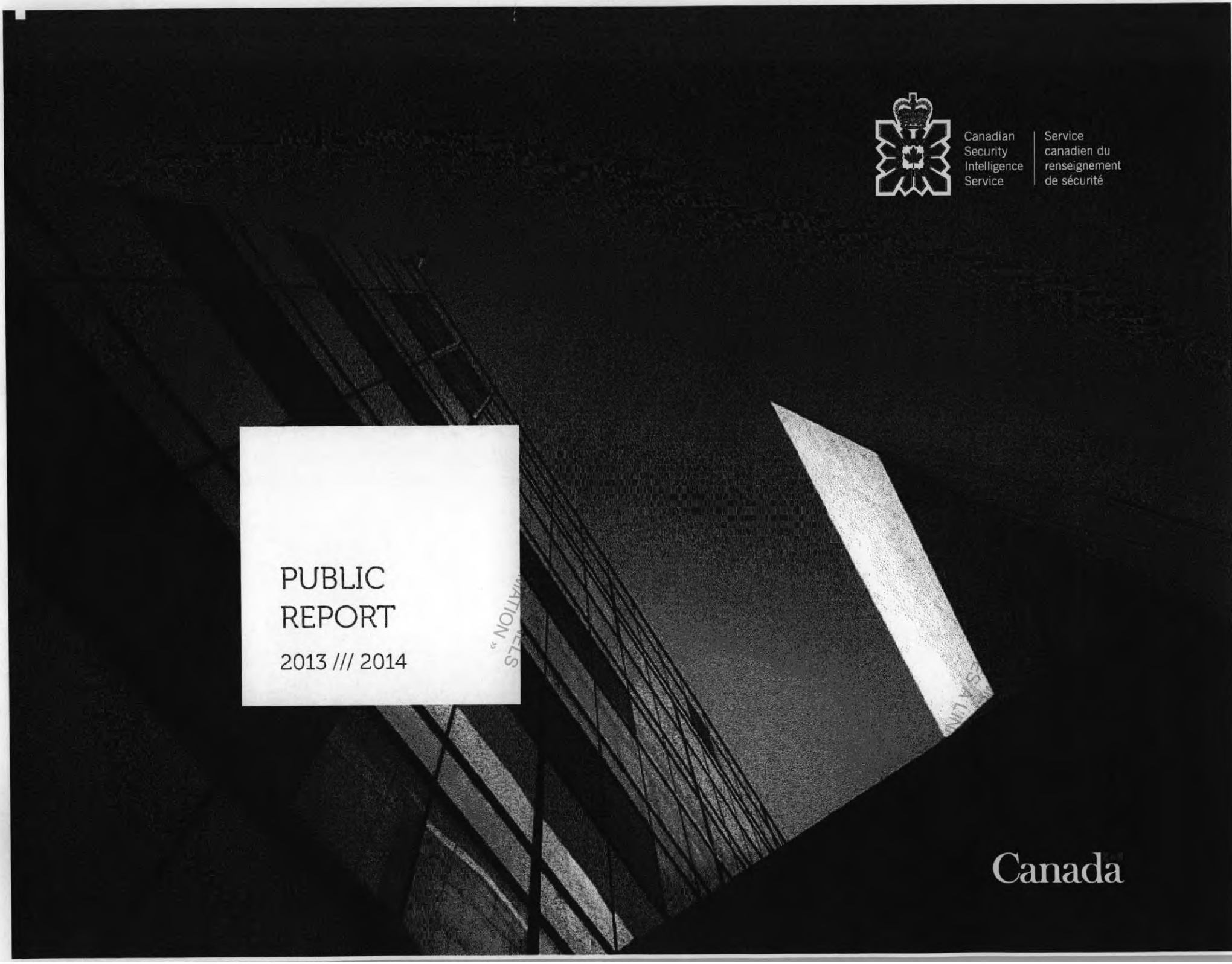

Canadian Security Intelligence Service
Service canadien du renseignement de sécurité
PUBLIC REPORT
2013 /// 2014
Canada

PUBLIC REPORT

2013 /// 2014

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

"PROCESSED UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

NHQ BUILDING /// OTTAWA

/// MESSAGE FROM OUR DIRECTOR

As I write these words, many in our nation are still coming to terms with the events of last fall when two Canadians, radicalized to violence, launched separate attacks against fellow citizens, one in Saint-Jean-sur-Richelieu, Quebec, and the other in Ottawa. Two unarmed members of the Canadian Armed Forces were killed. The Canadian Security Intelligence Service (CSIS) joined the rest of the country in mourning their loss.

The attacks exposed in a most vivid way the vulnerability to terrorism that an open society like Canada faces. There was a period after 9-11 when many people assumed that an effective terrorist attack was necessarily one that involved a network of highly trained operatives bent on committing a spectacular, mass-casualty event. In truth, a single assailant with low-tech weaponry – a rifle or even a car – can bring tragedy and insecurity to our communities, as we saw in Canada.

That Canada is not immune to this kind of violence has long been clear to those of us in the national security community – and to anyone else who follows the news of the day. The October attacks in Saint-Jean-sur-Richelieu and Ottawa were not the only major terrorism-related story of 2014. A month earlier, in an Ottawa courtroom, a 34-year-old Canadian was convicted of planning to commit acts of terrorism in Canada. The sentencing hearing was notable not just for the lengthy prison term given to the accused – 24 years – but for the court's vivid reaction to what the individual intended to do.

"You are now a convicted terrorist," said the presiding judge. "That fact carries with it an utterly deplorable stigma that is likely impossible to erase … You have betrayed the trust of your government and your fellow citizens. You have effectively been convicted of treason, an act that invites universal condemnation among sovereign states throughout the world."

An accomplice was also convicted of terrorism-related offences and sentenced to 12 years. The evidence presented in court indicated that the men were seeking to establish a functioning terrorist cell in Canada; they might have succeeded if not – to quote the judge again – for the "vigilant and tireless" work of our national security agencies. The scope of the problem was further illustrated when terrorism- related charges were laid against a 15-year-old boy from Montreal in December 2014, and then against a group of Ottawa men in January 2015.

There are violent people and violent groups that want to kill Canadians. It's a sobering observation to make, and there is no euphemistic way of making it.

During the review period of the CSIS 2013-14 Public Report, the phenomenon of so-called foreign fighters gained increased prominence. The attention and concern has in my view been entirely legitimate. The fanaticism associated with al-Qaeda and murderous off-shoots such as the Islamic State in Iraq and the Levant (ISIL) is resonating with some individuals in Canada.

Community leaders, teachers and most of all parents have seen young people pursue a cause that has no good outcome. A number of these young Canadians have died in the foreign lands to which they have been drawn. There is no doubt that some of these Canadians have also killed people.

CSIS has been clear about the security challenge. We are interested in Canadian extremists who return to this country more radicalized than when they departed. Will their status as veterans of a foreign conflict better enable them to recruit other Canadians? Will they use their foreign contacts to set up networks in Canada to facilitate the movement of fighters, material and money in and out of the country?

And, most importantly, will they use their terrorist training to attempt violent acts here in Canada? Europe has already suffered such attacks. 2015 began with the January massacres in Paris at a magazine office and a Jewish grocery store. At least one of the attackers was reported to have had terrorist training in Yemen. Some months earlier, a French citizen and "returnee" from Syria went on a shooting spree in Belgium and killed a number of innocent civilians.

Even if a Canadian extremist does not immediately return, he or she is still a Canadian problem. Just as Canada expects other nations to prevent their citizens from harming Canadians and Canadian interests, we too are obligated to deny Canadian extremists the ability to kill and terrorize people of other countries. And, lastly, there is the threat posed here by frustrated extremists who have been unable to join the fight abroad. It is for all of these reasons, as our Public Report makes clear, that terrorism continues to be the most significant threat to Canada's security interests.

Terrorism, however, is far from the only threat. Espionage against Canada's economic, political and military interests is an ongoing concern. In December 2013, a Canadian citizen living in Ontario was arrested and charged under the *Security of Information Act* for allegedly passing sensitive information to a foreign entity. This was barely nine months after another Canadian, naval officer Jeffrey Delisle, was sentenced to 20 years in prison also for violating the *Security of Information Act* and selling secrets to a hostile foreign entity.

These espionage cases are high-profile for the simple fact that they met a criminal threshold and became publicly known. Cyber intrusions orchestrated by hostile foreign states, such as the one in the summer of 2014 against the National Research Council of Canada, are also increasingly of concern. There are many other activities occurring all the time in Canada – not just espionage but clandestine foreign influence – and while not in the public eye, they are equally damaging to Canadian security and sovereignty.

The year 2014 marked the 30th anniversary of the creation of CSIS. We are proud that in these past three decades we have matured into a valued and respected Canadian institution (see "Thirty Years of National Security", page 9). The work we do is complex and sensitive, seemingly more so every year in a constantly changing threat environment.

Yet ever constant is our commitment not only to fulfill our mandate of keeping Canada and Canadians safe, but to do so in a way that is consistent with Canadian values. We promise to do so for the next 30 years, and beyond.

Michel Coulombe

///
THIRTY YEARS OF NATIONAL SECURITY

The year 2014 marked the 30th anniversary of CSIS's creation. Before 1984, security intelligence was a police function, housed within the RCMP. Over time, however, a consensus emerged that this role should more properly be assigned to a separate civilian agency which would not have powers of arrest or detention.

When Canada's Parliament created CSIS three decades ago, the Cold War was still raging. Conflict between states represented the major threat to international security. Flash forward to today and we have a multitude of security challenges that were never envisioned, from cyber-espionage to "super-empowered" non-state actors – super-empowered in the sense that they can kill thousands of people, as al-Qaeda did on September 11, 2001.

The occasion of our 30th anniversary provoked considerable reflection across the Service. Have we adapted to a security environment that is radically different from the one that existed at our founding?

We have. Most notably, the collapse of the Soviet bloc and the rise of transnational terrorism compelled us to develop a whole new range of expertise. That there has not been a mass-casualty terrorist attack in Canada in the post-9-11 period is testimony to our counter-terrorism capacity. Many terrorist plots have been thwarted, most famously the "Toronto 18" case which resulted in numerous criminal prosecutions and some life sentences.

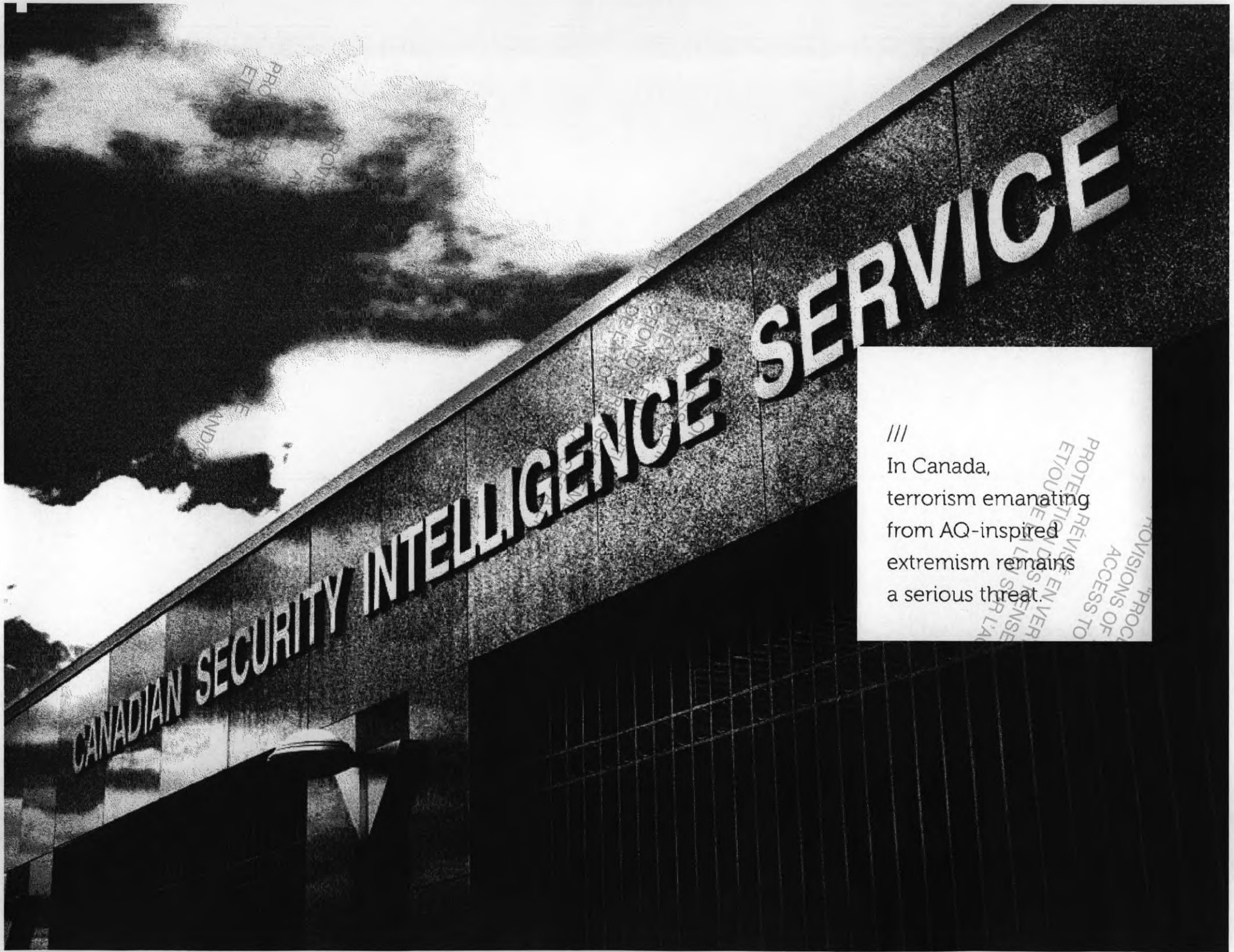
We have innovated in the areas of science and technology. The newer generation of CSIS staff are always amused to learn that 30 years ago much of our business was still paper-based, replete with handwritten files and index cards. Today we have leading-edge solutions in information-management.

Our approach to internal management and external communications has also matured. Historically, intelligence services which had roots in paramilitary culture might not have always recognized the value of organizational transparency. That has changed. As a Top 100 employer in Canada, the Service today cultivates a participatory working environment where employees are engaged at all levels. Similarly, notwithstanding the sensitivity of our mandate, we are increasingly finding ways to participate in the public conversation about national security.

Thirty years ago a civilian intelligence service was an untested idea, and in some quarters perhaps a controversial one. Today CSIS is an established and respected Canadian institution. Because the Service enjoys high employee retention rates, some of the same personnel who came aboard in 1984 and were tasked with building the organization have played key roles in transforming it.

It's impossible to predict how the global security environment will evolve over the next 30 years, but evolve it will – and so will CSIS along with it.

TABLE OF CONTENTS



///

In Canada, terrorism emanating from AQ-inspired extremism remains a serious threat.

THE THREAT ENVIRONMENT 2013-2014

Canada is a multicultural and diverse nation that possesses a wealth of human capital and natural resources. It is one of the most desirable places to live, continually ranking near the top of global surveys for its high standard of living. Security remains essential to the preservation of Canada's way of life and the protection of those who reside within its borders. In today's complex, interconnected world, threats to national security are many, multi-faceted and continually evolving, and quite often originate in places far removed from our borders. Under the *Canadian Security Intelligence Service (CSIS) Act* (1984), the Service is mandated to investigate activities that may on reasonable grounds be suspected of constituting a threat to the security of Canada. The Service's priorities include threats emanating from or related to terrorism, espionage and foreign interference, proliferation and cyber-threats. The following is a summary of the key threats to Canada since April 2013.

Terrorism

Terrorism at home and abroad

Terrorism continues to be the most significant and persistent threat to Canada's national security, and the period since April 2013 has witnessed a substantial progression in the domestic and international terrorist threat. Within Canada, there were high-profile incidents of Canadians travelling abroad to engage in terrorist activities. In the United States, the terror attack at the April 2013 Boston Marathon demonstrated the ongoing threat to the West from homegrown violent extremism.

Internationally, the al-Qaeda (AQ) network continued to face significant adversity. Internal disputes within the global network led in 2013-14 to the Islamic State in Iraq and the Levant (ISIL) breaking away from the AQ fold. That said, the threat from international terrorism remains substantial and terrorist movements remain active in North and West Africa, Somalia, Iraq, Syria and elsewhere. They continue to inflict casualties against innocent civilians – including Canadians – and to destabilize countries and entire regions, thereby posing a threat to Canadian interests abroad.

In Canada, terrorism emanating from AQ-inspired extremism remains a serious threat. Despite a weakened AQ Core, the Service continues to see support for the AQ cause in Canada. The arrest of two individuals in April 2013, as part of an alleged AQ-linked plot to attack a train in southern Ontario, is proof of these evolving plots. In recent

months, Canadians have been killed while fighting alongside extremists in Syria and Iraq.

There are three primary ways in which terrorism continues to threaten 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 that support terrorism globally, including fundraising to support attacks and militant groups;

- Third, terrorists and their supporters employ social media to reach individuals in Canada for operational purposes and to radicalize them. Some of these radicalized individuals may conduct attacks before travelling abroad or travel overseas to obtain training or to engage in terrorism in other countries. They endanger themselves and pose a risk to the countries to which they have travelled. Should they return to Canada, they may pose a threat to national security by attempting to radicalize others, train them in terrorist methods, or conduct terrorist attacks on their own.

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 2012 and expanded upon in the 2013 and 2014 Public Reports on the Terrorist Threat to Canada.

Radicalization

The radicalization of Canadians towards violent extremism continues to be a significant concern to the Service and its domestic partners. Radicalization is the process whereby individuals abandon otherwise moderate, mainstream beliefs and at some stage adopt extremist political or religious ideologies. Radicalized individuals may advocate violent extremism or mobilize to become engaged in violent extremism. Activities can range from attack planning against Canadian targets, sending money or resources to support violent extremist groups abroad, and/or influencing others (particularly youth) to adopt radical ideologies. These individuals may also attempt to travel abroad for terrorist training or to engage in fighting. If they become seasoned fighters with experience in conducting terrorist attacks or assist in the radicalization of others, such individuals can pose a serious threat to the national security of Canada.

In October 2013, British authorities detained four individuals for allegedly planning attacks in the United Kingdom. At least one of the individuals had been to Syria and returned to the UK in mid-2013. In February 2014, British authorities arrested another four individuals, one of whom had reportedly travelled to Syria and attended a terrorist training camp. In May 2014 a French citizen, who is believed to have

spent a year in Syria fighting alongside jihadists, conducted a terrorist attack when he opened fire at the Jewish Museum in Brussels, killing four people. These cases demonstrate the potential threat some returnees may pose to national security after their return home. Even if they do not return, foreign fighters pose significant problems insofar as these individuals lend support to the terrorist cause abroad. The deaths of Canadians in Syria and Iraq are indicative of this trend and highlights the challenge posed by the travel of radicalized individuals for terrorist purposes. In April 2013, the Canadian government passed legislation which makes it illegal to leave Canada for the purpose of committing terrorism.

In order to generate a better understanding of the phenomenon, the Service conducts research on radicalization in Canada. CSIS has found that radicalized individuals come from varied social backgrounds and age groups, with a wide range of educational credentials and often appear to be fully integrated into society. This makes the detection of radicalized individuals particularly challenging.

Al-Qaeda Core

Based predominantly in the tribal areas of Afghanistan and Pakistan, Al-Qaeda (AQ) Core has experienced a series of major setbacks, going back to the 2011 death of its leader and founder, Osama bin Laden. As a result of a potent and sustained counter-terrorism campaign led by the United States, AQ Core's leadership has been degraded significantly over the past several years. Nevertheless, AQ Core continues to be flexible and still commands the loyalty of several affiliate organizations and associated regional extremist groups. In 2013, bin Laden's successor Ayman al-Zawahiri named the leader of AQ's affiliate in Yemen as his deputy. This marks the first time since 2001 that AQ's top leadership is not in its entirety based in the Afghanistan-Pakistan theatre, demonstrating that AQ continues to exhibit resilience and an ability to adapt in the face of adversity.

