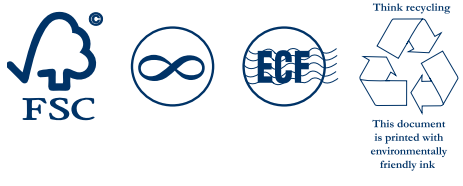
Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

PUBLIC REPORT 2010-2011

Canada

Cat No. PS71-2011

ISSN: 1188-4415



MESSAGE FROM THE DIRECTOR

The fiscal year 2010-2011 was both a challenging and a successful one for CSIS. Several counter-terrorist operations by the Service and its partners resulted in the prevention of attacks in Canada. Internationally, we continued to exert an effective presence, including in Afghanistan where the intelligence we collected saved lives.

Gratifying as it is to survey a year of achievements, doing so provokes some wistfulness. All of us would prefer to live in a world where a peaceable country such as ours had no need to maintain a robust security and intelligence apparatus – a world where threats to our security were decreasing rather than increasing, where adversaries were disappearing faster than they are appearing, where the methods by which Canadian interests can be harmed were diminishing rather than expanding.

Unfortunately, that is not the world Canadians find themselves in.

While the "9-11 era" might be over, symbolized by the demise of Osama bin Laden, violence committed in the name of extremist political or religious ideologies remains a global scourge. Oppressive governments continue to produce, or seek to produce, weapons of mass destruction, thereby jeopardizing international security. Economic and strategic competition among nations has produced levels of hostile foreign espionage that rival those witnessed during the Cold War.

The threats to Canada's national security are different from those faced by previous generations.

Back when the world's most powerful countries were in thrall to totalitarian, expansionist governments – namely, fascist or communist – democracies such as ours had a feeling of existential vulnerability. Today the spectre of armies invading our shores to overthrow our system of government has diminished. But it's equally true that today, in the age of globalization, a handful of men or women with the right weapons can cause the sort of destruction that in years past only a large number of trained soldiers could have done.

Today's world is interconnected in ways we are only beginning to understand. The globalization of ideas and of technology is a positive development when those ideas and technologies are vehicles for human advancement. It is a less positive development when they are put to the service of human conflict. The complexity of the threat environment – evolving as rapidly as technology itself – presents an unprecedented challenge for the national security community.

It used to be that we knew, by and large, what the threat was and who our adversaries were. Today it can be hard sometimes to identify either.

On the espionage front, cyber attacks against sensitive information systems will happen instantaneously, in Internet time, with victims not knowing how they were hit or by whom, in some cases not even knowing they've been hit at all. On the terrorism front, the Internet enables extremists to create virtual communities. Terrorists no longer need to maintain the operational security of safehouses, because they can share and obtain tradecraft from the isolation of their one-room apartments.

Anders Breivik of Norway did not need the support of a large network to carry out one of the most horrific terrorist attacks of 2011. He represented the most difficult threat to detect – the "lone actor." Extremists of all stripes have taken note. Terrorist leaders used to call upon supporters to enrol in training camps abroad but now those supporters are being asked simply to mount attacks where they are. The terrorist message has been tailored to the medium.

The above examples illustrate how the Service needs to adapt to ever-changing threats. On the analytical side, we have recruited and trained top-tier analysts and subject-matter experts. We are doing, for example, cutting edge research on the dynamics of radicalization, because detecting violent extremists isn't enough. We need also to understand them – to understand how seemingly ordinary young men or women can grow up in Canada yet come to reject the Western democratic values that underpin Canadian identity, instead replacing them with the nihilist ideology of al-Qaeda.

The past year was a significant one in Canadian security history because the story of the Toronto 18 reached its legal conclusion in an Ontario courtroom (see *Making History*, page 21). The work leading to the successful prosecution of members of that terror cell was a model of cooperation between the Service, law enforcement – principally the RCMP – and the Public Prosecution Service of Canada. It was important for Canadians to see that terrorism is a global phenomenon and our country is in no way immune, and also that threats can originate from both inside and outside our borders.

When we talk of confronting new realities, we include economic realities. Taxpayers expect value and sound fiscal management from their public institutions. The Service will continue to identify the most effective options to reflect the environment in which we operate. The culture of innovation, efficiency and responsible resource management at CSIS is inherent with who we are and expresses itself both in good and in uncertain economic times.

