions with practitioners of foresight and the role that it can play in the field of intelligence analysis.

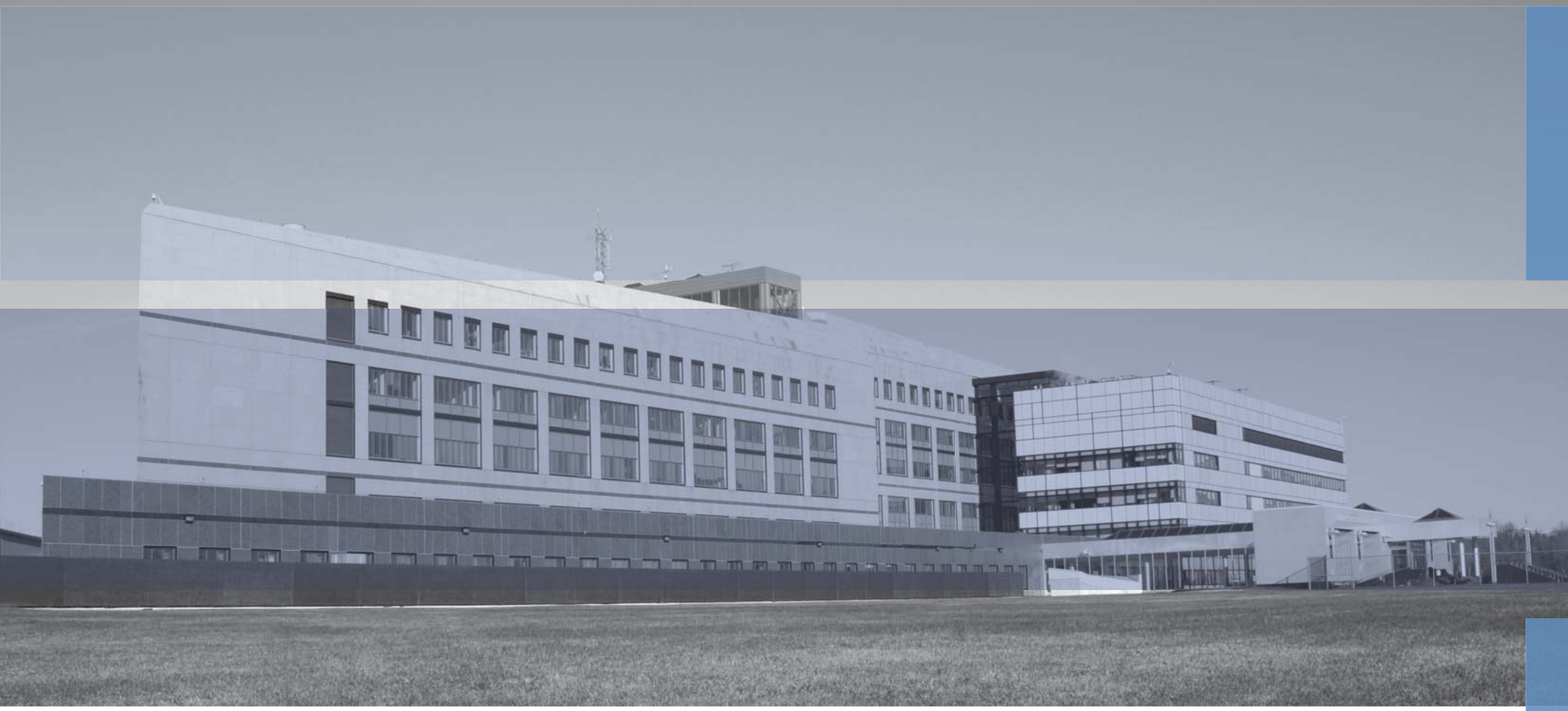
There is a significant interest on the part of experts to participate in activities sponsored by CSIS. Since 2008, the Service's Academic Outreach Branch has organized nine international conferences, numerous seminars and workshops, and hundreds of noontime expert briefings in which outside experts speak to CSIS personnel on a topic

of mutual interest at the Service's National Headquarters in Ottawa. The lunchtime presentations are very popular, reflecting a commitment to professional development among CSIS personnel.