In early 2014 AQ also severed ties with its former affiliate, the Islamic State of Iraq and the Levant (ISIL, formerly Al-Qaeda in Iraq), after al-Zawahiri was openly rebuffed by ISIL's leadership when he attempted to mediate a dispute between ISIL and another group, Jabhat al-Nusra (JN). The incident represented arguably the most public disagreement among AQ leaders, and possibly the most serious defiance by an affiliate of AQ leadership since 2001. Furthermore, guidance issued by al-Zawahiri in 2013 for affiliates to avoid the bloodshed of innocent Muslim civilians was consistently ignored by AQ's affiliates. These developments, coupled with ISIL's conquest of key Iraqi cities and declaration of the Caliphate in June 2014, represents the most significant challenge to AQ Core's leadership, sources of revenue and ideological legitimacy since 2001.

Nevertheless, the AQ narrative continues to inspire extremists globally. This narrative alleges that the West is conspiring and waging war against Islam, and that there is an obligation on the part of 'true believers' to wage jihad against the West in order to defend the Islamic community. In place of the current regimes in the Muslim Middle East, these extremists claim to be working toward the creation of a sharia-based society under an Islamic Caliphate. Notwithstanding the

narrative, AQ-inspired extremists are often resilient in the face of local, regional and global events, and have adopted emerging technologies and changed their tactics in order to achieve their objectives. Furthermore, these extremist elements are deft at exploiting opportunities that allow them to expand into new areas while withstanding sustained counter-terrorism campaigns. While AQ Core and its affiliates remain central to the AQ global movement, the wide-ranging facilitation activities of individuals, with a large number of contacts, experience and knowledge, have created a web of transnational extremist networks that carry out the day to day activities of what its members call global jihad.

AQ Core was caught off-guard by the political uprisings of the "Arab Spring", which largely rejected the AQ narrative and message. AQ was initially absent in these revolutions, but some movements linked to AQ, or otherwise inspired by its narrative, have subsequently appeared in Arab Spring countries. The volatile security situation stemming from the Arab Spring has now provided room for AQ and its affiliates to operate more freely. Furthermore, the course of the Arab Spring has in some respects reinforced the AQ narrative. The overthrow of Egyptian president Mohammad Morsi in July 2013 and the subsequent designation of the Egyptian Muslim Brotherhood (EMB) as a terrorist group by the Egyptian authorities reinforced the AQ narrative that democracy is futile and that only jihad will bring about meaningful change in the Muslim world. The Arab Spring has thus afforded new opportunities to AQ Core.

AQ Core remains a dangerous terrorist group, which has thus far retained the intent to carry out major attacks against the West and to influence individuals to do the same. The group has not successfully executed an attack in the West since the 2005 bombing of the London Underground, although several attempts have been disrupted in other countries, demonstrating the ongoing intent and capacity for serious acts of violence against Western interests. The Service assesses 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.

AQ Affiliates

AQ affiliates based in the Middle East have benefitted from expanding the territory in which they are able to operate and develop sources of funding. In 2013 all the major AQ affiliates engaged in kidnapping for ransom activities, especially targeting Westerners, which provided them with money that could be used to expand their operational capacity. Kidnapping for ransom operations are likely to continue and will remain a serious threat to Canadians who travel to areas where AQ linked groups are known to operate.

Afghanistan

When Canada's combat role in Afghanistan ended in 2011, the role of the Canadian Armed Forces shifted to training the country's police force and army. The last of Canada's military trainers departed Afghanistan in March 2014 while remaining Coalition forces are to withdraw by the end of 2014. The security situation in Afghanistan remains precarious, however, with extremist groups like AQ, the Afghan Taliban and the Haqqani Network regularly conducting attacks against Afghans and foreigners alike. On January 18, 2014, two Canadian civilian contractors were killed in a suicide attack at a Kabul restaurant, and on March 20, 2014, two more Canadian civilians were killed when a Kabul luxury hotel was attacked by Taliban suicide bombers. These tragic incidents demonstrate the continued threat to Canadian interests in the country. The ongoing political uncertainty, the role of regional powerbrokers and a tenacious Taliban insurgency are likely to challenge the future stability of Afghanistan.

Somalia and Al Shabaab

Political instability, terrorism, and piracy continue to plague Somalia. The resulting problems which emanate from East Africa constitute significant threats to the security of Canada. In particular, the terrorist group Al Shabaab (AS) remains a significant threat to regional security despite losing control of territory in Somalia. Al Shabaab increased its operational tempo, conducting a number of lethal attacks in Somalia and Kenya in April and September 2013, respectively, including an attack on the Westgate Shopping Center in Nairobi, Kenya, during which at least 67 were killed, including two Canadian citizens.

A number of Somali-Canadians have travelled to Somalia for terrorist training. Some of these individuals have reportedly been killed. In April 2013, a Canadian was reported to have taken part in the deadly attacks on Mogadishu's Benadir Courts which killed numerous individuals. In April 2013, the Canadian government passed legislation which makes it illegal to leave Canada for the purpose of committing terrorism.

Al-Qaeda in the Arabian Peninsula (AQAP)

The Yemen-based Al-Qaeda in the Arabian Peninsula (AQAP) remains a significant terrorist threat with the capacity and intent to carry out attacks within Yemen and against the international community. Although AQAP continues to maintain a specialized cell dedicated to Western operations, in 2013-14 it focused much of its attention against the Yemeni government. However, AQAP propaganda continues to

underline the importance of striking at the international community as well as the need for extremists to engage in self-generated acts of domestic terrorism, criminality and sabotage; its magazine, *Inspire*, continues to release easy to understand how-to-guides for building explosives.

Ansar Bayt al-Maqdis (ABM)

Ansar Bayt al-Maqdis (ABM), an AQ-affiliated group based in the Sinai Peninsula, has responded to AQ's call to jihad. Since the July 2013 removal of the Morsi government in Egypt, the ABM has conducted several significant attacks, the majority of which were directed at Egyptian government and security forces. However, in February 2014, the group carried out a suicide attack against tourists near Taba, on the Israeli-Egyptian border, killing three South Koreans. In May 2014 it attacked another tourist bus in southern Sinai.

Jabhat al-Nusra (JN)

JN has emerged as an AQ node in Syria and is one of the many groups fighting against President Bashar Al-Assad's regime. In 2013 it openly pledged allegiance to AQ Core leader, Ayman al-Zawahiri. JN has focused its operations against the Syrian regime; however, infighting among opposition groups like JN, ISIL and others may have a detrimental impact on their ability to topple the Syrian regime. The ongoing chaos in Syria and Iraq means that these groups will continue to draw Westerners who seek to engage in violent extremism or to support it. There is growing concern that extremism in Syria and Iraq will result in a new generation of battle-hardened extremists who may eventually return to their home countries or continue to export terrorism abroad.

Al-Qaeda in the Islamic Maghreb (AQIM)

In North Africa, Al-Qaeda in the Islamic Maghreb (AQIM) continued to pursue a campaign of violence, 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. In addition, AQIM has continued to exploit the security vacuum provided by the Libyan and Tunisian revolutions.

AQIM has exploited developments in northern Mali to increase its operational capacity, sanctuary and influence. It has aligned itself with local extremist groups, and together they were able to effectively gain control of most of northern Mali. France's military intervention against the militants in December 2012 succeeded in weakening AQIM but the group and its allies have proven to be resilient. Political stability in northern Mali will likely remain elusive for some time, providing space for the extremists to re-establish some safe havens.

The very fluid regional security environment has important implications for Canada as a number of Canadian businesses across the wider region could be at risk.

Boko Haram

In Nigeria, the violent Islamist extremist group Boko Haram has become increasingly lethal and sophisticated over the past year, with the group escalating its violent campaign to undermine the Nigerian government's authority in the country's northeast. Boko Haram's April 2014 abduction of almost 250 schoolgirls has drawn international attention.

Suspected Boko Haram elements were also believed to be behind the April 2014 kidnapping of Canadian Sister Gilberte Bussière and two Italian priests in the far northern region of Cameroon. The victims were released on June 1. The incident is the latest demonstration that kidnapping remains one of the primary threats to Canadians across the wider North/West Africa region. It also suggests that Nigerian-based extremist groups increasingly have the intent and the capacity to carry out operations against Western interests outside of Nigeria.

Although Boko Haram directs many of its deadly attacks against the Nigerian state in northern Nigeria, the group has also conducted some indiscriminate attacks in the Nigerian capital, Abuja, increasing the risk to Canadian interests.

Islamic State of Iraq and the Levant (ISIL)

The Islamic State of Iraq and the Levant (ISIL, formerly Al-Qaeda in Iraq or AQI) has since 2004 been a deadly force within Iraq but in April 2013 expanded its activities into Syria. However, a serious dispute in 2013 between the Syrian Islamist group Jabhat al-Nusra (JN) and ISIL led AQ leader Ayman al-Zawahiri to side with JN. When ISIL defied the AQ Core leadership, the latter disavowed the group in February 2014. ISIL thus remains an AQ offshoot with no organizational relationship with the AQ Core leadership.

After its June 2014 gains in Iraq, ISIL (now called "Islamic State") announced on June 29 the establishment of the Caliphate stretching from the Syrian governorate of Aleppo in the west to the Iraqi province of Diyala in the east. Although ISIL's extreme brutality has been a source of tension with other extremist groups, as of the summer of 2014 it had managed to gain control of a significant share of Iraqi and Syrian territory.

Iran

Iran has a well-documented history of providing funds, weapons, training and political support to a range of designated terrorist groups, including Lebanese Hizballah, Palestinian groups such as Hamas and Palestinian Islamic Jihad (PIJ), and several Shia militias in Iraq, such as Kataib Hizballah and Asaib Ahl al-Haq. Several of these terrorist groups have been mobilized by Iran in support of the Syrian regime. Supporting these groups gives Iran regional leverage from the Levant and Gaza to Iraq. In addition to its sponsorship of terrorist groups, Iran continues to be a major regional and international security concern. Its activities in the areas of proliferation and offensive cyber operations continue, as does its support for the Syrian regime.

In September 2012, the Government of Canada severed diplomatic relations with Tehran and simultaneously designated the country as a sponsor of terrorism under the *Justice for Victims of Terrorism Act*. In December 2012, 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 May 2013, the Government of Canada announced additional sanctions against Iran under the *Special Economic Measures Act (SEMA)* and the cessation of virtually all economic activity with Iran. As of spring 2014, Canada and Iran have no formal diplomatic relations.

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. The Bulgarian authorities reported in 2013 that a dual Lebanese-Canadian citizen had participated in the July 2012 Burgas Airport bombing linked to Hizballah, which killed one Bulgarian and five Israelis. 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 southern 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 retains 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.

Terrorism and the Threat to Regional States: The Case of Iraq

Exploiting sectarian tensions and grievances, terrorist groups continue to pose a threat to states and to regional stability in the Middle East. Following the US withdrawal from Iraq in December 2011, sectarian tensions resurfaced as a result of the Syrian conflict, the escalating Sunni Islamist insurgency and the sectarian policies of the Shia-dominated Iraqi government. As violence surged, ISIL conducted operations in northwestern Iraq in early 2014 and expanded its offensive in early June 2014 with the capture of Mosul, Iraq's second largest city, and large swaths of Sunni-populated territory. The Iraq crisis has the potential to undermine the viability of the Iraqi state, exacerbate existing sectarian conflicts, and may provide ISIL with a base of operations from which to conduct new operations that threaten Canadian and Western interests.

Domestic Extremism

While small in number, extremists in Canada, motivated by an ideology or a political cause, are capable of orchestrating acts of serious violence. Left-wing extremists often operate in small cells or promote direct attacks against the capitalist system or modern civilization including sabotage of critical infrastructure. Right-wing extremist circles appear to be fragmented and primarily pose a threat to public order and not to national security.

Terrorist Financing, Financial Investigation and Listings

Terrorist organizations require financial resources in order to recruit and train followers to distribute propaganda and to carry out their attacks. Denying terrorists access to funds makes their activities more difficult and less likely to happen. The economics of terrorism are complex, however. Terrorist financing is frequently transnational in scope and may involve numerous actors using a multiplicity of practices. In order to counter such activity, counter-terrorism authorities 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 a group as a terrorist entity under the *Criminal Code*.

Canada presently has a total of 53 entities listed, the most recent additions being Al-Murabitoun, Al-Muwaqi'un Bil Dima, Movement for Oneness and Jihad in West Africa (MOJWA), and IRFAN-CANADA. Once a group has been designated as a terrorist entity, the group's assets in Canada are frozen and any financial and material support to the listed entities constitutes a criminal offence.

Illegal Migration

Canada remains a preferred destination for immigrants from around the world, thousands of whom come to Canada annually to create economic opportunities for themselves and for Canada. The unfettered movement of people, goods and services is also increasingly important to Canada's economic prosperity in a globalized economy. However, the business of human smuggling poses mounting risks in this context. Human smuggling networks, particularly those based in South and Southeast Asia, rely more and more on the worldwide, interconnected air travel system as a method of travel to North America. Most of the internationally disparate smuggling networks depend on large-scale document forgery, multiple facilitators and linkages of secondary associates providing global coverage. CSIS works closely with its domestic and foreign partners to mitigate the risks associated with illegal migration, in particular the potential exploitation of these networks by state and non-state actors.

Espionage and Foreign Interference

Protecting Canadian Sovereignty

While counter-terrorism remains a priority for the Service, during the period covered by this Report 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. As a result, Canada remains a target for traditional espionage activities, many of which continue to focus on our advanced technologies and government proprietary and classified information, as well as certain Canadian resource and advanced technology sectors.

Espionage Threats

A number of foreign states, with Russia and China often cited in the press as examples, continue to gather political, economic, and military information in Canada through clandestine means. Canada's advanced industrial and technological capabilities, combined with expertise in a number of sectors, make our country an attractive target for foreign intelligence services. Several key sectors of the Canadian economy have been of particular interest to foreign agencies, including but not limited to aerospace, biotechnology, communications, information technology, nuclear energy, oil and gas, as well as the environment. The covert exploitation of these sectors by foreign states, in order to advance their own economic and strategic interests, may come at the expense of Canada's national interests, including lost jobs and revenues, and a diminished competitive global advantage.

State-Owned Enterprises – With Opportunity Comes Risk

Highly developed and industrialized countries such as Canada face aggressive and increasing competition, lawful and otherwise, from developing nations determined to improve their economic standing. Among the most effective and least costly methods to achieve these goals is economic espionage. Other foreign-influenced activities include clandestine attempts to circumvent Canada's laws and policies, the compromise of loyalties of Canadians, penetration through cyber operations, and the pursuit of objectives that are detrimental to Canada's own economic security.

State-Owned Enterprises (SOEs) are commercial entities operated by foreign governments that can further the legitimate policy and economic goals of the nations they represent. Certain SOEs may, however, be used to advance state objectives that are non-transparent or benefit from covert state support such that competitors may be disadvantaged and market forces skewed.

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. These concerns include the consequences that may arise from foreign state control over strategic resources and their potential access to sensitive technology.

Foreign Interference

Canada is an open, multicultural society that has traditionally been vulnerable to foreign interference activities. When diaspora groups in Canada are subjected to clandestine and deceptive manipulation or intimidation by foreign states seeking to gather support for their policies, or to mute criticism, these activities constitute a threat to the security if not the sovereignty of Canada. 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 into the future.

Ukraine: Regional Crisis, International Implications

The crisis in Ukraine, which was triggered by mass protests against the Viktor Yanukovych government's plans to strengthen Ukraine's ties with Russia, turned violent in February 2014, and forced Yanukovych to flee the country. Russia responded by increasing its military presence in the Crimea, where a March 16 referendum ostensibly endorsed secession from Ukraine and paved the way for Russia's March 21 annexation of the peninsula. Russia also worked with members of the Russian minority in eastern Ukraine, who organized a self-proclaimed separatist entity. Since April 2014, Ukraine has conducted counter-insurgency operations against these separatist forces, who likely shot down Malaysian Airlines Flight MH17 over eastern Ukraine on July 17.

Russia's violation of Ukraine's sovereignty demonstrates its defiance of international norms. Its support for pro-Russian separatists in Ukraine has protracted the conflict, and contributed to regional instability. The Russian government continues to use the Ukrainian conflict to promote its security, economic and strategic interests - which may not coincide with Canadian and Western interests. The Government of Canada has clearly articulated its support for Ukraine, and on March 17, 2014, issued the Special Economic Measures (Russia) Regulations.

Cyber Security and Critical Infrastructure Protection

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. From these activities, it is clear that Canada remains a target for malicious, offensive cyber activities by foreign actors, who target the networked infrastructures of both the public and the private sectors, as well as the personnel using these systems. These actors are increasing in number and capability. Their cyber operations include surveillance, compromise, and exfiltration and exploitation efforts and are conducted for some form of gain, including the acquisition of proprietary information, data relating to business deals and assets, and public and private-sector strategic plans. A high-profile example of this was the cyber exploitation, in late June 2014, of the National Research Council of Canada (NRC) computer network, which forced it to shut down its information technology (IT) network and rebuild its information security framework.

Although attacks may come from the virtual realm, their consequences are very real. Increasingly, individuals, groups or organizations with malicious intentions are able to mount computer network operations (CNO) against Canada – through the global information infrastructure – without having to set foot physically on Canadian soil. These hostile actors include both state and non-state actors – such as foreign intelligence agencies, terrorists, or simply lone actors – who may also work together towards a common goal. Moreover, these hostile actors

have access to a growing range of malware tools and techniques. They frequently employ carefully crafted e-mails (known generally as "phishing"), 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 CNO. Foreign intelligence agencies use the Internet to conduct espionage, 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, almost all in support of wider espionage goals. The Government of Canada witnesses serious attempts to penetrate its networks on a daily basis. On the other hand, there are politically-motivated collectives of actors who will attempt to hijack computer networks to spread mischief or propagate false information; however, these do not necessarily represent a threat to Canada's national security.

CSIS is also aware of a wide range of targeting against the private sector in Canada and abroad. The targets of these attacks are often high-technology industries, including the telecommunications and aviation sectors. However, the Service is also aware of CNO against the oil and gas industry and other elements of the natural resource sector, as well as universities engaged in advanced research and development. In addition to stealing intellectual property, one of the objectives of state-sponsored CNO is to obtain information which will give their domestic companies a competitive edge over Canadian firms – including around investment or acquisition negotiations with Canadian companies and the Government of Canada.

There have also been recent cases of CNO, such as the 2012 computer network attacks (CNA) on Saudi Aramco which shut down 30,000 computers. This operation was reportedly aimed at disrupting oil and gas production and demonstrates expanding capabilities. Similar attacks on infrastructure targets in Canada could impact our way of life in very significant ways. The security of supervisory control and data acquisition (SCADA) systems and industrial controls systems (ICS), upon which the public and private sectors depend, is becoming increasingly important. Should such destructive cyber-operations be successfully targeted against systems in Canada, they could affect any and all areas of critical infrastructure.

The on-going conflicts in Ukraine and Syria have seen the use of destructive cyber capabilities deployed by state and sub-state actors – reminiscent of similar uses of cyber means to complement the real-world confrontations around the Georgian conflict in 2008, and against the Estonian state in 2007; similarly, the conflict between Israel, Palestinian groups, and Hizballah has long seen offensive cyber means used between the different combatants. While these conflicts may not present an immediate national security threat, given the instantaneous nature of global cyber transactions, foreign actors may stage an operation against a Canadian target with little forewarning. The Service works closely with other government departments and international partners in order to remain abreast of the global threat.