At CSIS we are keenly aware of the special role Canadians have given us. We are often asked if it is frustrating to work under the condition that our successes are known, most of the time, only to ourselves. If ever that is a burden it is far outweighed by the unique compensation of which we are the recipient, and that is the privilege of contributing to a safer and stronger Canada.

Richard B. Fadden
Director, Canadian Security Intelligence Service

TABLE OF CONTENTS

THE THREAT ENVIRONMENT

THE THREAT ENVIRONMENT

Terrorism and Extremism

As in recent years, the greatest threat to the national security of Canada is terrorism, a phenomenon that, in Canada, has been associated with a variety of radical political and religious movements.

Although the face of terrorism continues to be a diverse one, today the most salient threat has the form of Islamist extremism. In 2010-2011 there were many reminders that the threat is real and serious. The last members of the domestic

terrorist network known as the Toronto 18 received their prison sentences, culminating in a life term for Sahreef Abdelhaleem (see *Making History* on page 21). Yet just as the Toronto 18 case reached its judicial conclusion, the existence of an unrelated suspected terrorist cell became public with the arrests in August 2010 of three Ontario men.

While some Canadian terrorists have sought to commit attacks here at home, others have been implicated in plots against targets abroad. Canadians seeking to conduct terrorism in other countries are of concern to Canada in the same way that Canada expects foreign governments to take responsibility for their own citizens who support terrorism against Canadians. In March 2011, Canadian authorities issued arrest warrants for two former Winnipeg residents suspected of travelling abroad for the purpose of supporting terrorism. The warrants, issued in absentia since the accused are no longer in Canada, illustrated the transnational nature of the terrorism threat today.

Despite a series of setbacks including the death of leader Osama bin Laden, Al Qaeda (AQ) remains one of the most dangerous terrorist groups in the world. Failed terrorism plots in a number of Western countries have led investigators back to largely ungovernable areas in the border regions of Afghanistan and Pakistan. The region will remain a significant source of terrorist activity for the foreseeable future.

Groups affiliated with AQ in different parts of the world also pose significant terrorist threats. In 2010, Al Qaeda in the Arabian Peninsula (AQAP), based out of Yemen, asserted itself as an AQ affiliate that continues to present a significant danger to the West. The group is determined and innovative, as was made clear by its attempt in the fall of 2010 to blow-up cargo planes over North America using doctored printer-cartridges. This innovative attack-planning had already been demonstrated by its previous 2009 Christmas Day attempt to blow up a US-bound airliner as it approached Detroit. Had these attacks been successful, the airplanes might well have been downed over Canadian cities, resulting in significant Canadian casualties.

AQAP has suffered noteworthy setbacks with the deaths of two key members, Anwar al-Awlaki and Samir Khan. Both were US citizens and the creators of AQAP's English-language jihadist publication *Inspire*. Despite their elimination, the group is believed to retain operational capacity. Furthermore, AQAP is in an excellent position to exploit the unrest in Yemen and other parts of the Arab world in order to enhance its operational capabilities.

Other Al Qaeda-affiliated groups also survived, notwithstanding vigorous counter-terrorism operations. Al Qaeda in Iraq (AQI), which had repeatedly been described as in a state of near collapse due to US pressure in Iraq, demonstrated resilience with a number of attacks in 2010 and 2011. In North Africa, Al Qaeda in the Islamic Maghreb (AQIM) continues to pursue a campaign of kidnapping and small-scale attacks in the Sahel and North Africa. The threat posed by AQIM may increase if it is able to exploit the current unrest in North Africa.

A major national security concern for Canada emanates from the troubled African state of Somalia, where the ruthless terrorist group Al Shabaab controls significant parts of the country and operates with relative impunity. Numerous young Somali-Canadians have travelled to Somalia for terrorist training, a disturbing phenomenon that has also been seen in the US and in other Western countries with a Somali diaspora. There have been reports that some of these individuals, including Canadians, have been killed as a result. Although it falls outside the review period of this report, in October 2011 an alleged Al Shabaab suicide bomber delivered a message specifically calling for attacks inside Canada, among other countries.

Somali-Canadians are rightly worried about the radicalization of some of their youth, and the national security community – including CSIS – is committed to helping families and communities keep their children from pursuing a path that can have no good outcome.

Groups such as Al Shabaab, AQ, and those affiliated with AQ continue to train terrorists and to encourage supporters around the world to carry

out attacks against Western targets. The recruitment of Western citizens to participate in terrorist acts is a priority for these groups, because such operatives have easy access to Europe and North America.