During 2011-2013, outside experts engaged CSIS staff on discussions covering a range of security and strategic issues, including: the changing leadership of the Chinese Communist Party; the availability and safety of bio-chemical weapons in Syria; radicalization trends in West and East Africa and South Asia; the future of politics in Iraq; the changing nature of North Korea's political economy and challenges confronting the Putin presidency in Russia. The Academic Outreach Branch also commissioned several experts in support of a foresight project aimed at developing alternative future scenarios for the Al-Qaeda phenomenon in the year 2018. The results are now available on our website.

Intellectual engagement with scholars outside the professional security establishment helps the Service ask the right questions – and avoid surprises – on issues pertaining both to the Canadian and global security environments. The program is still young, but it is playing an important role in enabling CSIS to adopt a more holistic approach when reviewing and assessing national and international issues of interest. Ensuring that we have access to all of the information possible allows the Service effectively and accurately to fulfil its mandate, and to do so responsibly.

The Academic Outreach program promotes partnerships with other government departments. Canada's Foreign Affairs, Trade and Development, the Privy Council Office, the Canadian Food Inspection Agency, the Department of National Defence and the International Development Research Centre provided support to some of the CSIS international conferences. The lunchtime series is also open to analysts from the broader intelligence community. These shared events provide an opportunity for members of the intelligence community across government to liaise and collaborate.



CSIS BUILDING HEADQUARTERS | OTTAWA

CONTACT US

National Headquarters

Canadian Security Intelligence Service
P.O. Box 9732, Station T
Ottawa ON K1G 4G4

Tel. 613-993-9620 or 1-800-267-7685 toll-free (Ontario only)
TTY 613-991-9228 (for hearing-impaired, available 24 hours a day)

Media and Public Liaison Queries:

CSIS Communications Branch
P.O. Box 9732, Station T
Ottawa ON K1G 4G4
Tel. 613-231-0100

Regional Offices

Atlantic Region	P.O. Box 126, Station Central Halifax NS B3J 3K5 Tel. 902-420-5900
New Brunswick District	P.O. Box 6010, Station A Fredericton NB E3B 5G4 Tel. 506-452-3786
Newfoundland and Labrador District	P.O. Box 2585, Station C St. John's NL A1C 6J6 Tel. 709-724-8650
Quebec Region	P.O. Box 2000, Station A Montreal QC H3C 3A6 Tel. 514-393-5600 or 1-877-223-2265 toll-free (Quebec only)

Quebec City District	P.O. Box 10043, Station Sainte-Foy Quebec QC G1V 4C6 Tel. 418-529-8926
Ottawa Region	P.O. Box 9732, Station T Ottawa ON K1G 4G4 Tel. 613-998-1679 or 1-800-267-7685 toll-free (Ontario only)
Toronto Region	P.O. Box 760, Station A Toronto ON M5W 1G3 Tel. 416-865-1480
Prairie Region (Alberta, Saskatchewan, Manitoba, Northwestern Ontario, Yukon, Northwest Territories, Nunavut)	P.O. Box 47009 62 City Centre Edmonton AB T5J 4N1 Tel. 780-401-7800 or 1-800-661-5780 toll-free (Prairie only)
Calgary District	P.O. Box 2671, Station M Calgary AB T2P 3C1 Tel. 403-292-5255
Saskatchewan District	P.O. Box 5089, Station Main Regina SK S4P 4B2 Tel. 306-780-5512
Manitoba District	P.O. Box 771, Station Main Winnipeg MB R3C 4G3 Tel. 204-954-8120
British Columbia Region	P.O. Box 80629 South Burnaby BC V5H 3Y1 Tel. 604-528-7400

EXECUTIVE ORGANIZATIONAL CHART