Weapons of Mass Destruction

Counter-Proliferation: 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 global challenge and a significant threat to the security of Canada and its allies. Whether proliferation is carried out by state or non-state actors, the pursuit of WMD increases global tensions and may even precipitate armed conflicts in some regions. Canada participates in several international fora and is a party to many international conventions and other arrangements designed to stem the proliferation of WMD. CSIS works closely with both domestic and foreign partners to uphold our country's commitment to the cause of non- and counter-proliferation.

Canada is a leader in many high technology areas, some of which are applicable to WMD programs. As a result, states of proliferation concern seeking to advance their own WMD programs have targeted Canada in an attempt to obtain dual-use technologies, materials and expertise. CSIS investigates these attempts to procure WMD-applicable technology within and through Canada, and in turn advises the Government of Canada 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 global 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. Under the Joint Plan of Action (JPA) concluded on November 24, 2013, Iran essentially froze its nuclear program in its current state, with some limited "roll-back" in regard to its stock of enriched uranium. The JPA took effect on January 20, 2014, and several rounds of negotiations aimed at reaching a comprehensive solution of the issue have occurred since then between Iran and the five permanent members of the United Nations Security Council plus Germany (P5+1). On July 18, 2014, the JPA was extended by four months, until November 24, 2014, to permit a continuation of the negotiations.

North Korea

North Korea has shown no serious inclination to "de-nuclearize," as called for by the international community. During 2013 North Korea resumed operation of its plutonium-producing reactor at Yongbyon. It is also building an experimental light-water reactor that could be an additional source of plutonium for weapons; and is greatly expanding its centrifuge facility at Yongbyon, capable of providing enriched uranium to further increase its nuclear arsenal. North Korea is also actively developing a wide range of ballistic missiles, including

a new road-mobile, intercontinental ballistic missile (ICBM) capable of reaching North America.

There is concern as to how this aggressive and unpredictable country may ultimately use its nuclear weapon capability. Many observers expect North Korea in the not-too-distant future to resume underground nuclear tests and flight tests of long-range ballistic missiles.

Other CBRN Issues

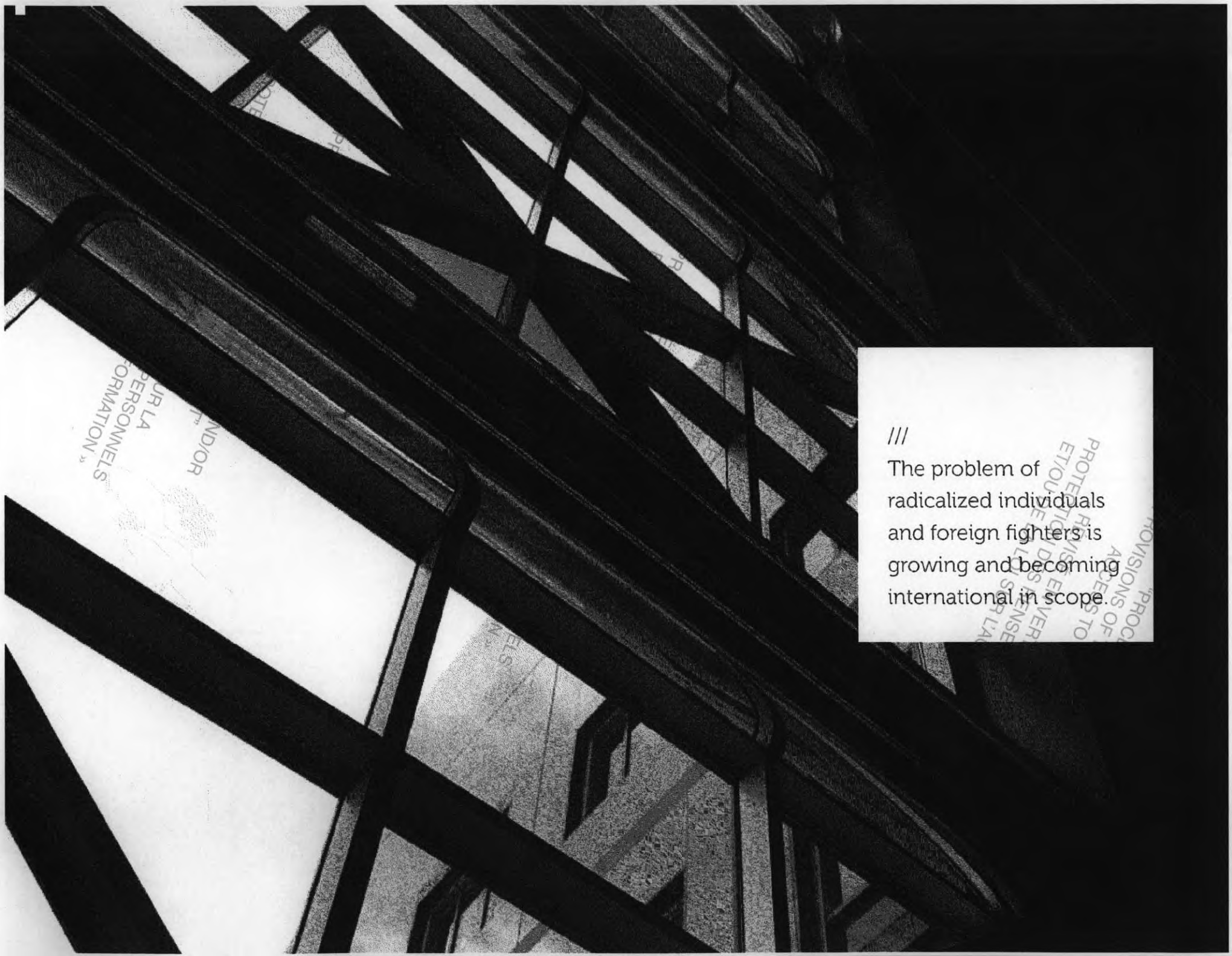
In South Asia, the rapidly expanding nuclear arsenal of Pakistan and questions over the security of those weapons systems given the domestic instability in that country remain principal concerns.

Despite the recent supervised destruction of Syria's declared chemical weapons (CW) stockpile, completed in mid-2014, the country is widely suspected of retaining some of its stocks and capability. It is also believed to have continued using chemical agents (such as chlorine) in small-scale attacks on its domestic opposition, in contravention of its new obligations under the Chemical Weapons Convention.

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 and peaceable country with a strong sense of the fundamental values and freedoms embedded in our way of life. However, there continue to be several 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 and the coercion and manipulation of diaspora communities. Terrorism and radicalization threaten the loss of life at home and abroad. The dynamics of the threat environment, as they are witnessed by the Service and briefly described above, will continue to be at play for the next year. Vigilance, adaptability and a continued partnership with the Government of Canada's Ministries and agencies and foreign partners will help mitigate both the domestic and the international threat environment for Canada.



///

The problem of radicalized individuals and foreign fighters is growing and becoming international in scope.

TERRORIST GROUP PROFILE: THE ISLAMIC STATE OF IRAQ AND THE LEVANT

The Islamic State of Iraq and the Levant (ISIL) originated in October 2004 as the AQ affiliate, Al-Qaeda in Iraq (AQI). AQI conducted several lethal terrorist operations against United States and Coalition forces and the Shia-dominated Iraqi authorities. In 2006 AQI rebranded itself as the Islamic State of Iraq, but following the outbreak of the Syrian conflict in April 2013 it again retitled itself as ISIL to emphasize its presence in both Iraq and Syria. It quickly became one of the leading Sunni Islamist militant groups in Syria, where it contested Jabhat al-Nusra (JN, the al-Nusra Front) for official status as the AQ representative. Disagreements between JN and ISIL compelled the AQ leader Ayman al-Zawahiri to intervene and side with the former. When ISIL defied the AQ Core leadership, the latter publicly disavowed the group in early February 2014.

ISIL launched a dramatic offensive in Iraq in early June 2014, which led to its capture of Mosul on June 10. It also seized a large part of Al Anbar, Diyala, Ninawa, and Salah ad-Din governorates. On June 29, 2014, ISIL announced the establishment of a Caliphate stretching from the Syrian governorate of Aleppo in the west to the Iraqi province of Diyala in the east, and renamed itself the "Islamic State." In the process, it has undermined the viability of the Iraqi state.

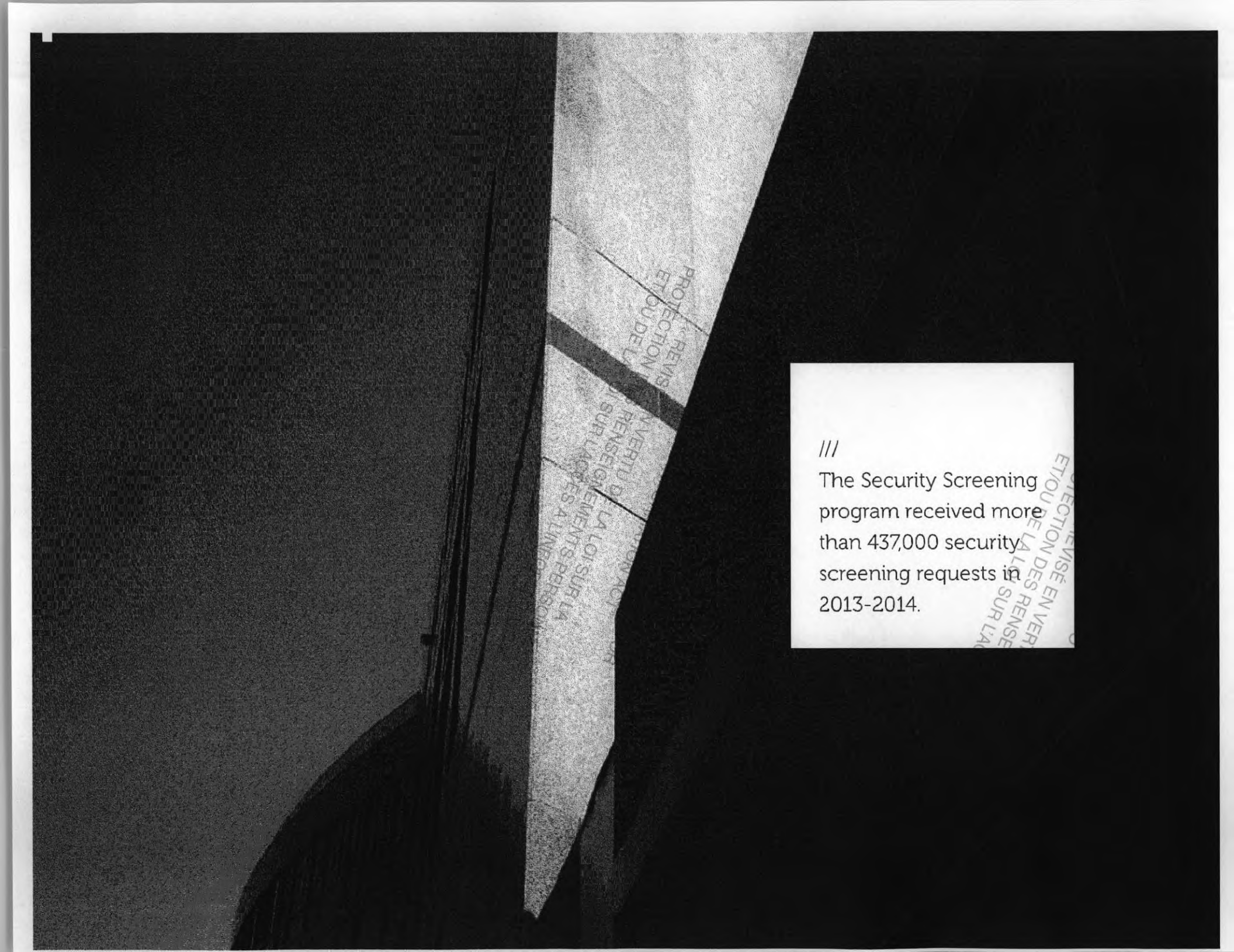
Even before its recent gains in Iraq, ISIL had acquired an infamous reputation for causing mass civilian casualties. There seems no limit to the group's capacity for committing grotesque acts of violence, such as the beheading of western journalists. ISIL will often film these horrific acts and incorporate the material into sophisticated propaganda campaigns with an international reach. Canadian extremists have featured prominently in ISIL propaganda.

Despite its rupture with AQ Core, ISIL has won the endorsement of some prominent ideologues and an oath of fealty from the Sinai-based entity, Ansar Bayt al-Maqdis (ABM). In Iraq, ISIL has several allies including a variety of former insurgents, Sunni tribal leaders and even former Baathist military officers. ISIL is financially autonomous, able to derive a variety of revenues from the territories it controls, including through kidnapping and extortion, and has recently gained additional military stockpiles in Iraq.

ISIL's violent message has won adherents from abroad. Several hundred and possibly thousands of foreign fighters, including radicalized Europeans, Australians and North Americans, have travelled to Syria

and Iraq to join the group. Some Canadians have been killed fighting alongside ISIL in Iraq and Syria. A French national who fought in Syria perpetrated a terrorist attack in Belgium in May 2014. The problem of radicalized individuals and foreign fighters is growing and is becoming international in scope.

In its previous Public Reports and elsewhere, CSIS has raised concern about the growing number of Canadian citizens who have left the country to participate in foreign terrorist activities. In light of the growing menace posed by ISIL and its ability to attract foreign fighters, CSIS again draws attention to this problem. No country can become an unwitting exporter of terrorism without suffering damage to its international image and relations. Furthermore, Canada has legal obligations to promote global security which must be honoured, which means assuming responsibility for its own citizens. The problem is not uniquely Canadian, but Canadians who travel to commit terrorism abroad are still very much a Canadian "problem." What is more, the foreign fighter phenomenon poses other security threats to our country. There is always the possibility that radicalized individuals who travel to support terrorism abroad will return to Canada, even more deeply radicalized than when they left, battle-hardened, and likely possessing new skills that could pose a serious threat to Canada and its citizens.



///

The Security Screening program received more than 437,000 security screening requests in 2013-2014.

SECURITY SCREENING

The CSIS Security Screening program helps defend Canada and Canadians from threats to national security, including terrorism and extremism, espionage, and the proliferation of weapons of mass destruction. Security Screening prevents persons who pose these threats from entering or obtaining status in Canada, or from obtaining access to sensitive sites, government assets or information.

One of the most visible of the Service's operational sectors, the Security Screening program, received more than 437,000 security screening requests from a wide variety of government clients in 2013-2014.

Government Security Screening

For government employees and some contractors employed by the government, their work entails having access to sensitive information and sites. As such, security clearances are a condition of their employment. In support of the Government of Canada departmental and agency decision-making on the granting, denial or revocation of security clearances, the Government Security Screening program conducts investigations and provides security assessments under the authority of sections 13 and 15 of the *CSIS Act*.

CSIS government security screening and security assessments address national security threats defined in section 2 of the *CSIS Act*, as well as criteria set out in the federal *Policy on Government Security (PGS)*, and other legislated requirements. While government screening security assessments play a critical role in the decision-making process concerning a security clearance, the PGS assigns client departments and agencies the responsibility for the decision to grant or deny such clearances.

CSIS government security screening also conducts screening to protect sensitive sites from national security threats, including airports and marine facilities, Ottawa's Parliamentary Precinct and nuclear power facilities.

Through its government screening program, CSIS also assists the RCMP with the accreditation process for Canadians and foreign nationals seeking access or participating in major events in Canada (for example, the 2015 Pan Am and Parapan Am Games in Toronto). Government security screening and security assessments are provided in support of the Canada-US Free and Secure Trade (FAST) program that helps expedite the movement of approved commercial drivers across the border.

Through reciprocal screening agreements, CSIS may also provide security assessments to foreign governments and international organizations (for example, NATO) concerning Canadians seeking employment which requires access to sensitive information or sites in another country. These reciprocal screening agreements are approved by the Minister of Public Safety after consultation with the Minister

of Foreign Affairs. As with all government employment-related clearances, Canadian citizens must provide their consent prior to screening being conducted.

Immigration and Citizenship Screening

CSIS' Immigration and Citizenship Screening program conducts screening investigations in order to provide security advice to the Canada Border Services Agency (CBSA) and Citizenship and Immigration Canada (CIC) regarding persons attempting to enter or claim status in Canada who might represent a threat to national security. Conducted under the authority of sections 14 and 15 of the *CSIS Act*, this screening supports the administration of the *Immigration and Refugee Protection Act* (IRPA) and the *Citizenship Act*.

Through this program, CSIS provides security advice on permanent residence and citizenship applicants; persons applying for temporary resident visas (whether visitors, foreign students or temporary foreign workers); and, persons applying for refugee status in Canada.

While CSIS provides advice to CBSA and CIC on potential threats to national security, CIC is responsible for decisions related to admissibility into Canada, the granting of a visa, or the acceptance of applications for refugee status, permanent residence or citizenship.

CSIS also works with Government of Canada partners in reviewing the national security component 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 focusing resources on legitimate threats to Canada and Canadians and helping to facilitate the travel of legitimate applicants.

Government: Screening in Action I

While conducting a security screening investigation for a federal government department, CSIS learned that an individual who required a secret clearance was known to have close personal associations with representatives of a foreign government that is engaged in espionage against Canada as defined in section 2(a) of the *CSIS Act*. Based on these associations, the Service assessed that the individual may engage in activities that pose a threat to the security of Canada. The requesting department accepted the assessment, and subsequently denied the individual's clearance and terminated the individual's employment.

While conducting a security screening investigation for a federal government department, CSIS learned that an individual who required a secret clearance had promoted the ideology of, and had worked for an organization suspected of providing funds to, a listed terrorist entity in Canada. The Service assessed that the individual may engage in activities posing a threat to the security of Canada. The requesting department accepted the assessment and subsequently denied the individual's clearance.

Immigration: Screening in Action II

CSIS information indicated a temporary resident visa (TRV) applicant was suspected of membership in an officially-recognized terrorist group and of facilitating relations between the group and a country of security concern. CSIS provided the Canada Border Services Agency (CBSA) with security advice in accordance with s.14 of the *CSIS Act*. In turn, CBSA recommended that the subject was inadmissible to Canada, and Citizenship and Immigration Canada (CIC) denied issuance of the TRV.

CSIS information indicated that a permanent resident (PR) applicant had been heavily involved in assaulting students as the head of a dissident monitoring group during his time as a student at a foreign university in a country of national security concern. The Service provided security advice to CBSA, and CBSA recommended that the subject was inadmissible to Canada.

Requests Received 2013-2014*

Permanent resident applications	61,600
Front-end screening**	8,500
Citizenship applications	208,800
Temporary resident applications	46,300

* Figures have been rounded.

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

Government Screening Programs 2013-2014*

Federal Government Departments	47,400
Free and Secure Trade (FAST)	13,800
Transport Canada (Marine and Airport)	37,100
Parliamentary Precinct	1,100
Nuclear Facilities	7,900
Provinces	240
Site Access–Others	4,000
Special Events Accreditation	0

* Figures have been rounded.

///

During 2013-2014, CSIS continued to share information on security issues with a wide variety of domestic partners.

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 2013-2014, 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 enforcement – the RCMP – collect evidence for criminal prosecution.

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

The international security environment continues to result in increased threats to Canada and its interests, both domestically and abroad. Ongoing conflicts in several regions of Africa, the Middle East, Asia, Eastern Europe and elsewhere showed no signs of abating during the 2013-14 period, and continue to have serious national and international

security implications. Worldwide incidents of terrorism, espionage, weapons proliferation, illegal migration, cyber-attacks and other acts targeting Canadians — directly or indirectly — remain ever present. Since the bulk of such threats originate from (or have a nexus to) regions beyond Canada's borders, CSIS needs to be prepared and equipped to investigate the threat anywhere.

While many such threats have existed for decades, others have emerged more recently. Kidnappings of Canadians and foreigners by terrorist groups — considered rare even a decade ago — have become much more commonplace, with such activity having occurred in countries such as Cameroon, Niger, Afghanistan, Colombia, Iraq, Somalia, Kenya, Pakistan and the Sudan. On the cyber front, foreign governments, terrorists and hackers are increasingly using the Internet and other means to target critical infrastructure and information systems of other countries.