The threat of "home-grown" extremism is of paramount concern to Canadian national security. It refers to the indoctrination and radicalization of individuals into the ideology espoused and propagated by Al Qaeda. This threat can be seen in several recent cases globally: in February 2012, four UK citizens, arrested in December 2010, were convicted of plotting to bomb the London Stock Exchange; similarly, in July 2011, a US soldier was arrested for plotting a shooting at the US military base Fort Hood, looking to replicate the earlier shooting by Major Nidal Hasan. All admitted to having read *Inspire* magazine.

CSIS has worked diligently to understand the dynamics of radicalization – the process whereby individuals move from holding moderate, mainstream beliefs towards adopting extremist political or religious ideologies. In early 2011, CSIS's Intelligence Assessments Branch produced an important research report on radicalization in Canada. The study does not identify a single, predictable pattern of radicalization. The process by which someone moves from moderate beliefs to extremist beliefs is a personal one. It varies from individual to individual. There is no single, linear process that leads to extremism.

Several drivers do appear with some frequency, however, including the adoption of significant grievances against Western governments, their societies and way of life, as well as the conviction that the Muslim world is under attack and needs defending through the use of violence. The influence of a charismatic ideologue such as the late Anwar Al-Awlaki becomes magnified in these environments. The abundance of Internet-based lectures and propaganda supporting a radical cosmology also contributes to the process.

Violent extremists have come from all social and age levels, are spread widely across the educational spectrum and can appear fully integrated into society, making detection and intervention difficult. As a result of these challenges, CSIS continues to study the phenomenon and is working with allies in this regard.

Hizballah's main preoccupations in 2010-2011 were to extend influence over Lebanese political life while managing allegations regarding its involvement in the 2005 murder of former Prime Minister Rafiq Hariri. Hizballah continued the pace of its Syrian and Iranian-supported military rearmament. The improved quantity, lethality and sophistication of its weapons systems have reinforced its dominance in the south of Lebanon and the Bekaa Valley, where the authority of the Lebanese Armed Forces is severely restricted. Hizballah maintains training camps, engages in weapons smuggling and drug trafficking, and also maintains an arsenal of thousands of rockets aimed to the south, at Israel. Hizballah's increasing political role and military capabilities directly serve the geo-political interests of its Iranian and Syrian patrons.

Combining Palestinian nationalism with Islamist extremism, Hamas paradoxically continues to advocate the destruction of Israel on the one hand, and a long-term ceasefire on the other. Hamas's engagement in politics since its 2007 takeover of Gaza and its competition with Fatah has forced the group to develop a delicate balance between competing interests. Hamas has had to tone down some of its Islamist rhetoric, frequently placing secular political considerations before strictly religious objectives. Hamas's immediate concerns centre on lifting the economic blockade of Gaza and securing the release of prisoners in Israel. While it insists on maintaining control of Gaza, it also seeks to avoid being marginalized in any negotiations with Israel. In part, this may explain its recent reconciliation with Fatah.

Birth of a revolution

On December 17, 2010, a Tunisian fruit vendor named Mohamed Bouazizi set himself on fire to protest the lack of economic opportunity and political freedom in his country. His suicide became a symbolic expression of despair that resonated among millions of other young people in the Arab world. Mass protests and then revolution ensued, leading to the collapse of long-standing regimes in some Middle Eastern countries.

Will the upheaval of the political order in the Middle East diminish or increase the threat to Canadian security interests? That is a complex question, one that will preoccupy CSIS for the next year and beyond. Analysts are well aware that the region lacks a strong tradition of democratic politics. The various repressive regimes have always had opponents, but those opponents have not typically exhibited democratic instincts. There is a perennial anxiety that violent extremists will see in the tumult an opportunity to strengthen their own hand.

At the same time, it's impossible to watch the Arab Spring and not hope that it marks the stirring of genuine democratic reform. The drama is only beginning. It is one the whole world is watching, because the outcome has implications for international security.

TUNISIANS PARTICIPATE IN THE POPULAR UPRISING THAT TOPPLED THEIR LONG-STANDING DICTATOR.