Additionally, other, more familiar threats continue to evolve. The globalization of terrorism is expanding the breadth of radicalization, as individuals influenced by extremist ideology who were once content to support their extremist beliefs from afar — including a significant number of Canadians — are now travelling abroad to participate in terrorist activity, particularly (but not exclusively) to conflict zones. Those that fight and train with terrorist groups overseas could return to Canada with certain operational skills and experience allowing them to conduct domestic attacks themselves, or teach such techniques to fellow Canadian extremists. Others within Canada continue to be inspired and directed by those same terrorist entities to recruit and support their extremist ideology and activities. Espionage threats, often involving the usual suspects, have certainly not disappeared during this latest 'age of terrorism'. They have, in fact, become far more complex and increasingly difficult to detect and counter due to continuing advancements in technology and the globalization of communications.

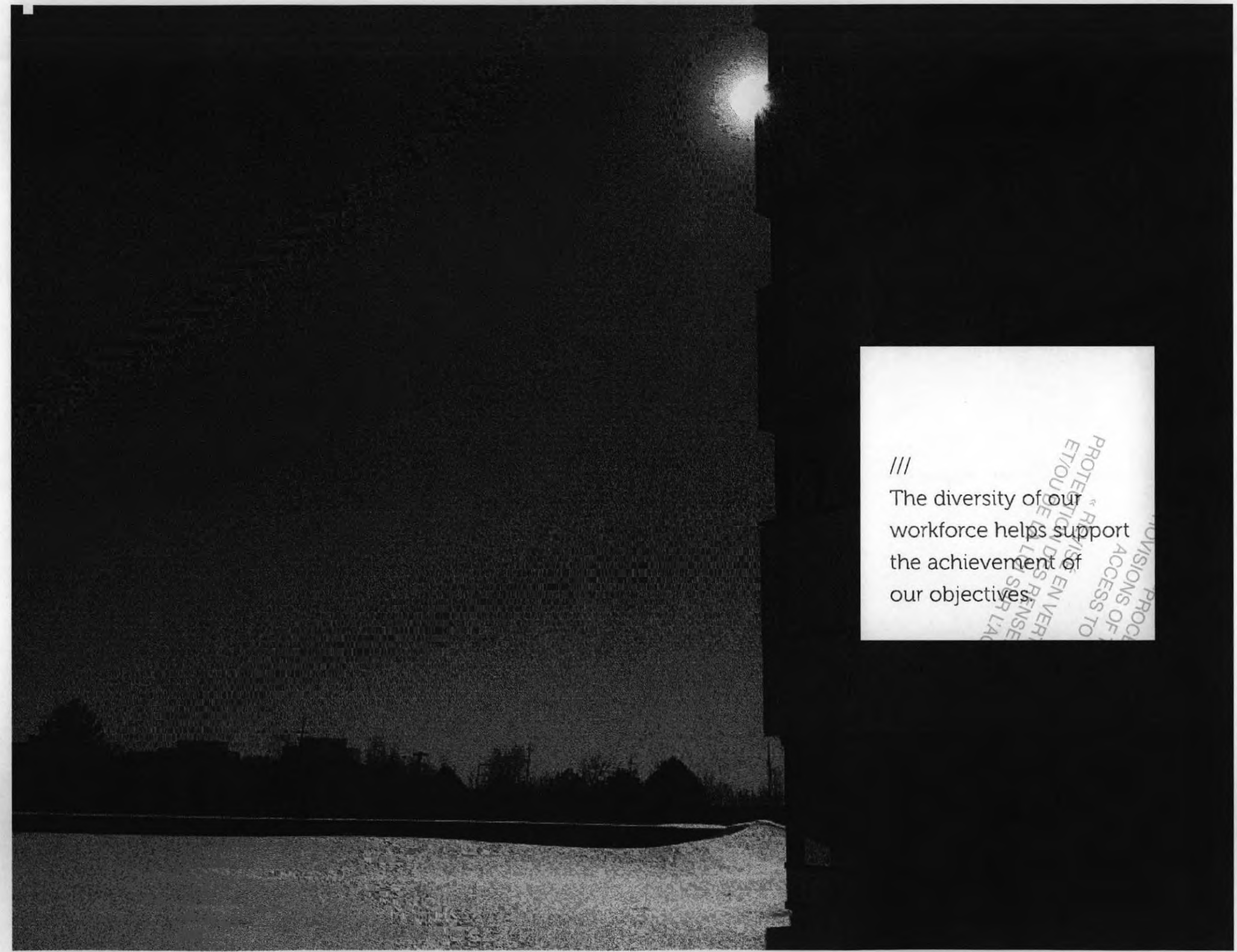
Whether countering traditional threats or newer ones, CSIS must remain adaptable in order to keep abreast of developments in both the domestic and international spheres. Despite differences in mandate, structure or vision, security intelligence agencies around the globe are all faced with very similar priorities and challenges. To meet the Government of Canada's priority intelligence requirements, CSIS has established information-sharing arrangements with foreign organisations. These arrangements provide CSIS access to timely information linked to a number of threats and allow the Service (and, in turn, the Government of Canada) to obtain information which might otherwise not be available.

As of March 31, 2014, CSIS had over 290 arrangements with foreign agencies or international organisations in some 150 countries and territories. This includes one new foreign arrangement approved during the 2013-2014 fiscal year by the Minister of Public Safety. Of those arrangements, 69 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 nine 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.

CSIS regularly assesses its foreign relationships, and reviews various government and non-government human rights reports and assessments for all countries with which the Service has implemented Ministerially-approved arrangements.

CSIS also has officers stationed in various cities around the world whose role is to collect and, when required, share security intelligence information related to threats to Canada, its interests and its allies with host 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).

CSIS remains committed to collecting security intelligence information — within Canada and abroad — on threats to Canada, its interests and those of our allied international partners.



///

The diversity of our workforce helps support the achievement of our objectives.

A UNIQUE WORKPLACE

Our People

The people of CSIS are committed to maintaining an organization that is adept, flexible and innovative in the delivery of its mandate and in the pursuit of its significant mission. This commitment is critical when operating in an environment that is continually changing and faced with ongoing fiscal restraints.

At the beginning of the 2013-2014 fiscal year, CSIS had over 3,000 full time employees divided evenly along gender lines. Collectively, our employees speak 109 languages. 68% of our employees speak both official languages and 20% 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 42 years. The Service employs individuals in a variety of settings and has employees working in different fields such as Intelligence Officers, Analysts, Engineers and Translators, to name a few.

The diversity of our workforce helps support the achievement of our objectives. It allows us to better understand the demographics of the Canadian communities we protect, therefore better equipping us to collect relevant and accurate intelligence. A diverse and inclusive work environment ensures an engaged workforce, innovative thinking and ultimately results in an increase in the quality of our products and services.

A number of human resources programs have helped transform our organization into the highly regarded, award winning agency that it is today. These programs continue to be a huge success, in terms of promoting innovation and employee engagement. One initiative from this past year gave CSIS employees the opportunity to 'pitch' their technology themed proposals directly to a panel of four senior Executives offering access to a designated reserve of funds and resources to help implement the chosen ideas. Recognizing the significant stress associated with relocation, another initiative was introduced, creating a new "one-stop shop" containing all related information for domestic and foreign relocations - now accessible to employees on a new intranet site. A new publication, directed towards managers, was introduced to provide timely and relevant information/ tips on various topics for those in a supervisory role in order to help enhance management and leadership skills within the Service ranks. In addition to these initiatives, the Service held its fourth annual Professional Development Day, along with the development of an extensive Wellness Program, which incorporates new initiatives with respect to mental and physical wellness.

CSIS is recognized as an employer of choice, not just because the work we do is inherently interesting, but because we have a progressive

workplace culture where our employees are recognized for their skills, talents and contributions. For seven years running, we have been named one of Canada's Top 100 Employers. The Service has also been named one of the National Capital Region Top Employers for seven consecutive years. We were named one of the Top Employers for Canadians over 40 from 2009 to 2013 and finally, in 2013, we were honored as one of Canada's 10 Most Admired Corporate Cultures. We pride ourselves as being a career employer and are proud to say that our resignation rate has remained under 1% over the last 10 years.

The Service recognizes that learning and training are essential components of a successful organization as well as imperative tools to continually renew and retain our employees. As such, CSIS continues to invest in ongoing learning for all employees. Our vision is to provide all employees, regardless of their function, level or location, with opportunities to learn from the day they arrive in the Service to the day they leave. Learning Paths for each occupational group are accessible to all employees across the Service. Individual Learning Plans are currently being piloted, and a Service-wide launch is anticipated for early 2015. These personalized plans will enable employees and supervisors to collaboratively map out an employee's learning and development.

The Service understands the value of "e-learning" and how it can be incorporated with other training methodologies to enhance overall learning (i.e., videoconference, mentoring, instructor-led, virtual, simulation and online). Although e-learning is not compatible for every type of course content, it is at the forefront of our learning strategy.

CSIS has a specialized in-house group consisting of e-learning specialists and instructors who are responsible for the design, development and delivery of in-house virtual / simulation and online training. Cutting edge hardware/software is used extensively for this purpose.

More than 100 leadership development, software training, professional development, and operational online courses have been made available to employees at all levels via the Learning Management System. As a result, employees have 24/7 access to courses from external vendors and key partners – right at their desktops - to enhance their knowledge and skills, for their current and future roles. This new approach has increased access, reach and timeliness of training.

A number of our classrooms have been equipped with smart boards, which are actively being used for course design and delivery. CSIS has constructed an in-house Simulation / Virtual Training Lab, which houses state-of-the-art equipment, and is utilized within many of our courses.

An updated Management Development Program (MDP) was launched to better identify and develop managers to support the Service's organizational and operational objectives. Participants are given the opportunity, over a period of up to 5 years, to acquire leadership knowledge, know-how, and abilities through challenging assignments, leadership development, and mentoring.

Over the last two years, the Service introduced a new integrated succession planning process which allows for a 5 year forcast period. This initiative, directed towards Service executives, allows for better talent analytics in order to predict and manage executive staffing actions and development.

Finally, the CSIS Strategic Priorities align with and support the Clerk of the Privy Council's Blueprint 2020 vision and pillars.

Recruitment

Recruiting and Staffing has streamlined its internal Career Opportunities (CO) and external recruiting to ensure that the Service has the right talent to deliver on our mandate.

Our national recruiting strategy continues to move forward across Canada. A more modern approach to recruiting continues to place technology at the forefront by using social media outlets such as Twitter and LinkedIn and other innovative recruiting strategies with IT professionals being our main focus.

The Service undertook, for the first time, a targeted recruiting blitz in the Greater Toronto Area in September 2013 to attract IT professionals to apply at csiscareers.ca. The initiative resulted in many advertising firsts for CSIS. Most notably:

- Radio ads
- posters in the TTC (subway);
- Digital ads in the office network and restaurants;
- "Open doors" style career information sessions; and
- Direct mail campaign through LinkedIn sent to 6,000 IT professionals.

Our recruiting activities and targeted messaging have increased awareness surrounding our role and mandate, which in turn, has resulted in well-suited candidates applying for positions.

We have received more than 100,000 CVs in the past two years and more than 1,000,000 hits to csiscareers.ca. Twitter is now used as a regular marketing tool to announce events attended by CSIS recruiters. Tweets are sent out every week to invite potential applicants to come and meet the recruiters.

In early 2014, a call went out to the general public to come and meet CSIS recruiters in the Ottawa and Gatineau area. This is the first time CSIS hosted its own event. The initiative attracted more than 1,200 people over eight sessions – triple the anticipated amount. Hits to csiscareers.ca went up 40% the week of the event.

In 2013-14, the Service attended 85 booth-space events across Canada, ran 37 advertising spots, held 33 career information sessions and attended 12 networking events.

The student co-op program is an important part of CSIS's recruiting strategy. A full-time co-op coordinator was assigned in 2012. In just two short years, CSIS received close to 1,700 applications from

university and college co-op students across Canada; of the students selected for co-op terms, 74% were hired full time upon graduation. Students hired by CSIS have the opportunity to participate in:

a) "meet and greet" with the CSIS Director;
b) "speed networking" session where co-op students meet senior CSIS managers;
c) Direct communication with the Co-op Coordinator; and
d) Informal networking and team building activities.

At CSIS, the development, growth and retention of our employees are a priority. Therefore we strive to offer promotional opportunities to our employees first. Annually, the Service hosts a Professional Development Day where employees have the opportunity to:

- Explore the various career opportunities that exist within the Service.
- Discover the types of skills and experience required for a job/career that may be of interest.
- Learn about the roles and functions of other branches/regions within the Service.
- Attend presentations

Financial Resources

CSIS's final expenditures for 2012-2013, the last period for which figures are available, amounted to $496 million.

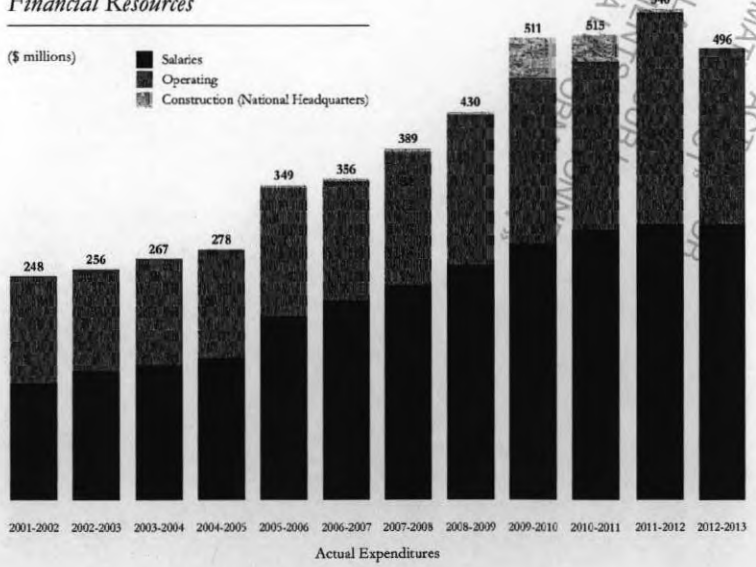
The Service's financial resources increased from 2001-2002 to 2011-2012, partly as a result of new funding for public security and anti-terrorism initiatives allocated in the December 2001 Federal Budget. Funding was also provided to augment the Service's foreign collection capabilities, to administer 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.

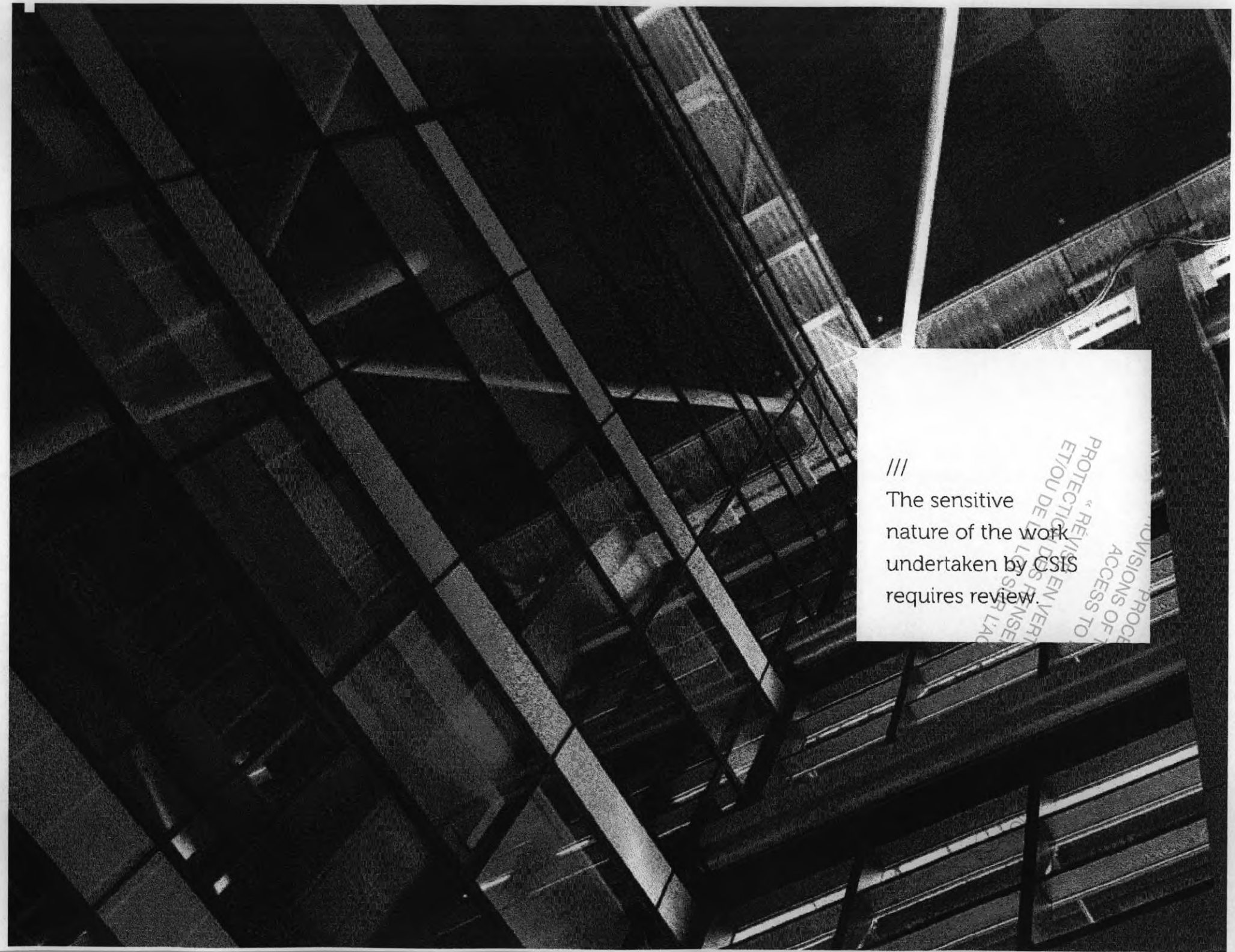
Construction costs shown are for the expansion of CSIS National Headquarters. Costs incurred from fiscal year 2003-2004 to 2006-2007 represent expenditures associated with the project definition stage. In 2007-2008 and 2008-2009, costs incurred were mainly attributable to the building's site preparation. The construction of Phase III began in the summer of 2009, with total expenditures of $4.9 million in 2011-2012. Phase III was officially opened by the Minister of Public Safety in October 2011.

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, CSIS' budget was reduced by an additional $13.7 million in 2012-2013. Further reductions of $20.2 million were realized in 2013-2014. Reductions will increase to $24.5 million in 2014-2015 and moving forward.

Financial Resources





///

The sensitive nature of the work undertaken by 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 some of its responsibilities to SIRC, in particular the annual certificate. SIRC is also now required to brief the Minister at least once a year on the Service's duties and functions.

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 a majority 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*.

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.

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 and senior management.

In 2012-2013, the ATIP Unit conducted a number of awareness sessions for a number of managers and specialized groups. In addition, as part of CSIS' E-learning initiative, an ATIP awareness video was developed. This video is a requirement for all new employees and acts as a reference for all others. The objective of the sessions and the video was to provide employees 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.

During the last fiscal year, the CSIS ATIP Unit received a total of 350 requests under the *Privacy Act* and 913 requests under the *Access to Information Act*. The Service's on-time completion rate was 96% for Privacy requests and 97% for Access requests.

CSIS Internal Audit Branch / Disclosure of Wrongdoing and Reprisal Protection

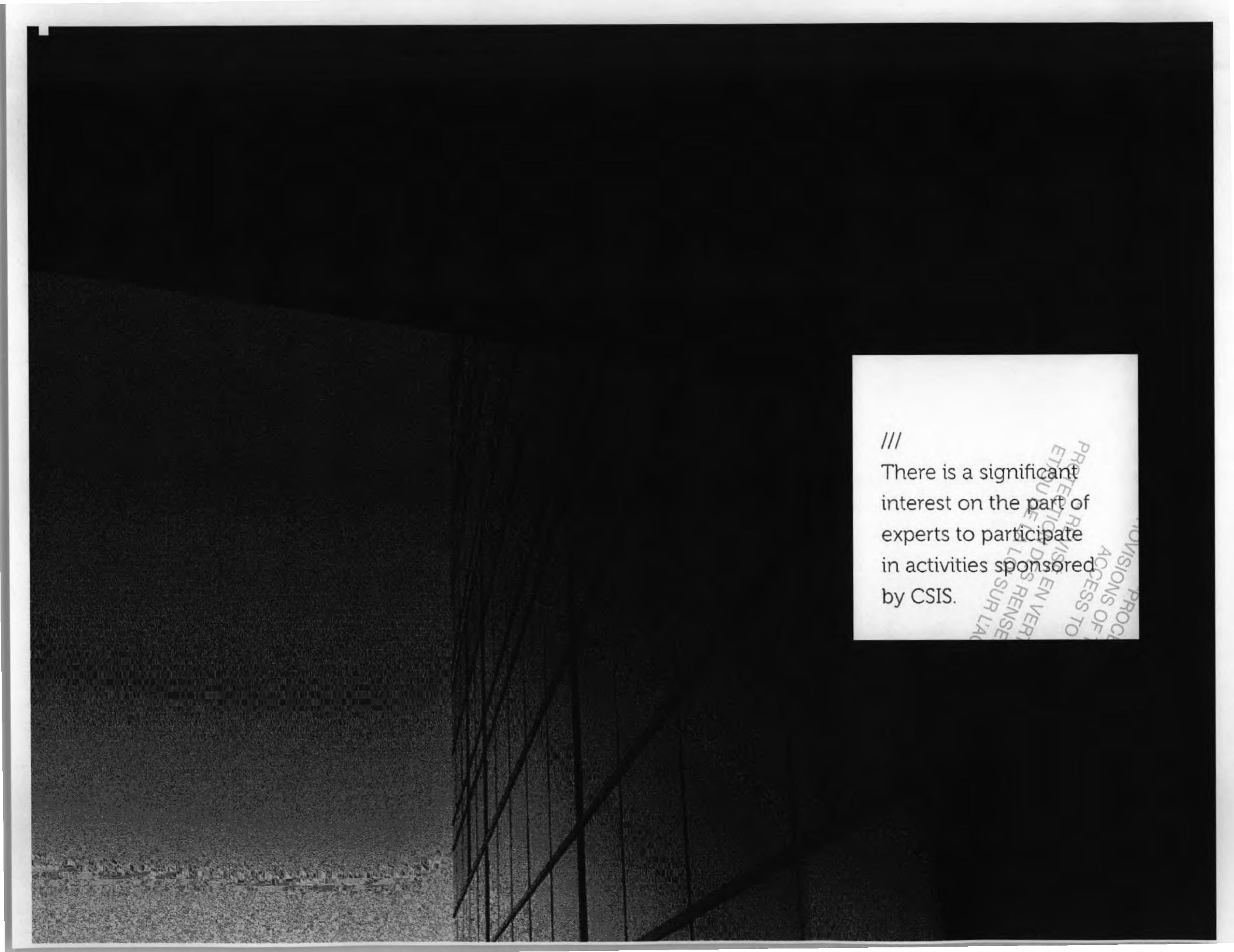
The Internal Audit (IA) Branch is led by the Chief Audit Executive (CAE), who reports to the CSIS Director and to the CSIS External Audit Committee (AC). The CAE provides assurance services to the Director, Senior Management and the AC, as well as independent, objective advice and guidance on the Service's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

The AC continued to bring about improvements to the delivery of assurance services by examining CSIS' performance in the areas of risk management, control 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 have also been recognized by the Treasury Board Secretariat in context of the Management Accountability Framework, which has continued to rate the audit function as "Strong", the highest possible rating.

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.



///
There is a significant interest on the part of experts to participate in activities sponsored by CSIS.

SPEAKING TO CANADIANS

The Public conversation on National Security: Media and Public Liaison

In today's environment, our mission statement to protect Canada's national security interests and the safety of Canadians resonates with the people of CSIS more than ever. The men and women of CSIS take pride in carrying out this role, and they also recognize that to do so effectively requires engaging in a dialogue with citizens, organizations, communities, and the media across the country and around the world.

Historically, CSIS has not always had a visible public presence, owing to the assumption that intelligence services are supposed to operate "in the shadows". A low or non-existent profile was perhaps considered a good thing, and as such there was little need for an active media and public liaison office. Over the last decade, however, that perspective has changed. Whether intelligence services like it or not, in the era of social media and cable news the conversation about domestic and global security is a public one – and ordinary citizens rightly feel they have a stake in that conversation.

The role of the Service's media and public liaison is to help educate Canadians about issues of national security that matter to them. At times this can be challenging due to the fact that CSIS cannot disclose specific details about our investigations, methodologies, or activities. But we can – and we are – helping to raise security awareness, and also to demystify some of our own work.

We often say that while CSIS is the keeper of many secrets, we need not be a secret organization. Where we can find appropriate opportunities to promote an informed dialogue about the security environment, we try to take them.

The Service recognizes that our ability to operate effectively depends on our having the public trust. And the Service also recognizes that organizations that practice transparency, to the extent they can, typically enjoy more trust than organizations that don't.

Academic Outreach

The Academic Outreach program at CSIS seeks 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, etc. – to identify new avenues of research.

Academic Outreach (AO) hosted two conferences in 2013-2014 that brought together multi-disciplinary groups of experts from several countries. The first conference was entitled "Political Stability and Security in West and North Africa" and examined the drivers of violent extremism in this region. The second conference, held under the theme of "Pitfalls and Promises: Security Implications of a Post-revolutionary Middle East", anchored a broad discussion of the Middle East in an exploration of the Syrian civil war and the dynamics refashioning Egypt's political landscape.

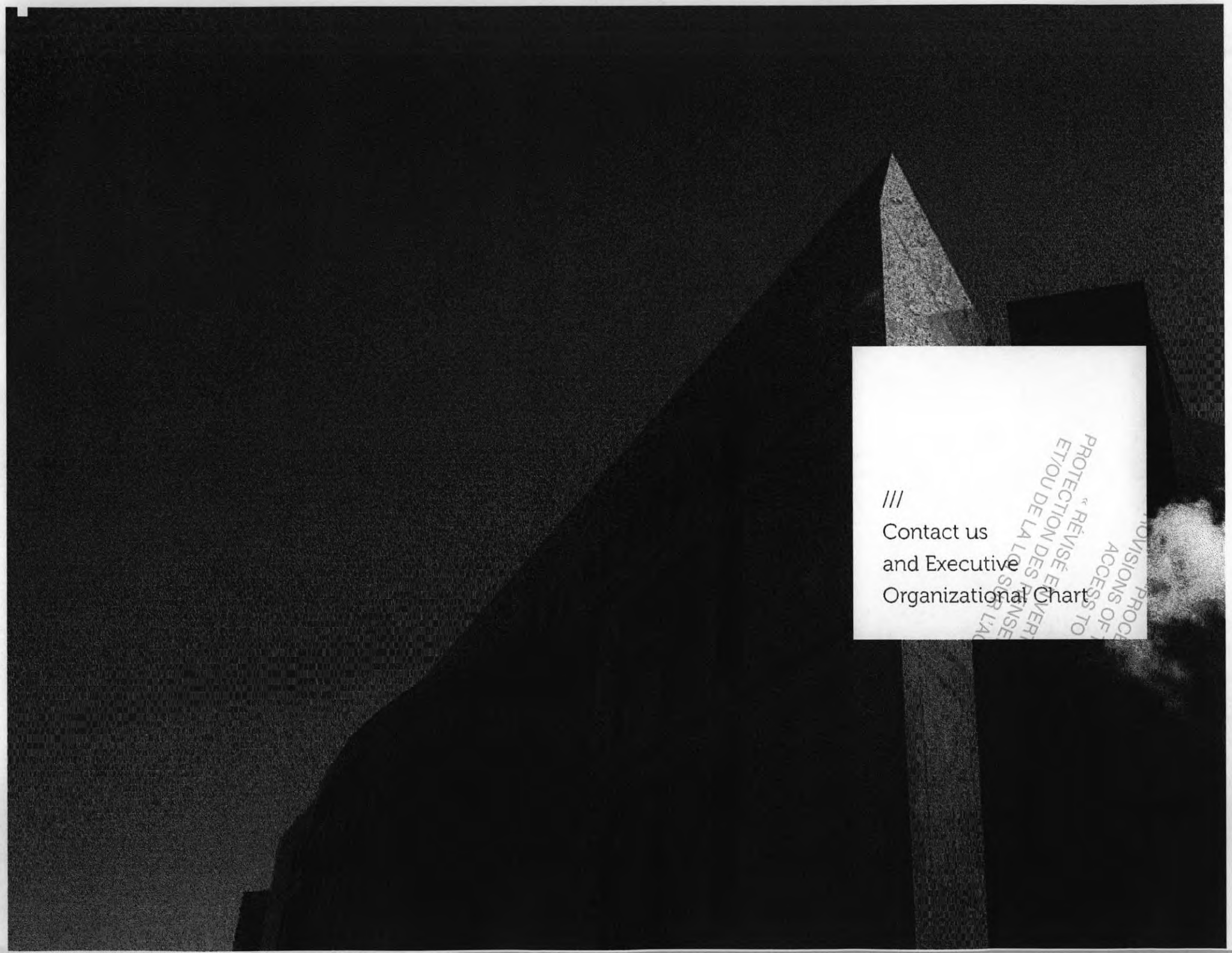
The international conferences, however, represent only one component of the AO program. We also hosted a number of in-depth briefings on other topics of interest. For instance, one examined the potential implications of the withdrawal of NATO forces from Afghanistan. The speaker's knowledge, based on years of experience and much field research work, outlined scenarios as to the future of the country. Another briefing looked into the evolving interests and designs of Russia towards the Middle East.

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 eleven 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 2013-2014, outside experts engaged CSIS staff on discussions covering a range of security and strategic issues, including: the results of the June 2013 Iranian elections; the evolving phenomenon of the extremist travellers, otherwise known as "foreign fighters"; Hizballah's tactics and ambitions; China's Arctic strategy; and Iran's nuclear program.

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 program also serves as an important tool of strengthening partnerships with foreign organisations; its last conference on West and North Africa was designed and organised jointly with the United Kingdom's Cabinet Office. 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.



///

Contact us and Executive Organizational Chart

/// 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:

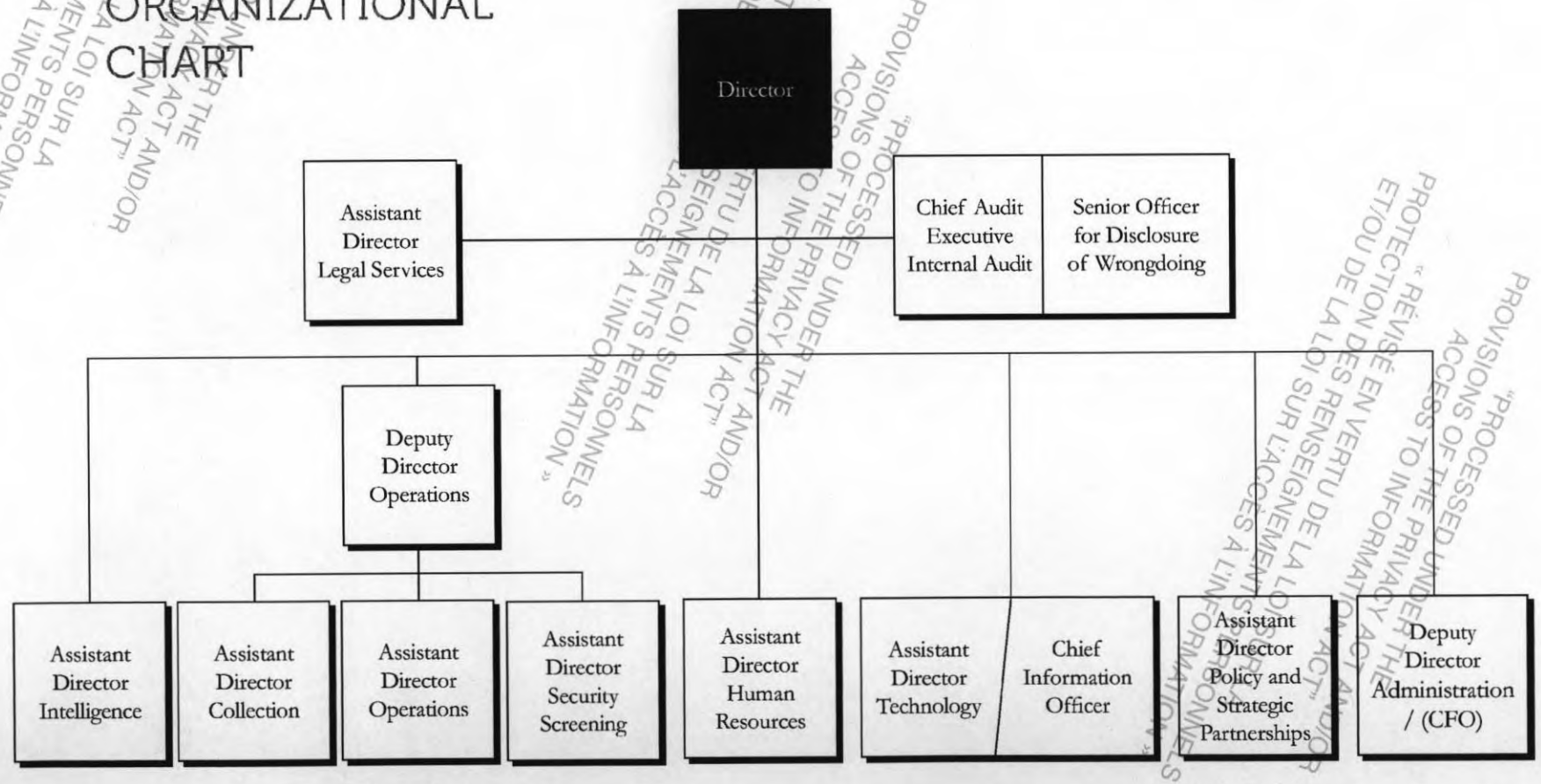
CSIS Communications Branch
P.O. Box 9732, Station T
Ottawa ON K1G 4G4
Tel. 613-231-0100

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, St-Jacques Station 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



NOTES

Canadian Security Intelligence Service
Service canadien du renseignement de sécurité

CSIS PUBLIC REPORT 2019

A safe, secure and prosperous Canada through trusted intelligence and advice.
Des renseignements et des conseils fiables pour un Canada sûr et prospère.

Canada

Aussi disponible en français sous le titre : Rapport public du SCRS 2019
www.canada.ca

Published in April 2020

CSIS PUBLIC REPORT 2019

3103(18/09)

TABLE OF CONTENTS

3103(18/09)

CONFIDENCE

OUR
VISION

A SAFE, SECURE AND PROSPEROUS CANADA THROUGH TRUSTED INTELLIGENCE AND ADVICE.

3103(18/09)

MESSAGE FROM
THE DIRECTOR

On July 16, 2019, CSIS employees from coast to coast celebrated our 35th anniversary a little older, a great deal wiser and more proud than ever before about how we have come together to protect the security of Canada at home and abroad. As Director, I take enormous pride in the fact that, thirty five years on, CSIS continues to demonstrate its value to Canadians by providing the Government with crucial information and advice linked to threats to the security of Canada and our national interests.

In June 2019, the *National Security Act, 2017* received Royal Assent and became law. This legislation modernized the original *CSIS Act* by addressing outdated legal authorities, introducing new safeguards and accountability measures as well as clarifying CSIS' responsibilities. While this has addressed specific challenges and provides some new modern authorities, there is still work to be done.

CSIS must continue to provide timely and relevant intelligence to Government. Going forward, that will require a renewed vigilance in assessing whether our current authorities are keeping pace with continuous changes in the threat, technological and legal landscape. Much has changed since our formation in 1984. Our authorities must evolve with the world around it and keep pace with changes.

Whether it's al-Qaida, Daesh or Blood and Honour, CSIS remains seized with the threat these groups pose to Canadians at home and abroad. These groups continue to be powerful influencers who can shape the pace and direction of mobilization through their efforts to inspire, enable and direct violence globally. These and other like-minded groups can reach into Canadian communities to encourage individuals to carry out acts of terrorism, domestically or abroad. The threat posed by those who have travelled for nefarious purposes and who then return to Canada continues to be a priority for CSIS.

As the world becomes smaller and more competitive, nation states are naturally seeking every advantage to position themselves as leaders in a lucrative global economy. As a result of this competitive thirst, hostile state actors seek to leverage all elements of state power to advance their national interests. This threat represents the greatest danger to Canada's national security and can have a tremendous impact on our economic growth, ability to innovate, sovereignty and national interest. That is why CSIS is now routinely engaging with a variety of stakeholders across the Government of Canada and the private and research sectors, to learn from and advise on the nature of potential threats so that they are better prepared and can protect their important work.

As we have seen elsewhere in the world, democratic institutions and processes, including elections, are valuable targets for hostile state actors. Our country is not immune to threat activities in this area. In the lead up to the 2019 Federal Election, CSIS was a key member of the Security and Intelligence Threat to Elections (SITE) Task Force. As a member of the task force, CSIS collected information about foreign interference and provided advice, intelligence reporting and assessments to the Government about hostile state activities that could pose a

3103(18/09)

threat to the election. CSIS' threat reduction mandate provided the Government of Canada another tool to respond to threats, including foreign influenced activity, if required. Finally, CSIS participated in briefings to political parties, Elections Canada and the Commissioner of Canada Elections on the threat of foreign interference to ensure Canadians could participate freely and fairly in the democratic process.

SITE is now seen as a model for our allies around the world on how different departments and agencies within government can work together and leverage their own unique authorities to ensure free and fair elections for their citizens.

The variety and complexity of threats Canada continues to face means that CSIS must continue to recruit a new generation of professionals who have the skills, knowledge and commitment to work in security and intelligence. Our workforce is more diverse than ever before. Employees with different life experiences and backgrounds bring new ideas and make CSIS stronger. Our commitment to diversity and inclusion is at the core of CSIS — because it is not just important, it's a matter of national security. It is our diversity that allows us to better understand all the Canadian communities we protect. The work of making CSIS more representative of Canada is never finished.

My focus as Director has been to ensure all our employees come to work every day in a safe, healthy and respectful environment. With that in mind, I am very proud of the progressive changes that we have introduced to improve workplace policies and practices through a modern people strategy. It is incredibly important that every employee at CSIS understands that they play a crucial role in our mission to keep Canada and Canadians safe from threats at home and abroad and that they are well-supported by the organization. We recognize that there is more work to be done and will continue to make every effort to ensure our employees feel respected and valued.

Transparency and accountability are the hallmarks of a modern intelligence service. That is why CSIS welcomed changes introduced through the *National Security Act, 2017* to help bolster our already robust oversight and accountability mechanisms. In order for CSIS to do its important work of keeping Canadians safe from threats at home and abroad, we must have the trust of Canadians. It is a responsibility we do not take lightly and work hard to earn every day. Though the *National Security Act, 2017* made significant and critical changes to our legal mandate, the threat environment we face today and in the future requires further reflection to ensure that we have the tools required of a modern intelligence agency.

As part of CSIS' ongoing commitment to public accountability, I welcome the tabling in the House of Commons of this CSIS Public Report, which provides an opportunity to report on our priorities and activities during 2019. CSIS will continue to fulfill our mandate of keeping Canada and Canadians safe – and do so in a way that is consistent with Canada's values and the trust Canadians place in us.