Other forms of violence, motivated by ideology, continue to threaten Canadian national security. Domestic or "multi-issue" extremists in Canada, though small in number, are capable of orchestrating acts of violence, as illustrated by the 2010 firebombing of a Royal Bank branch in Ottawa. This represented a serious case of politically motivated violence against the financial sector. The grievances harboured by those who oppose issues such as the perceived oppressive effects of capitalism are likely to continue and may trigger additional acts of serious violence.

Right-wing extremism has not been a significant problem in Canada in recent years. Those who hold such views have tended to be isolated and ineffective figures. However, the 22 July 2011 bombing and shooting rampage in Oslo, Norway, which killed 77 people, showed that a marginalized individual, if properly motivated, can successfully execute mass-casualty terrorism. The fact that such "lone actors" are by definition operating individually increases their chance of operational success, because they are hard to detect.

The varied nature of the terrorist threat requires a multi-tiered response. CSIS works locally, nationally and internationally to identify threats to Canada and to its foreign partners. The arrangements CSIS has established with services and agencies in Canada, and around the world, ensure that the information-exchanges necessary to combat terrorism are in place.

Saving lives, far from home

Of all the successes in 2010-2011, the Service is particularly proud of our work in Afghanistan. Beginning in 2002, CSIS played a critical role in supporting Canada's combat mission in that country. Information collected by CSIS in Afghanistan saved lives – Canadian lives and the lives of Afghan civilians. The end of the Canadian combat mission in Afghanistan has changed how CSIS focuses its efforts in that region, but it has not brought those efforts to an end. Our mandate is to follow the threat. And as long as the activities of extremist networks operating in Afghanistan threaten Canadian interests, the region will remain an important intelligence concern for the Service.

Terrorist Financing and Financial Investigation

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

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

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

In 2010, a British Columbia man, Prapaharan Thambithurai, was the first person to be charged and convicted for terrorist financing. He pleaded guilty to the offence and was sentenced to six months in jail after admitting to police that some of his collection was directed to the Liberation Tigers of Tamil Eelam, a listed terrorist entity in Canada. A 2011 Crown appeal for a longer sentence was dismissed by the BC Court of Appeal.

Some foreign investments in Canada can also pose wider national security concerns. The *Investment Canada Act* provides the Government of Canada with a mechanism to ensure that foreign investments are within Canada's national security interests. CSIS plays a contributing role by advising government of the national security implications that might arise from a proposed foreign investment.

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 poses a significant threat to the security of Canada, its allies and the international community. Regardless of whether proliferation is carried out by state or non-state actors, the pursuit of WMD increases global tensions and may even precipitate armed conflicts. Their actual use in war, the idea of which is anathema to Canadian values, would cause unspeakable suffering and devastation. Canada is a party to many international conventions and other arrangements designed to stem the proliferation of WMD, and CSIS works closely with both domestic and foreign partners to uphold the nation's commitment to this cause.

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

The danger of nuclear proliferation remains acute. 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 and successive UN Security Council resolutions demanding that it cease such activity.

North Korea has twice tested a nuclear explosive device. The country is believed to have sufficient plutonium for a small arsenal of nuclear weapons and it recently revealed the existence of a uranium enrichment program that could further add to its arsenal. North Korea's nuclear proliferation has a destabilizing impact on the Korean Peninsula and Northeast Asia. Canada has significant economic and strategic interests in this region that could be at risk from North Korea's activities in this regard. South Korea is Canada's seventh-largest trading partner and the third-largest in Asia after China and Japan. There are more than 20,000 Canadians living in South Korea and 200,000 Canadians of Korean origin who could be deeply affected in the event of a conflict.

North Korea has shown no inclination to "denuclearize," as called for by the international community and, moreover, has been proven willing to export its nuclear technology to states such as Syria. In South Asia, a principal concern remains the nuclear arsenal of Pakistan and questions over the security of those weapons systems given the domestic instability in that country.

A number of terrorist groups have sought the ability to use CBRN materials as weapons. Some groups such as Al Qaeda have pursued efforts to cause mass casualties with biological agents such as anthrax, or improvised nuclear explosive devices. While the technological hurdles to such efforts remain 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 would far outweigh the actual casualties inflicted.

Keeping threats out

Whatever the threat to Canada, we at CSIS believe that it should be stopped as early as possible – at its source if practical – and not necessarily overtly or in the public eye. To this end, we are actively working with our partners to ensure the forward defence of Canada. Through our overseas operations, CSIS plays a key role in helping to curb irregular and illegal migration to Canada. We provide security screening advice to Citizenship and Immigration Canada, and we participate in joint intelligence operations against complex trafficking, smuggling and financing networks that seek to exploit Canada. These efforts help keep potentially dangerous individuals from entering this country.

Cybersecurity

The Internet and other communication technologies allow any individual, group or organization to attack Canada without having to set foot here. These hostile actors can include both state and non-state actors: foreign intelligence agencies, terrorists, "hactivists" or simply malicious individuals acting alone. Regardless the motivation, hostile actors have access to a growing range of cyber attack tools and techniques. Media reporting on cybersecurity reflects a growing awareness of the destructive impact that such attacks can have on Canada, both for the private and public sector. As technologies evolve and become more complex, so too do the challenges of detecting and protecting against cyber attacks.

We have seen attacks against a wide variety of departments at the federal, provincial and even municipal level. In January 2011, attackers targeted the networks of the Finance Department and Treasury Board. Unfortunately attacks like this are not a rare exception. The Government of Canada is now witnessing serious attempts to penetrate its networks on a daily basis.

In the private sector we also observe a wide range of targeting. The main target, which is similar in traditional economic espionage, is the aerospace and high-technology industry. From the attackers' perspective, it is significantly cheaper and often less difficult to steal research than to develop it. Another traditional economic espionage target we often come across is the oil and gas industry and universities involved in research and development. In addition to stealing intellectual property, state-sponsored attackers are also seeking any information which will give their domestic companies a competitive edge over Canadian firms: an example would be inside knowledge of upcoming negotiations – personalities involved, their likes and dislikes, and so on.

CSIS broadly defines a cyber-related attack as the use of information systems or computer technology as either weapon or target to gain unauthorized access to, or direct malicious activity against, computers, networks, or communications. Attackers have employed carefully crafted e-mails, social networking services and other vehicles to acquire government, corporate or personal data. Foreign intelligence agencies use the Internet to conduct espionage operations, as this is a relatively low-cost and low-risk way to obtain classified, proprietary or other sensitive information.

Given the borderless and instantaneous nature of cyber transactions, foreign actors could stage an operation against a Canadian target in a very short period of time. Cyber operations targeting Canada will likely persist in the foreseeable future as technological advances make this form of espionage particularly attractive.

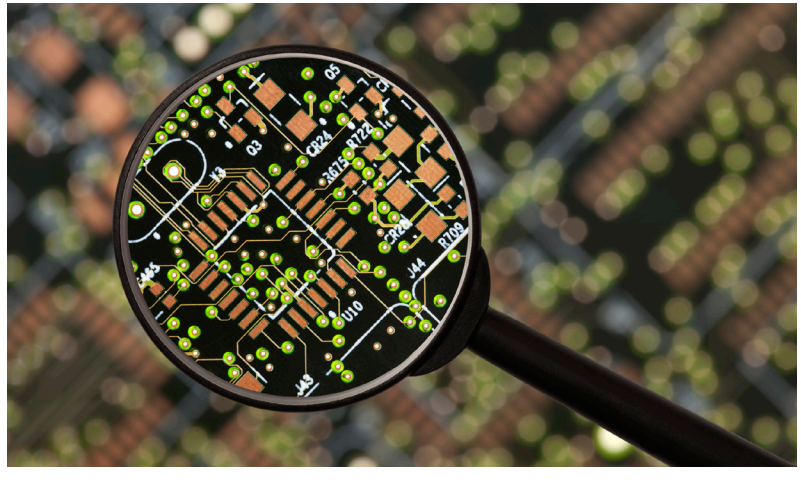
Cyber attacks, however, are not limited to data theft or espionage. An adversary can also target critical infrastructure – energy grids, communication networks, financial systems – and disrupt our way of life in very significant ways. For instance, the August 2003 blackout that affected 50 million people across eastern North America shows the

potential impact a major cyber event could have. Although the incident was not a terrorist or cyber attack, it highlighted the vulnerability of technologically advanced societies.

Because the threat from cyber-espionage, cyber-sabotage and other cyber operations are part of a broader economic threat to key sectors of Canadian society, CSIS works closely with other government departments such as the RCMP, the Department of National Defence (DND), the Communications Security Establishment Canada (CSEC), and Public Safety Canada (PSC). CSIS also liaises with international partners in order to remain abreast of the global threat.