David Vigneault, Director

3103(18/09)


RELEVANCE

CSIS AT A GLANCE

CORE MANDATE

- Investigate activities suspected of constituting threats to the security of Canada.
- Advise the Government of these threats.
- Take lawful measures to reduce threats to the security of Canada.

THREATS TO THE SECURITY OF CANADA

- Terrorism and violent extremism
- Espionage and sabotage
- Foreign influenced activities
- Subversion of government

PARTNERSHIPS

- Nearly 80 arrangements with domestic partners
- Over 300 arrangements with foreign partners in 150 countries and territories

ACCOUNTABILITY

- Canadian Public
- Minister of Public Safety and Emergency Preparedness
- Federal Court
- Attorney General
- National Security and Intelligence Review Agency
- Intelligence Commissioner
- National Security and Intelligence Committee of Parliamentarians
- Auditor General
- Privacy Commissioner
- Information Commissioner
- Commissioner of Official Languages

DUTIES AND FUNCTIONS

- Investigate activities suspected of constituting threats to the security of Canada and report on these to the Government of Canada.
- Take measures to reduce threats if there are reasonable grounds to believe the activity constitutes a threat to the security of Canada.
- Provide security assessments on individuals who require access to classified information or sensitive sites within the Government of Canada.
- Provide security advice relevant to the exercise of the *Citizenship Act* or the *Immigration and Refugee Protection Act*.
- Conduct foreign intelligence collection within Canada at the request of the Minister of Foreign Affairs or the Minister of National Defence.

3103(18/09)

DEPARTMENTAL RESULTS FRAMEWORK AND FINANCIAL REPORTING

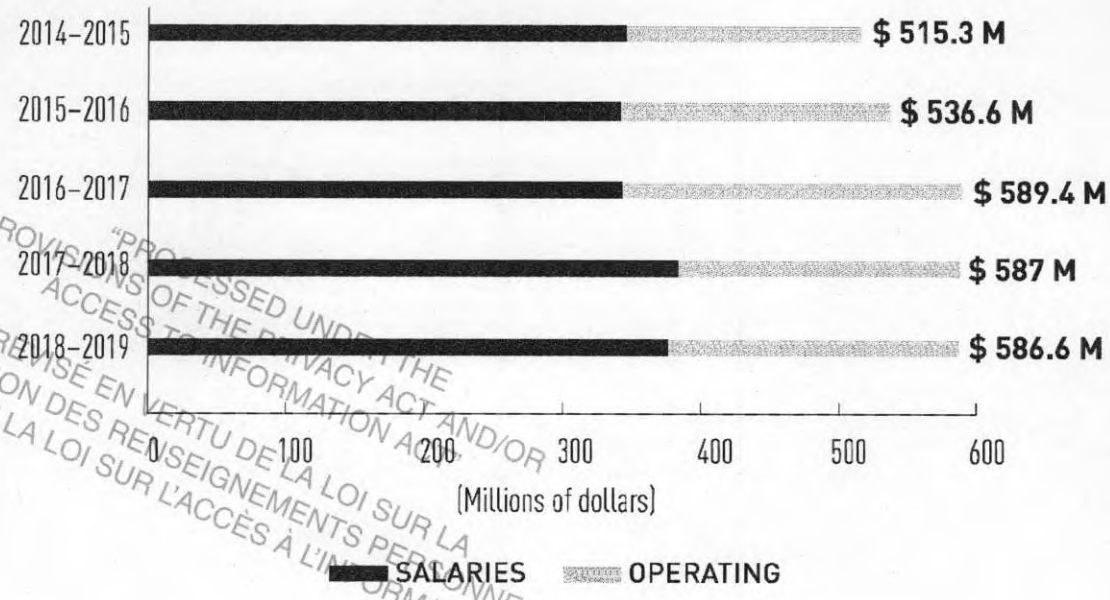
DEPARTMENTAL RESULTS

CSIS obtains relevant information and intelligence to carry out its national security activities.	CSIS intelligence informs government decisions and actions relating to Canada's security and national interests.	CSIS threat reduction measures diminish threats to the security and safety of Canada and Canadians.	The assessments of the Integrated Terrorism Assessment Centre (ITAC) inform Government of Canada's decisions and actions relating to the terrorism threat.

PROGRAM INVENTORY

Operational Program Management	Regional Collection	Operations Enablement	Intelligence Assessment and Dissemination	Security Screening	Integrated Terrorism Assessment Centre

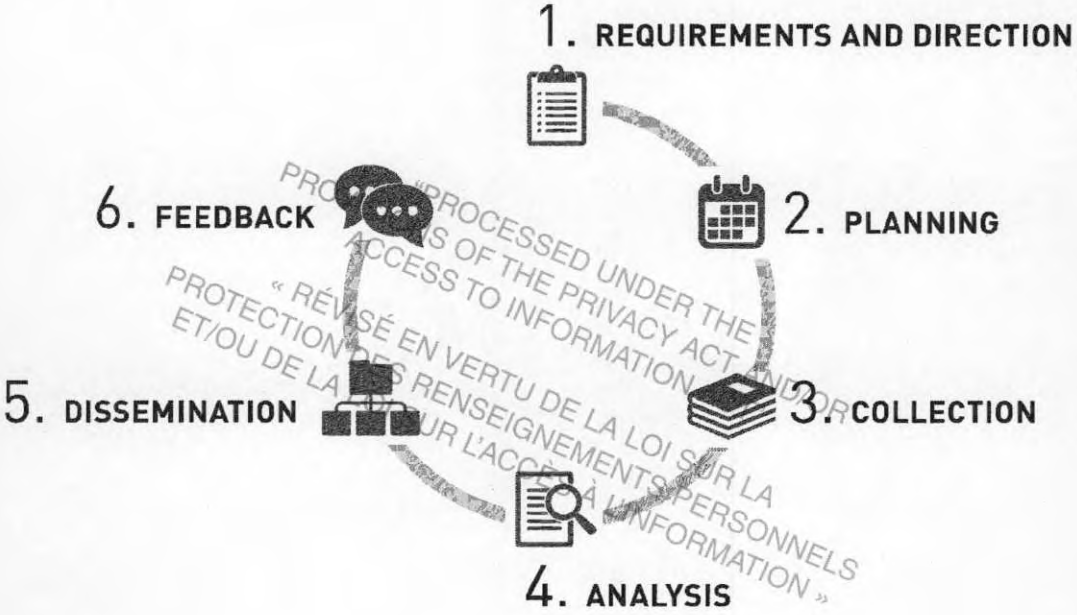
ACTUAL EXPENDITURES



3103(18/09)

THE INTELLIGENCE CYCLE

CSIS gathers intelligence and disseminates its assessments to appropriate government clients using a process known as the "intelligence cycle."



REQUIREMENTS AND DIRECTION

The *CSIS Act* gives CSIS the mandate to investigate activities suspected of constituting threats to the security of Canada, including espionage, terrorism, violent extremism, foreign influenced activities and subversion of government through violence.

Through this mandate, CSIS receives direction from the Government of Canada on the intelligence requirements:

- Government Intelligence Priorities as established by Cabinet through discussion and consultation with the relevant Ministers and the Security and Intelligence community.
- Minister's Direction on Intelligence Priorities, which translates the Government Intelligence Priorities into specific collection direction for CSIS.

3103(18/09)

PLANNING

The Government and Ministerial Direction on Intelligence Priorities, the *CSIS Act* and the needs of domestic partners are all taken into consideration when developing the annual collection strategy.

Responding to this direction, CSIS establishes internal direction and annual collection plans to meet the intelligence needs of Canadian government departments and agencies.

COLLECTION

CSIS uses a variety of methods to collect information on threat actors whose activities are suspected of constituting a threat to national security.

This information is collected from various sources, including:

- Open sources
- Members of the public
- Human sources
- Foreign governments
- Canadian partners
- Technical interception of communications

Any intrusive measure, or those affecting the privacy of Canadians, requires obtaining a warrant authorised by the Federal Court.

ANALYSIS

CSIS analysts use their knowledge of regional, national and global trends to assess the quality of all types of information collected. The information is analysed in order to produce useful intelligence for clients and consumers.

CSIS analysts examine the information provided by other Canadian government departments and agencies, foreign intelligence agencies, intelligence collected through investigations, as well as open sources. The analysis process results in intelligence reports and threat assessments.

DISSEMINATION AND FEEDBACK

CSIS disseminates intelligence products primarily to the Government of Canada and law enforcement authorities. CSIS also disseminates intelligence to its global intelligence alliance with the United States, United Kingdom, Australia and New Zealand, also known as Five Eyes partners, as well as other foreign partners.

An integral part of the intelligence cycle is collecting feedback on intelligence products from all partners. CSIS gathers product specific feedback from all partners and routinely gathers requirements from the Government of Canada to help shape and drive collection and production efforts.

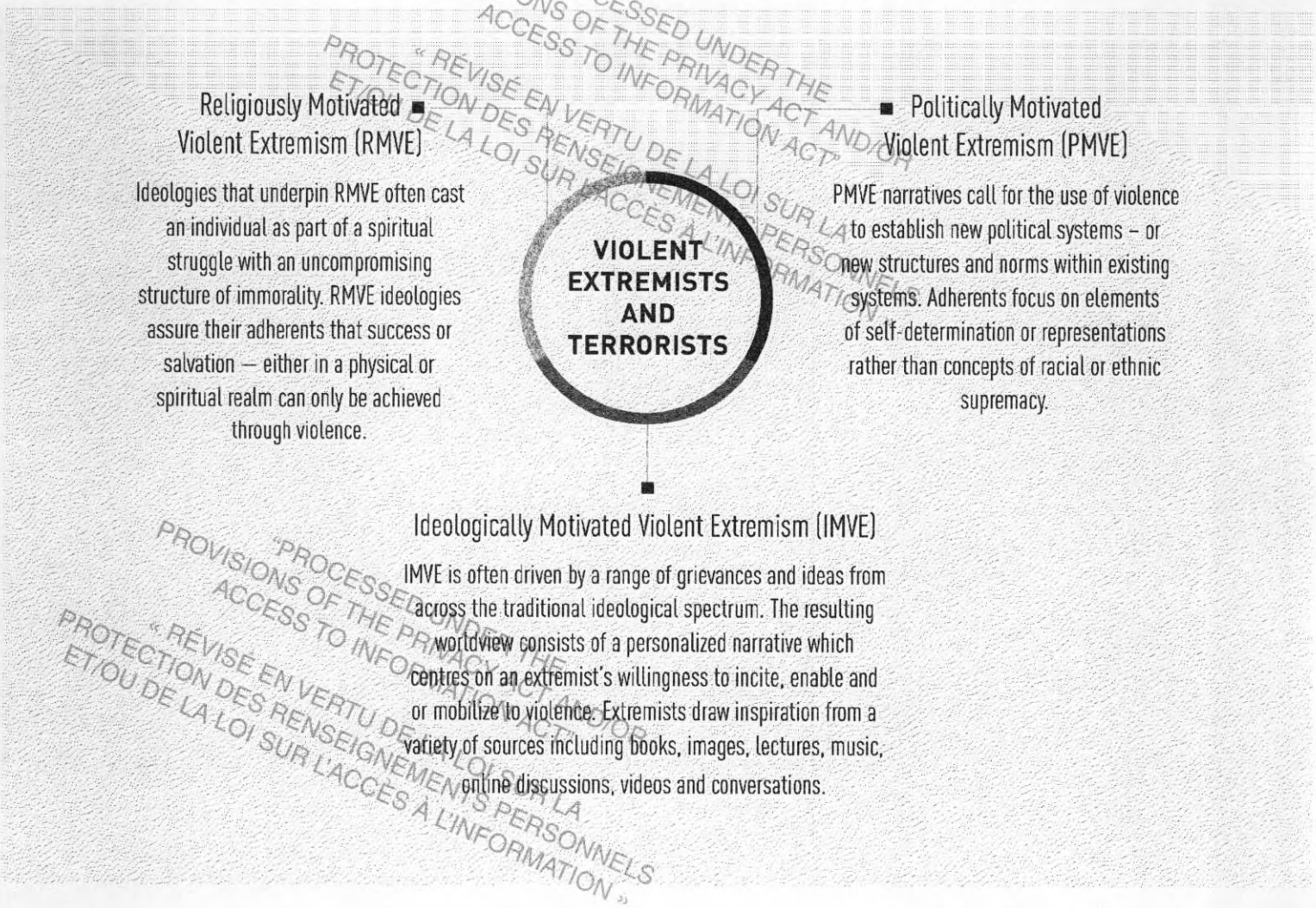
3103(18/09)

THREATS TO THE SECURITY OF CANADA AND CANADIAN INTERESTS

TERMINOLOGY – WORDS MATTER

The terminology used when discussing threats to our national security is important. It matters not only to understand the impact various violent extremist movements have on their adherents, but it also helps ensure that language used does not unintentionally or unfairly stigmatize any given community.

In pursuit of this objective, CSIS sought to develop comprehensive terminology which is linked not only to the *CSIS Act*, but also to Section 83 of the *Criminal Code of Canada*. Moving forward, CSIS will use the following terminology in its discussions of the violent extremist terrorist threat landscape:



3103(18/09)

TERRORISM AND VIOLENT EXTREMISM

The threat landscape surrounding religiously, politically or ideologically motivated violent extremism continues to evolve in Canada and is increasingly changing in a borderless online space. Violent extremist propaganda continues to flourish in this global landscape and cannot be defined by a single coordinated narrative. While no single group has a monopoly on this threat, listed terrorist entities such as Daesh and al-Qaida are well known for leveraging their elaborate online presence to inspire, enable and direct threat actors in support of their activities. Their success has provided a playbook for threat actors in other extremist milieus and the impact has been far reaching — influencing those who support these ideologies to travel, train, fundraise, recruit or plan attacks either within Canada or abroad.

CSIS is mandated to investigate these threats and in certain cases, take measures to reduce them. In doing so, CSIS is charged with providing advice to the Government of Canada regarding the threat landscape, identifying Canadian connections to international groups and identifying potentially violent religiously, politically or ideologically motivated individuals or cells.

GLOBAL

Internationally, security threats impacting Canadians and Canadian interests have largely come from listed terrorist entities and aligned groups such as Daesh. Despite the loss of physical territory in Iraq and Syria, the group continues to dominate the extremist landscape in the Middle East, Asia and Africa. Al-Qaida and al-Qaida-aligned groups also remain present in these regions. In Yemen, both al-Qaida and Daesh have continued to take advantage of the ongoing civil conflict to effectively use vast uncontrolled areas to expand their ranks and enhance their capabilities.

Both Daesh and al-Qaida affiliate Jamaat Nusrat al-Islam Wal Muslimin (JNIM) have conducted frequent and complex attacks in Mali, Niger and Burkina Faso and continue to pose a threat to stability in the region. In November 2019, suspected violent extremists attacked a convoy of buses transporting local employees of a Canadian mining company in eastern Burkina Faso. 38 people were killed and dozens more were injured.

Al-Qaida-aligned al-Shabaab remains the dominant terrorist group in the Horn of Africa. Military activities against al-Shabaab by the United States and other foreign militaries have not hampered its expansion into new areas or diminished the lethalness of its attacks.

The growth of networks sympathetic to al-Shabaab and their form of extremism laid the groundwork for the eventual spread of Daesh affiliates into Somalia and the development of Daesh affiliates in East Africa. In April 2019, Daesh formally recognized the *wilayat* Central Africa, further expanding the official footprint of Daesh to include the Democratic Republic of the Congo and Mozambique. Canadians in this region continue to face an elevated risk of being targeted in terrorist attacks. On July 12, 2019, a Canadian journalist was killed in an al-Shabaab attack on a hotel in Kismayo, Somalia.

The global reach of al-Qaida and Daesh makes both groups an ongoing threat to Canada's national security.

DOMESTIC

Recent acts of serious violence in the West have been typically characterized by low-resource, high-impact events. While previously seen as the hallmark of religiously motivated violent extremist groups such as al-Qaida or Daesh, these strategies are being employed across the violent extremist spectrum. Examples include repeated use of firearms, vehicles and knives in attacks throughout Europe and North America. Despite the decrease in sophistication, the impact and lethality of attacks remain high, as perpetrators often strike soft targets.

3103(18/09)

IDEOLOGICALLY MOTIVATED VIOLENT EXTREMISM (IMVE)

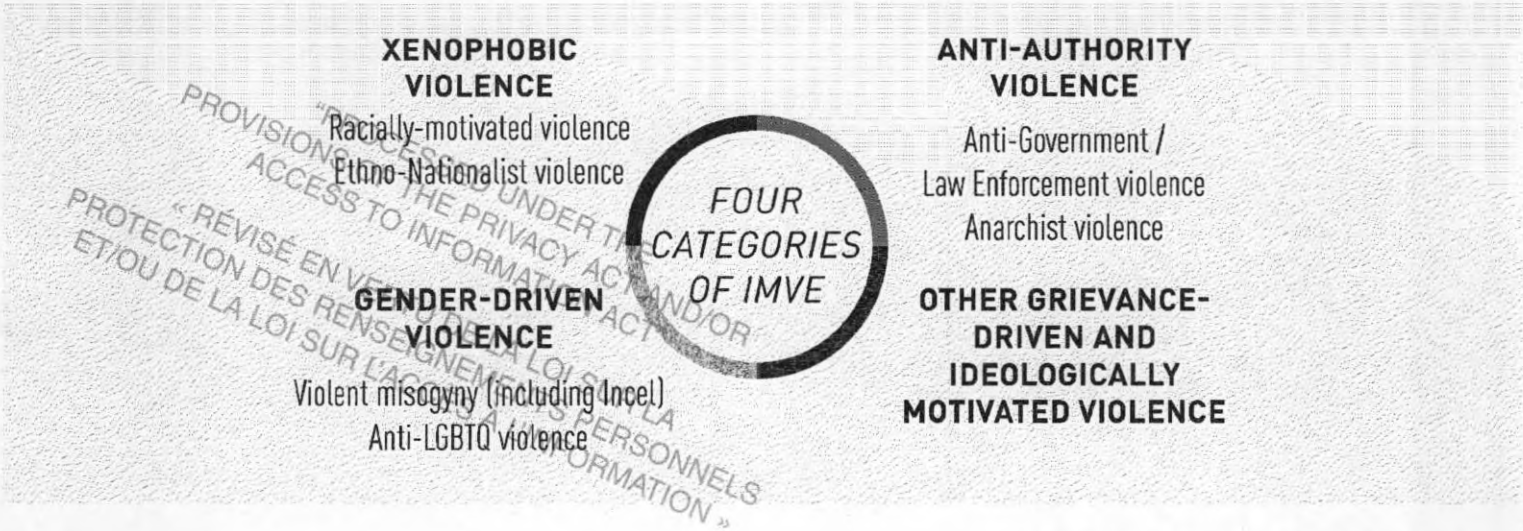
Ideologically motivated violent extremism (IMVE) is often driven by a range of grievances and ideas from across the traditional ideological spectrum. The resulting worldview consists of a personalized narrative which centres on an extremist's willingness to incite, enable and or mobilize to violence. Extremists draw inspiration from a variety of sources including books, images, lectures, music, online discussions, videos and conversations.

Given the diverse combination of motivations and personalized worldviews of recent mass-casualty attackers, the use of such terms as "right-wing" and "left-wing" is not only subjective, but inaccurate in describing the complexity of motivations of IMVE attacks in Canada and abroad.

EXAMPLE OF IMVE

On January 13, 2020, an individual pleaded guilty to two counts of attempted murder and one count of breach of probation. The individual stabbed a woman multiple times and injured her baby on June 3, 2019. He self-identified as an Incel (involuntarily celibate) and took some inspiration from the 2018 Toronto van attack in which 10 people were killed and 16 wounded.