As outlined in the Government of Canada's Cyber Security Strategy, CSIS will analyze and investigate domestic and international threats to the security of Canada, responding to the evolution in cybersecurity technologies and practices.

Canada's National Strategy for Critical Infrastructure and the Action Plan for Critical Infrastructure promote partnerships among critical infrastructure sectors and all branches and levels of government, to improve information sharing and protection.



Espionage and Foreign Interference

CSIS continues to investigate and advise the Government of Canada on espionage and foreign interference. Espionage is a reality in the post-Cold War era where economic and strategic competition is both global and intense. Canadian interests are damaged by espionage activities through the loss of assets and leading-edge technology; the leakage of confidential government information or applications; and the coercion and manipulation of ethno-cultural communities in Canada.

Foreign governments have traditionally conducted covert intelligence-gathering operations in Canada through diplomatic missions, various organizations, and by recruiting agents or informants. As a founding member of the North Atlantic Treaty Organization (NATO), a signatory to a number of other multilateral and bilateral defence agreements, and a close economic and strategic partner of the United States, Canada remains an attractive target for espionage. A number of foreign governments continue to clandestinely gather political, economic and military information in Canada; they have also targeted Canada's NATO allies for information related to NATO's military and political activities.

In recent years there have been several high-profile cases in Canada, the US and Europe highlighting the use of "illegals" – foreign intelligence operatives living in their target country under assumed identities, without the protection of diplomatic immunity. The use of illegals is an example of a very traditional approach to espionage – that is, the use of human intelligence – but espionage via technology, especially cyberspace as detailed earlier, is becoming more significant every year.

Looking North

CSIS is a national service with a national presence, and that includes the Canadian North. As the Arctic becomes ever-more attractive to foreign countries as a source of natural resources and possible trade routes, the Service will play a role in helping the federal government ensure the sovereignty and security of Canada's Arctic Archipelago and adjacent waters.

The Arctic occupies an important place in our collective consciousness, but it is also increasingly acquiring a strategic dimension. A key component of Canadian national identity is our status as a northern country, and that is worth protecting.

CSIS HAS A ROLE TO PLAY IN HELPING THE FEDERAL GOVERNMENT ENSURE THE SOVEREIGNTY AND SECURITY OF THE CANADIAN NORTH.

In today's global economy, knowledge is power, especially in areas of science and technology. Many countries will therefore go to great lengths to find an advantage, which has led to a noticeable increase in clandestine attempts to gain unauthorized access to proprietary information or technology.

As a world leader in communications, biotechnology, mineral and energy extraction, aerospace and other areas, Canada remains an attractive target for economic espionage. Several countries engage in economic espionage against Canada to acquire expertise, dual-use technology and other relevant information related to those and other sectors. It's important to note that those who commit economic espionage are not just interested in domestic Canadian interests and resources. Canada's commercial interests abroad are similarly vulnerable. The implications of economic espionage on Canada can be measured in lost jobs, in lost tax revenues and in an overall diminished competitive advantage.