- **Xenophobic Violence**
  Xenophobic violence is defined as the fear or hatred of what is perceived to be foreign, different or strange, which leads to racially motivated violence. This has traditionally been referred to in the Canadian context as white supremacy or neo-Nazism.
- **Anti-authority Violence**
  Anti-authority violence is defined as the opposition to, or rejection of, the authority of the State which leads to anti-Government and violence against law enforcement. The 2014 Moncton shooting is an example of anti-authority violence.
- **Gender-driven Violence**
  Gender-driven violence is defined as the hatred of those of a different gender and or sexual orientation which can lead to violent misogyny. The 2018 Toronto van attack is an example of gender-driven violence.
- **Other Grievance-driven and Ideologically Motivated Violence**
  Some ideologically motivated violent extremists act without a clear affiliation to an organized group or external guidance. They are nevertheless shaped by the echo chambers of online hate that normalize and advocate violence. More than ever, the internet allows individuals to not only share their extreme views, but also their manifestos and details of attacks. All these activities can inspire others to conduct attacks of their own.



3103(18/09)

RADICALIZATION, BOTH OFFLINE AND ONLINE, REMAINS A SIGNIFICANT CONCERN TO CANADA AND ITS ALLIES.

CANADIAN EXTREMIST TRAVELLERS

The Government of Canada has continued to monitor and respond to the threat of Canadian Extremist Travellers (CETs). CETs, in other words, are people who hold Canadian citizenship, permanent residency or a valid visa for Canada and who are suspected of having travelled abroad to engage in terrorism-related activities. CETs, including those abroad and those who return, pose a wide range of security concerns for Canada. While Canada's share of this problem is small, we are not immune to these threats.

There are approximately 250 CETs, both abroad and who have returned. Of the estimated 190 CETs currently abroad, nearly half have travelled to Turkey, Syria and Iraq. The remaining CETs are located in Afghanistan, Pakistan and parts of North and East Africa. These individuals have travelled to support and facilitate extremist activities and, in some cases, directly participate in violence. Some 60 individuals with a nexus to Canada who were engaged in extremist activities abroad have returned to Canada.

The conflict in Syria and Iraq has attracted a large number of extremists to fight overseas since it began in 2011. Several factors—including foreign authorities preventing entry at their borders, enhanced legislation in Canada deterring individuals from leaving and Daesh's loss of territory—have all contributed to the declining number of individuals travelling to join extremist groups in Syria and Iraq. Given the risk of death or capture by other armed groups and possible lack of valid travel documents and funds with which to travel, only a limited number of CETs from this conflict zone have successfully returned to Canada. Despite significant challenges CETs face in the conflict zone, many—both male and female—remain committed to extremist ideologies and may desire to leave the region if circumstances on the ground permit.

CSIS is aware of the serious threat posed by returning fighters who have not only shown the resolve to travel and join a terrorist group, but have often received training or gained operational experience while abroad. CSIS and other Government of Canada departments and agencies are well organized as a community to manage the threat posed by returning fighters.

3103(18/09)

NAVIGATING THE ONLINE SPACE

Increased use of the Internet and social media by threat actors represents a unique challenge for the security and intelligence community, including CSIS.

Threat actors have access to a wealth of information on the internet and online guides offer strategies, provide encouragement and incite and idolize perpetrators of successful violent acts. This information can empower those who would otherwise be incapable of conducting a more complex terrorist attack. Through media and social media outlets, there has been a surge in violent extremist and terrorist media production, as groups continue to spread their extremist messaging while attempting to recruit like-minded individuals to their cause.

Propaganda is disseminated using new methods and alternative platforms, many of which do not require identification in order to share links. This helps threat actors enhance the security of their activities, posing additional challenges for the security and intelligence community. Most notably, the increased use of encryption technologies allows terrorists to conceal the content of their communications and operate with anonymity while online. They can evade detection by police and intelligence officials, which often presents a significant challenge when governments investigate and seek to prosecute threat actors.

Social media platforms, Darknet libraries and encrypted messaging applications continue to represent an important aspect of terrorist messaging and recruitment to solicit attention to the cause and incite violence. Despite Daesh's loss of territory and leadership in recent years, their media production is ongoing—albeit in a diminished capacity—as it continues to spread its message by disseminating material across a variety of online platforms. Terrorist entities use cyberspace to enhance the security of their activities. CSIS assesses that Daesh will continue to inspire and or encourage operations abroad. Attacks undertaken by individuals whose radicalization is facilitated by learned tactics and online and emerging technologies are the direct result of aggressive terrorist media campaigns that aim to inspire more violence. Radicalization, both offline and online, remains a significant concern to Canada and its allies.

3103(18/09)

ESPIONAGE AND FOREIGN-INFLUENCED ACTIVITIES

As a core part of its mandate, CSIS investigates and advises the Government of Canada on threats posed by espionage and foreign-influenced activities. These activities are almost always conducted to further the interests of a foreign state, using both state and non-state entities. Espionage and foreign-influenced activities are directed at Canadian entities both inside and outside of Canada, and directly threaten Canada's national security and strategic interests.

These threats continue to persist and, in some areas, are increasing. Canada's advanced and competitive economy, as well as its close economic and strategic partnership with the United States, makes it an ongoing target of hostile foreign state activities. Canada's status as a founding member of the North Atlantic Treaty Organization (NATO) and its participation in a number of multilateral and bilateral defence and trade agreements has made it an attractive target for espionage and foreign interference.

Canadian interests can be damaged by espionage activities through the loss of sensitive and or proprietary information or leading-edge technologies, and through the unauthorized disclosure of classified and sensitive government information. A number of foreign states continue their attempts to covertly gather political, economic and military information in Canada. Multiple foreign states also target non-government organizations in Canada—including academic institutions, other levels of government, the private sector and civil society—to achieve these goals.

Foreign governments also continue to use their state resources and their relationships with private entities to attempt foreign interference activities in Canada. These activities are carried out in a clandestine or deceptive manner and can target communities or democratic processes across multiple levels throughout the country. Foreign powers have attempted to covertly monitor and intimidate Canadian communities in order to fulfil their own strategic and economic objectives. In many cases, clandestine influence operations are meant to support foreign political agendas—a cause linked to a conflict abroad—or to deceptively influence Government of Canada policies, officials or democratic processes.

ECONOMIC SECURITY

Economic espionage activities in Canada continue to increase in breadth, depth and potential economic impact. Hostile foreign intelligence services or people who are working with the tacit or explicit support of foreign states attempt to gather political, economic, commercial, academic, scientific or military information through clandestine means in Canada.

In order to fulfil their economic and security development priorities, some foreign states engage in espionage activities. Foreign espionage has significant ramifications for Canada, including lost jobs, corporate and tax revenues, as well as diminished competitive and national advantages. Canadian commercial interests abroad are also potential targets of espionage, and Canadian entities in some foreign jurisdictions can be beholden to intrusive and extensive security requirements.

3103(18/09)

CSIS CONTINUES TO INVESTIGATE AND IDENTIFY THE THREATS THAT ESPIONAGE AND FOREIGN INFLUENCED ACTIVITIES POSE TO CANADA'S NATIONAL INTERESTS...

With our economic wealth, open business and scientific environments, and advanced workforce and infrastructure, Canada offers attractive prospects to foreign investors. While the vast majority of the foreign investment in Canada is carried out in an open and transparent manner, a number of state-owned enterprises (SOEs) and private firms with close ties to their government and or intelligence services can pursue corporate acquisition bids in Canada or other economic activities. Corporate acquisitions by these entities pose potential risks related to vulnerabilities in critical infrastructure, control over strategic sectors, espionage and foreign influenced activities, and illegal transfer of technology and expertise. CSIS expects that national security concerns related to foreign investments or other economic activities in Canada will continue.

As difficult as it is to measure, this damage to our collective prosperity is very real. This reality has led to more and more governments openly discussing the changing security landscape with their businesses, their universities and the general public. The national security community and the business community have a shared interest in raising public awareness regarding the scope and nature of state-sponsored espionage against Canada and its potential effect on our economic growth and ability to innovate.

CSIS continues to investigate and identify the threats that espionage and foreign influenced activities pose to Canada's national interests, and is working closely with domestic and international partners to address these threats.

PROTECTING DEMOCRATIC INSTITUTIONS

Democratic institutions and processes around the world—including elections—are vulnerable and have become targets for international actors. Foreign threat actors—most notably hostile states and state-sponsored actors—are targeting Canada's democratic institutions and processes. While Canada's democratic institutions are strong, threat actors maintain a range of targets in order to try to manipulate the Canadian public and interfere with Canada's democracy. Certain states seek to manipulate and misuse Canada's electoral system to further their own national interests, while others may seek to discredit key facets of Canada's democratic institutions to reduce public confidence in the democratic system.

Among the safeguards put in place to protect Canada's democracy and the 2019 Federal Election was the creation of the Security and Intelligence Threats to Election (SITE) Task Force. As an active partner in SITE, CSIS worked closely with the Communications Security Establishment (CSE), the Royal Canadian Mounted Police (RCMP), Global Affairs Canada (GAC) and the Privy Council Office (PCO) to share information on election security. Through SITE, CSIS investigated possible foreign interference threats in the lead-up to and during the 2019 Federal Election. SITE proved to be a remarkable example of effective intelligence collaboration through increased intelligence and strengthening communications.

3103(18/09)

CYBER THREAT ACTORS CONDUCT MALICIOUS ACTIVITIES IN ORDER TO ADVANCE THEIR GEOPOLITICAL AND IDEOLOGICAL INTERESTS.

CYBER THREATS

Cyber-espionage, cyber-sabotage, cyber-foreign-influence, and cyber-terrorism pose significant threats to Canada's national security, its interests, as well as its economic stability.

Cyber threat actors conduct malicious activities in order to advance their geopolitical and ideological interests. They seek to compromise both government and private sector computer systems by using new technologies such as Artificial Intelligence and Cloud technologies or by exploiting security vulnerabilities or users of computer systems. Such activities are collectively referred to as "Computer Network Operations", or CNOs. State-sponsored entities and terrorists alike are using CNOs directed against Canadians and Canadian interests, both domestically and abroad. Canada remains both a target for malicious cyber activities, and a platform from which hostile actors conduct CNOs against entities in other countries.

State-sponsored cyber threat-actors use CNOs for a wide variety of purposes. These include theft of intellectual property or trade secrets, disruption of critical infrastructure and vital services, interference with elections, or conducting disinformation campaigns. In addition, non-state actors such as terrorist groups also conduct CNOs in order to further their ideological objectives such as recruitment and distribution of propaganda.

Canada's National Cyber Security Strategy views cyber security as an essential element of Canadian innovation and prosperity. CSIS, along with partners, particularly the Communications Security Establishment's Canadian Centre for Cyber Security, plays an active role in shaping and sustaining our nation's cyber resilience through collaborative action in responding to evolving threats of malicious cyber activity. While the CSE and CSIS have distinct and separate mandates, the two agencies share a common goal of keeping Canada, Canadians and Canadian interests safe and secure. In today's global threat environment, national security must be a collaborative effort. In responding to cyber threats, CSIS carries out investigations into cyber threats to national security as outlined in the *CSIS Act*. By investigating malicious CNOs, CSIS can uncover clues that help profile cyber threat actors, understand their methods and techniques, identify their targets of interest, and advise the Government of Canada accordingly.

3103(18/09)

SECURITY SCREENING

Through its Government Security Screening and Immigration and Citizenship Screening programs, CSIS serves as the first line of defence against terrorism, extremism, espionage and the proliferation of weapons of mass destruction.

The Government Security Screening (GSS) program conducts investigations and provides security assessments to address threats to national security. The security assessments are a part of an overall evaluation and assist Government departments and agencies when deciding to grant, deny or revoke security clearances. Decisions related to the granting, denying or revoking of a security clearance lies with the department or agency, not with CSIS.

GSS also conducts screening to protect sensitive sites from national security threats, including airports, marine and nuclear facilities. It assists the RCMP by vetting Canadians and foreign nationals who seek to participate in major events in Canada, such as G7 meetings and royal visits. It provides security assessments to provincial, foreign governments and international organizations when Canadians seek employment requiring access to sensitive information or sites in another country. All individuals subject to government security screening must provide consent prior to being screened.

The Immigration and Citizenship Screening (ICS) program conducts investigations and provides security advice to the Canada Border Services Agency (CBSA) and Immigration, Refugees, and Citizenship Canada (IRCC) regarding persons who might represent a threat to national security. Through this program, CSIS provides security advice on permanent residence and citizenship applicants; persons applying for temporary resident visas; and persons applying for refugee status in Canada. Decisions related to admissibility into Canada, the granting of visas or the acceptance of applications for refugee status, permanent residence and citizenship rest with IRCC.

IMMIGRATION AND CITIZENSHIP SCREENING PROGRAMS

REQUESTS RECEIVED*	2018–2019
Permanent Resident Inside and Outside Canada	41,900
Refugees (Front-End Screening**)	41,100
Citizenship	217,400
Temporary Resident	55,800
TOTAL:	**356,200**

GOVERNMENT SCREENING PROGRAMS

REQUESTS RECEIVED*	2018–2019
Federal Government Departments	74,900
Free and Secure Trade (FAST)	17,900
Transport Canada (Maine and Airport)	46,100
Parliamentary Precinct	2,900
Nuclear Facilities	10,000
Provinces	280
Others	3,300
Foreign Screening	490
Special Events Accreditation	12,500
TOTAL:	**168,370**

*Figures have been rounded
**Individuals claiming refugee status in Canada or at ports of entry

3103(18/09)

EXCELLENCE

OUR
PEOPLE

CSIS ACROSS CANADA

BRITISH COLUMBIA REGION
Burnaby, BC

PRAIRIE REGION
Edmonton, AB

■ District Offices

3103(18/09)

THE CSIS PEOPLE STRATEGY

In 2019, CSIS introduced a comprehensive and multi-year strategy to guide initiatives and modernize all areas of people management within the organization. The CSIS People Strategy sets out broad themes and initiatives for modernization, including improving human resource policies and processes, enhancing learning and talent management, and fostering a safe, healthy and respectful workplace. Collectively, the CSIS People Strategy sets a vision to attract, develop and retain the talent needed now and in the future in order to meet the organization's mission to keep Canada and Canadians safe from threats at home and abroad.

DEDICATED TO HEALTH AND WELLNESS

CSIS employees are the organization's most valuable resource and ensuring that their work environment is healthy, safe and respectful is essential. That is why CSIS is taking concrete steps to strengthen the cultural values of our workplace and ensure that every employee shares in the responsibility. This includes launching a values-based Code of Conduct, new guidelines on disciplinary measures and more mandatory training for supervisors. CSIS also launched the Respect Campaign to re-enforce the importance and value of civility and respect in the workplace and held numerous town halls across the country to discuss concerns with employees.

CSIS takes a holistic approach to health and wellness by considering the physical and psychological well-being of employees. The Health and Wellness Centre of Expertise located at our National Headquarters in Ottawa has a team that includes Psychologists and Mental Health Professionals, Occupational Health Nurses and Informal Conflict Management Services. CSIS remains committed to adopting the National Standard on Psychological Health and Safety in the Workplace and has integrated the concept across various organizational initiatives, including a Respect and Civility campaign.

An increase in mental health dialogue, training and awareness at CSIS has led to an increase in demand for the services and support of the Centre. There are several programs in place to address the needs of the organization and its employees, including a Disability Management Program that assists employees who are on medical leave to return to work as early and safely as possible. A comprehensive Employee Assistance Program offers a number of confidential services to employees and their immediate family members.

CSIS has a responsibility to protect employees against psychological injury which is why the Health and Wellness Centre of Expertise has undertaken several preventative initiatives such as developing mental health workshops, instituting mandatory Road to Mental Readiness (R2MR) training and delivering a course on Mitigating the Negative Effects of Exposure to Potentially Disturbing Material.

In recognition of the higher prevalence of Operational Stress Injuries in public safety personnel, CSIS has actively participated in initiatives related to the development of *Supporting Canada's Public Safety Personnel: An Action Plan on Post-Traumatic Stress Injuries* which was released in April 2019. The Action Plan is a key component of a broader Federal Framework, the establishment of which is required by the *Federal Framework on Post-Traumatic Stress Disorder Act*.

GBA+

CSIS is dedicated to ensuring that its activities are aligned with the Government of Canada's commitments to Gender Based Analysis Plus (GBA+). To enable this, CSIS will work to integrate GBA+ into its policies, programs, initiatives and operational activities. This will support evidence-based decisions, thus improving results for stakeholders, our employees and all Canadians. Diversity is a core part of our ability to protect Canada's national security.

3103(18/09)

RECRUITING FOR THE MISSION

CSIS recognises how important it is to bring new and diverse talent to its workforce. In 2019, CSIS organised over 100 recruiting events from coast to coast and sought talent for over 100 different positions within the organization. CSIS is updating its compensation and benefits package to ensure it remains competitive in the current job market.

CSIS continues to foster recruitment collaboration with our federal partners through the Federal Safety Security and Intelligence (FSSI) partnership. Beyond sharing best practices, FSSI partners benefit from the financial efficiencies of combining recruitment efforts between eight government departments. We are proud of the partnership developed with the Royal Canadian Mounted Police (RCMP), Public Safety Canada, Canada Border Services Agency (CBSA), Correctional Service Canada (CSC), Communications Security Establishment (CSE), the Department of National Defence (DND) and the Financial Transactions and Reports Analysis Centre (FINTRAC) to recruit top talent to work within public safety and security.

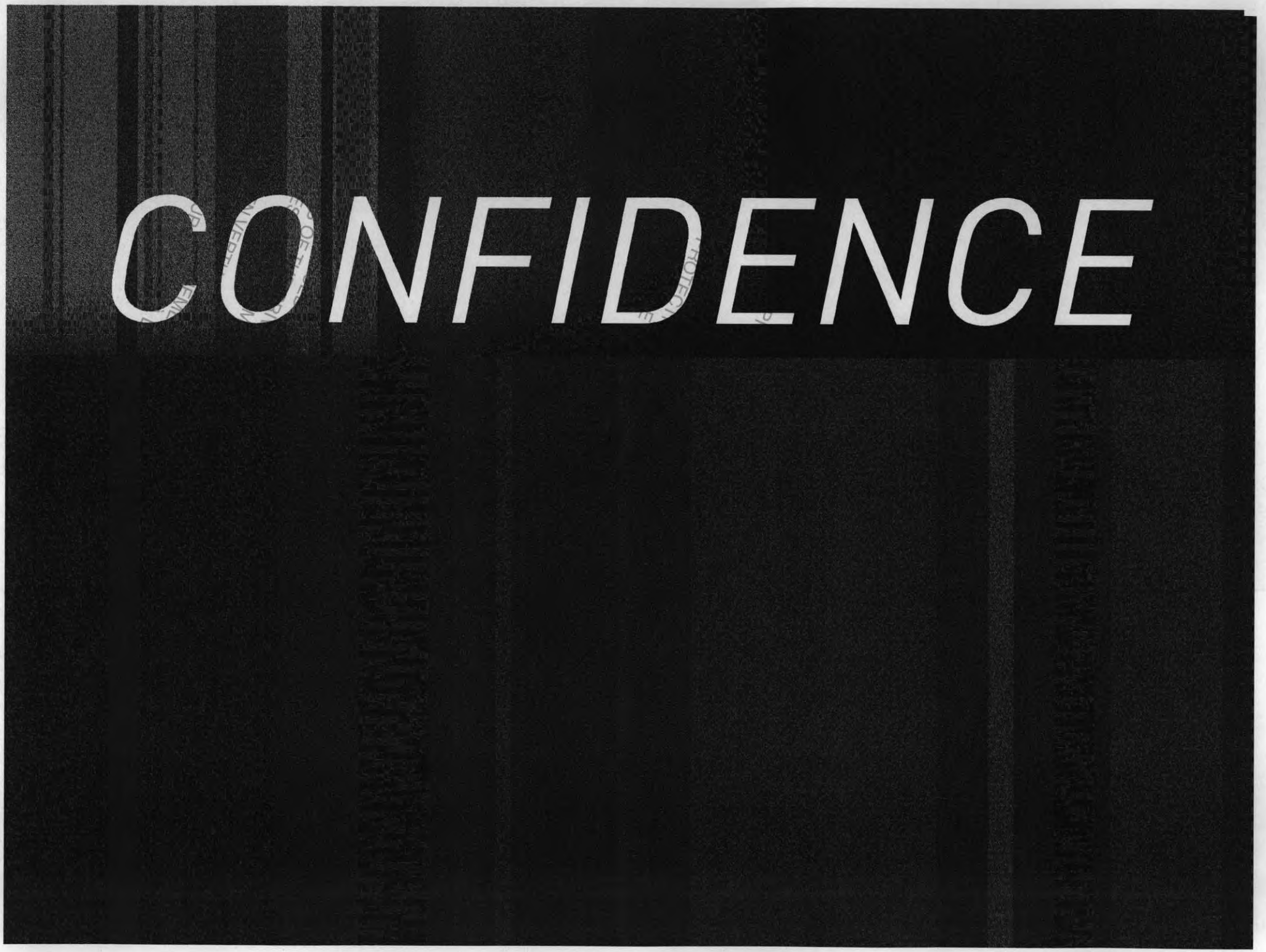
CSIS WOMEN'S NETWORK

On March 7, 2019 — the day before International Women's Day — the CSIS Women's Network officially launched with the aim to promote diversity of thought, address gender and unconscious bias, and provide networking and mentorship opportunities for women at CSIS.

The CSIS Women's Network was originally founded by a group of women professionals with the goal of supporting the advancement and well-being of women within the organization. Since then, the network has launched a speaker series where leaders and industry experts share career advice and inspire others to break through barriers and reach higher in their careers. The network's mentorship program has become a very popular resource for those seeking assistance and for those seeking to assist on how to navigate through the triumphs and challenges of any career.

The CSIS Women's Network adds to a growing list of other long-established professional networks and social committees including the CSIS Advisory Committee on Diversity and Inclusion, the CSIS Young Professionals Network as well as the CSIS Green Committee.

3103(18/09)


CONFIDENCE

ACCOUNTABILITY AND TRANSPARENCY

CSIS depends on the trust of Canadians to do its work. That is why robust oversight and accountability mechanisms are so fundamental. They provide assurance to Canadians that we continue to operate lawfully in our efforts to protect Canada and Canadians.

ACCOUNTABILITIES OF THE CSIS DIRECTOR

CSIS DIRECTOR

- **MINISTER OF PUBLIC SAFETY**
  Provides advice on national security policy, adherence to Ministerial Direction and the management of departmental operations, including an annual report.
- **NATIONAL SECURITY AND INTELLIGENCE ADVISOR**
  Ensures the NSIA remains informed of security and intelligence matters in the provision of advice to the Prime Minister.
- **CLERK OF THE PRIVY COUNCIL**
  Ensures the Clerk remains informed of overall performance and achievement of corporate priorities.
- **TREASURY BOARD**
  Exercises authorities under the *Financial Administration Act* and any relevant legislation or policies (e.g. controls, internal audit).
- **HUMAN RESOURCES**
  Exclusive authority over human resources management and appointment of employees.
- **LABOUR RELATIONS**
  Maintains productive labour-management relations as per the *Federal Public Sector Labour Relations Act* and *Public Servants Disclosure Protection Act*.

3103(18/09)

LEGAL

Ensures that CSIS and its employees act lawfully in the conduct of its affairs and operations.

REVIEW

Ensures that CSIS responds to inquiries from the National Security and Intelligence Review Agency (NSIRA) and National Security and Intelligence Committee of Parliamentarians (NSICOP) in the fulfillment of its statutory review function.

MANDATORY REPORTING

Ensures compliance with government reporting requirements, such as the Main Estimates, the Management Accountability Framework, Access to Information, and the Treasury Board Policy Suite.

PARLIAMENT

CORE MANDATE

- Public Accounts
- Government Operations and Estimates
- Standing Senate Committee on National Security and Defence
- Standing Committee on Public Safety and National Security

OFFICERS AND AGENTS OF PARLIAMENT

Ensures that CSIS responds to Agents and Officers of Parliament, including:

- Auditor General of Canada
- Information Commissioner
- Privacy Commissioner
- Parliamentary Budget Officer
- Commissioner of Official Languages

Ensures that CSIS responds to various government coordination bodies, including:

- Chief Statistician
- Chief Information Officer
- Ombudspersons
- Canadian Human Rights Commission

3103(18/09)

MINISTERIAL DIRECTION FOR ACCOUNTABILITY

In accordance with the powers granted by subsection 6 (2) of the *CSIS Act*, the Minister of Public Safety and Emergency Preparedness issued a new Ministerial Direction for Accountability to CSIS in September 2019.

This new direction restates the fundamental role that accountability plays in our system of government and the importance of maintaining the confidence of Canadians. It articulates two pillars of accountability for the organization: accountability to the Minister of Public Safety, who is responsible for CSIS; and external accountability through review bodies and to Canadians through transparency.

The issuance of this new Ministerial Direction for accountability modernized parts of the 2018 MD for Operations and Accountability. Efforts are underway to modernize the remaining sections. CSIS remains committed to supporting the Minister on this matter and show Canadians that we continue to be worthy of the trust they have vested in us to protect their safety and Canada's national security.

THE *NATIONAL SECURITY ACT, 2017*

The *National Security Act, 2017* introduced the most significant changes to the *CSIS Act* since our organization was created in 1984. These changes add greater transparency and accountability to our work, and modernize our authorities in specific areas.

There are three main changes to the *CSIS Act* introduced by the *National Security Act*:

1. THREAT REDUCTION MEASURES

CSIS' threat reduction mandate provides the Government of Canada with another tool to respond to threats to the security of Canada, capitalizing on the Service's unique intelligence collection function. Given the nature of our mandate, CSIS is often the first agency to detect threats to the security of Canada.

In some circumstances, no other Canadian partner may be able to take action against a threat, because of differing mandates and authorities or a lack of threat awareness.

Any threat reduction measure carried out by CSIS must be reasonable and proportional to the threat to be reduced. The new National Security and Intelligence Review Agency (NSIRA) is informed of every measure taken to ensure that CSIS upholds these requirements.

Amendments to the *CSIS Act* introduced by the *National Security Act* clarified wording in our threat reduction mandate to emphasize that measures taken by CSIS in this area are fully compliant with the Canadian Charter of Rights and Freedoms. They also introduced a fixed list of measures that CSIS can take, with a warrant, to reduce a threat. Together, these changes help Canadians better understand what CSIS can and cannot do to diminish threats to Canada's security.

2. JUSTIFICATION FRAMEWORK

The *National Security Act, 2017* amended the *CSIS Act* to recognize that it is in the public interest to ensure that CSIS employees can effectively carry out our intelligence collection duties and functions, including by engaging in covert activities, in accordance with the rule of law. A framework was also created and added to the *CSIS Act* that provides a limited justification for designated employees acting in good faith and persons acting under their direction to commit acts or omissions that would otherwise constitute offences.

This is particularly true for counter-terrorism operations where CSIS relies on the assistance of persons who have access to individuals, entities and activities that are relevant to its collection objectives. These persons (human sources, for example) are in a position to provide intelligence supporting mandated investigations; often, this information could not be obtained by any other means.

This justification framework offers protection from criminal liability for CSIS employees and directed persons, including human sources. It provides a clear legal authority for the commission and direction of otherwise unlawful activity, allowing the continuance of activities critical to operational success, and assuring the integrity of Service information collected pursuant to these activities. This includes providing logistical support for a source by paying for a meal during a meeting,

buying a cellphone or laptop to assist them in undertaking their work.

The *Act* also establishes robust measures to ensure this authority is exercised in a manner that is reasonable, proportional, transparent and accountable, including robust review by the Intelligence Commissioner (IC) and the National Security and Intelligence Review Agency (NSIRA).

WHY DOES CSIS NEED TO ENGAGE IN OTHERWISE ILLEGAL ACTIVITY?

CSIS' intelligence collection mandate is set out in sections 12 to 16 of the *CSIS Act*. In carrying out these duties and functions, CSIS relies on the assistance of persons, including human sources, who have access to people, organizations and activities that are relevant to our collection objectives. These individuals are in a position to provide intelligence – that often could not be obtained by other means – that support investigations. In sectors where the targets of an investigation are engaged in unlawful activities, sources may be required to participate to some degree, in order to gain trust, maintain credibility, and develop access. Designated CSIS employees may need to direct, support and pay these persons, to guide and facilitate their role in information and intelligence collection.

There are many checks and balances governing the CSIS' use of the justification framework. CSIS employees can only commit or direct otherwise illegal activity if it falls under a class approved by the Minister of Public Safety. The determinations of the Minister are subject to review and approval by the Intelligence Commissioner under the *Intelligence Commissioner Act*. Only employees designated by the Minister for this purpose can commit or direct otherwise illegal activity. In order to direct this activity, in addition to being designated, employees must have the authorization of a senior designated employee. Before committing or directing otherwise illegal activity, the employee must assess that this activity is reasonable and proportional, considering the nature of the threat, the nature of the activity, and the reasonable availability of other means to achieve the operational objective.

CSIS employees must successfully complete robust training prior to being designated by the Minister. This training is designed to ensure employees have a clear idea of the legislated requirements that govern their ability to commit or direct otherwise illegal activity, and a sound understanding of the policies and procedures that guide their application of this authority.

The establishment of the justification framework enables CSIS to carry out operational activities that are necessary to the achievement of our mandate. The clear authority it provides for the conduct of otherwise illegal activity enables CSIS to effectively investigate threats to the security of Canada, particularly those in the terrorist domain.

3. DATASET FRAMEWORK

The *National Security Act, 2017* also amended the *CSIS Act* to provide a clear legal mandate for CSIS' collection and retention of datasets. It lays out parameters by which CSIS can collect, retain, and query datasets containing personal information that is not directly and immediately related to a threat to the security of Canada. This framework facilitates CSIS analysis of data in support of our operations, where we increasingly rely on this technique to corroborate human and technical sources, further identify individuals of interest, and generate investigational leads.

The framework applies to every dataset that contains personal information that does not directly and immediately relate to activities that represent a threat to the security of Canada. It sets out three types of datasets: Canadian, foreign and publicly available. A Canadian dataset is defined in the *CSIS Act* as a dataset that predominantly relates to individuals within Canada or Canadians, which includes Canadian citizens, permanent residents or corporations incorporated or continued under the laws of Canada or a province.

Canadian and foreign datasets must remain segregated from operational holdings and can only be queried by designated employees in accordance with the provisions of the *CSIS Act*. *The Act* also sets out record-keeping and audit requirements and provides for robust review by the National Security and Intelligence Review Agency (NSIRA).

3103(18/09)

NATIONAL SECURITY AND INTELLIGENCE REVIEW AGENCY (NSIRA)

The Security Intelligence Review Committee (SIRC) expanded into the National Security and Intelligence Review Agency (NSIRA), and the scope of its responsibilities broadened. Now, in addition to reviewing the activities of CSIS, NSIRA has specific responsibility for reviewing the activities of the Communications Security Establishment (CSE), and can review any activity carried out by any federal department or agency, that relates to national security or intelligence. NSIRA also has the mandate to investigate a range of complaints related to national security, including those made pursuant to the *CSIS Act*, the *RCMP Act*, the *Citizenship Act* and the *Canadian Human Rights Act*.

Over the years, SIRC and CSIS developed an open exchange of information to support SIRC investigations; this same transparent relationship will continue with NSIRA. CSIS works diligently to ensure NSIRA has timely access to documentation required to satisfy their review requirements.

THE *AVOIDING COMPLICITY IN MISTREATMENT BY FOREIGN ENTITIES ACT*

CSIS takes the human rights reputation of the foreign agencies it engages with very seriously and opposes in the strongest possible terms the mistreatment of any individual by a foreign agency. CSIS has robust, long-standing policies and decision-making procedures in place to ensure that information sharing with foreign partners does not contribute to the mistreatment of any individual by a foreign entity. CSIS has been following Ministerial directions on such requirements for well over a decade.

The *National Security Act* also established the *Avoiding Complicity in Mistreatment by Foreign Entities Act*. This new law requires that direction related to the disclosure, solicitation and use of information that may lead to or be obtained from the mistreatment of an individual by a foreign entity be issued to the Department of National Defence, Global Affairs Canada, the Royal Canadian Mounted Police, Communications Security Establishment, Canada Border Services Agency and CSIS. In addition, the *Act* outlines CSIS' responsibility to provide a report to the Minister of Public Safety and Emergency Preparedness on the implementation of those directions.

Further to the passage of the *Act*, an Order-in-Council (OiC) laying out this direction was issued in September 2019. The OiC reinforces CSIS' longstanding responsibilities regarding information sharing with foreign entities. It dictates that if the sharing or requesting information would result in a substantial risk of mistreatment of an individual, and the risk cannot be mitigated, CSIS cannot share or request the information. If it is believed that information received by CSIS was obtained through mistreatment, CSIS must ensure that its use does not create a substantial risk of further mistreatment, used as evidence, or deprive anyone of their rights or freedoms, unless the use is necessary to prevent loss of life or significant personal injury.

TRANSPARENCY

The confidence of Canadians in the national security efforts of CSIS is fundamental to our legitimacy, operational effectiveness, and institutional credibility. While certain information on our activities and interests must remain protected, CSIS is steadfast in its commitment to making information about some of the activities more transparent to Canadians, ensuring there is no risk or compromise to our national security. Through public forums, public communications, social media platforms, CSIS endeavours to communicate transparently about our decision-making processes and national security activities. In 2019, CSIS also created an Academic and Stakeholder Engagement team dedicated entirely to finding opportunities to engage with Canadians in order to ensure their trust and confidence.

Engaging Canadians on the legal framework under which we conduct national security activities, and our respect for the privacy rights of Canadians, is a priority for the entire organization.

3103(18/09)

ACADEMIC OUTREACH AND STAKEHOLDER ENGAGEMENT

Academic Outreach is responsible for assisting CSIS and the broader Canadian intelligence community better understand current issues, develop a long-term view of various trends, challenge assumptions and cultural bias, and sharpen research and analytical capabilities. With its network of expert contacts across Canada and around the world, CSIS Academic Outreach's ability to quickly identify and engage leading experts on any number of subjects makes it a valuable resource for CSIS and its Government of Canada partners who are often required to respond urgently to 'surprises' in the geopolitical environment. The programme has recently evolved and is now more actively engaged in providing advice to Canadian academic institutions on how to protect their students, their research, and academic integrity from adversaries seeking to undermine the openness and collaborative nature of higher education in Canada.

Building on the success of Academic Outreach, in 2019, CSIS launched a complementary Stakeholder Engagement programme. The current threat landscape is compelling CSIS to expand its network of stakeholders to include those across a number of non-traditional sectors. These stakeholders can include Canadian industry, civil society, provincial and municipal officials, as well as other organizations. It is more critical than ever to engage with these stakeholders in a more open and transparent manner to sensitise them to threats and to enhance cooperation to help mitigate the risks of loss of sensitive technology and intellectual property, and to ensure that these stakeholders recognize CSIS as a partner in protecting the strength of Canada's social fabric and economic prosperity.

One of CSIS' important stakeholder relationships is the one it holds with the National Security Transparency Advisory Group (NS-TAG). The advisory group was established in 2019 and advises the Government of Canada on the implementation of the commitment to increase transparency across Canada's national security and intelligence departments and agencies. NS-TAG advises on how to infuse transparency into Canada's national security policies, programs, best practices, and activities in a way that will increase democratic accountability. It also seeks to increase public awareness, engagement, and access to national security and related information. Finally, it aims to promote transparency — which is consistent with CSIS' own long-established commitment with Canadians.

CSIS also engages in important dialogue with the Cross-Cultural Roundtable on Security (CCRS) and intends on continuing to pursue this important relationship and seek their perspectives on emerging developments in national security matters and their impact on Canada's diverse and pluralistic society.

3103(18/09)

FOREIGN AND DOMESTIC

COOPERATION

CSIS HAS MORE THAN 300 FOREIGN RELATIONSHIPS IN SOME 150 COUNTRIES AND TERRITORIES...

Information-sharing arrangements give CSIS access to timely information linked to potential threats to the security of Canada. Through these relationships, CSIS advances its own investigations into threats to the security of Canada and gains a greater understanding of the scope and nature of threats. The terrorist threat facing Canada and our partners is not restricted by municipal, provincial or national borders. With international travel becoming an increasing central element of global violent extremism, CSIS cooperation with our domestic and international partners is crucial to countering this threat.

CSIS has more than 300 foreign relationships in some 150 countries and territories, each authorized by the Minister of Public Safety and supported by the Minister of Foreign Affairs, in accordance with s.17(1)(b) of the *CSIS Act*. The process to establish arrangements with foreign agencies is stringent and takes into consideration a wide range of issues, including Canadian security requirements, respect for human rights and the reliability of the agency.

CSIS assesses all of its foreign arrangements, including human rights reputations of the country and agency with which we have an established an arrangement. CSIS applies human rights caveats on information shared with foreign partners which make clear expectations with regard to human rights. CSIS also seeks broader human rights assurances from foreign agencies when required and applies restrictions on engagement where there are serious concerns regarding potential mistreatment.

CSIS assesses potential risks of sharing with foreign entities and, where possible, measures are taken to mitigate risks of mistreatment. When a substantial risk of mistreatment cannot be mitigated, information is not shared. This decision-making process includes a senior-level committee known as the Information Sharing Evaluation Committee (ISEC) that is convened as required to assess whether there is a substantial risk of mistreatment as a result of sharing information with a foreign partner; and if so, whether that risk could be mitigated.

CSIS has strong and well-established relationships with many domestic partners throughout the Government of Canada as well as provincial and local law enforcement. Today's global threat environment requires that each partner use their mandate and legal authorities to protect Canada and Canadians from threats at home.

3103(18/09)

2020 AND BEYOND:

MODERNIZING CSIS' AUTHORITIES

The *National Security Act, 2017* introduced the most significant changes to CSIS since 1984, however work remains to ensure CSIS' authorities keep pace. Changes in our threat, operational, technological and legal environment continue to create challenges while expectations of CSIS continue to grow.

For example, technology has evolved dramatically, creating both new vulnerabilities that can be exploited by Canada's adversaries, and a data rich environment with enormous potential to leverage modern tools to support investigations, while ensuring Canadians' privacy is protected. Canada's national security landscape has also changed significantly. The distinction between threats to national security and threats to Canada's national interest – our economy, research and development – is increasingly blurred in the face of espionage by state actors who also seek to covertly undermine Canada's institutions. To operate effectively in this environment, CSIS must increasingly engage with a wide variety of stakeholders, including private sector and academia.

CSIS' critical engagement with the Federal Court further shapes our legal and operational realities. Key Federal Court decisions can have significant impact on our authorities and their limitations, creating tensions between technology in the context of modern investigations, and a statute drafted over thirty-five years ago.

Moving forward, it is important to consider Canadians' expectations of CSIS as a modern, accountable intelligence service. We must ensure CSIS has the authorities to provide timely, relevant advice in line with Government and Canadians' expectations of their intelligence service including expectations of accountability and transparency.

In this context, CSIS is working to ensure our authorities are, and continue to be, fit for purpose in our dynamic landscape. However, this work is not CSIS' alone. In ensuring we have the flexibility and foresight necessary to adapt to evolving threats, evolving technologies and an evolving society, we are working closely with our Government of Canada partners both within the Public Safety Portfolio and with the Department of Justice, as well as learning from allied experiences as these challenges are not Canada's alone. Cross-cutting work by external review agencies is also an important part of this work as it informs where CSIS, and its close partners, may be working with outdated authorities in an increasingly inter-connected world.

3103(18/09)