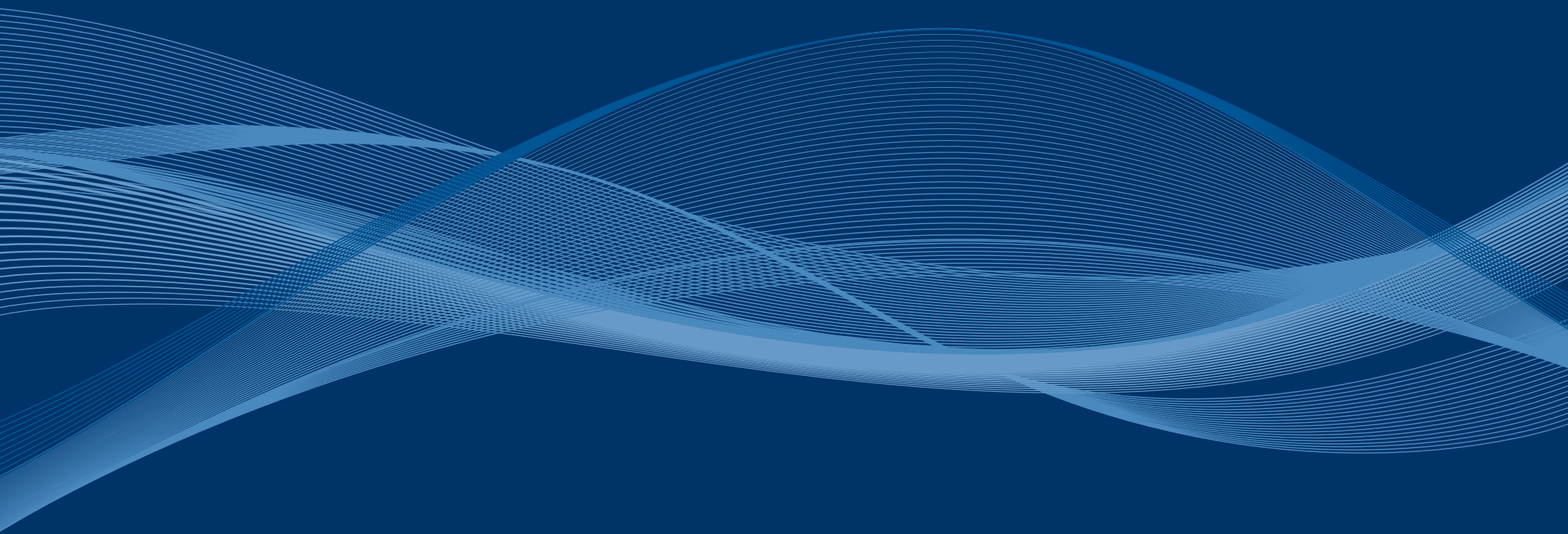
A related security issue is one of foreign investment. Canada is a trading nation, with economic wealth, advanced infrastructure and vast potential – all of which make Canada a natural and attractive prospect for foreign investors. While the vast majority of foreign investment in Canada is carried out in an open and transparent manner, certain state-owned enterprises (SOEs) and private firms with close ties to their home governments have pursued opaque agendas or received clandestine intelligence support for their pursuits here.

When foreign companies with ties to foreign intelligence agencies or hostile governments seek to acquire control over strategic sectors of the Canadian economy, it can represent a threat to Canadian security interests. The foreign entities might well exploit that control in an effort to facilitate illegal transfers of technology or to engage in other espionage and other foreign interference activities. CSIS expects that national security concerns related to foreign investment in Canada will continue to materialize, owing to the increasingly prominent role that SOEs are playing in the economic strategies of some foreign governments.

Finally, as per our legislative mandate, CSIS continues to investigate foreign interference. This refers to the phenomenon whereby foreign governments or their agents attempt to influence clandestinely Canadian policies and opinions. It also refers to the effort by some foreign powers to engage in covert monitoring and intimidation of diaspora groups in Canada.

Foreign interference is particularly nefarious because it can have the effect of disrupting the multicultural harmony that is central to Canadian identity. It is to protect immigrant communities that CSIS collects intelligence about foreign interference. Members of diaspora groups are typically the victims of foreign interference. They should be able to live in peace and not worry about being watched, harassed or coerced by foreign powers.

MAKING HISTORY (TORONTO 18)



MAKING HISTORY (TORONTO 18)

On March 4, 2011, the most important counter-terrorist operation in Canadian history reached its conclusion in a Brampton, Ontario, courtroom when Shareef Abdelhaleem received a life term in prison. He was the last member of the terrorist network known as the Toronto 18 to be sentenced.

The public story of the Toronto 18 began in early June of 2006 when law enforcement authorities arrested a large group of men and teenagers from the Toronto area on suspicion of planning a mass-casualty attack inside Canada.

At CSIS, though, the story began well before that. The Service was aware of the plot and, using an array of investigative tools from cutting-edge technology to old-fashioned human sources and surveillance, had been monitoring the suspects closely.

At the time of the arrests, some Canadians wanted to minimize the seriousness of the case, believing that terrorism is something that happens in other countries. Yet the subsequent criminal trials revealed that the Toronto 18 was the real thing, a *bona fide* instance of "homegrown" terrorism. Eleven of the original 18 were sent to prison.

Had the conspirators successfully executed their plan to set off bombs at the Toronto Stock Exchange and other public places, Canada would have been forever changed.

The case assumed historic significance for a number of reasons.

First, it raised the security awareness of Canadians. "T-18" is recognized as a counter-terrorism case-study, a model of how security officials and police authorities (CSIS and the RCMP) can work together in a way that achieves a common goal while not diluting or overstepping their respective legislative mandates.

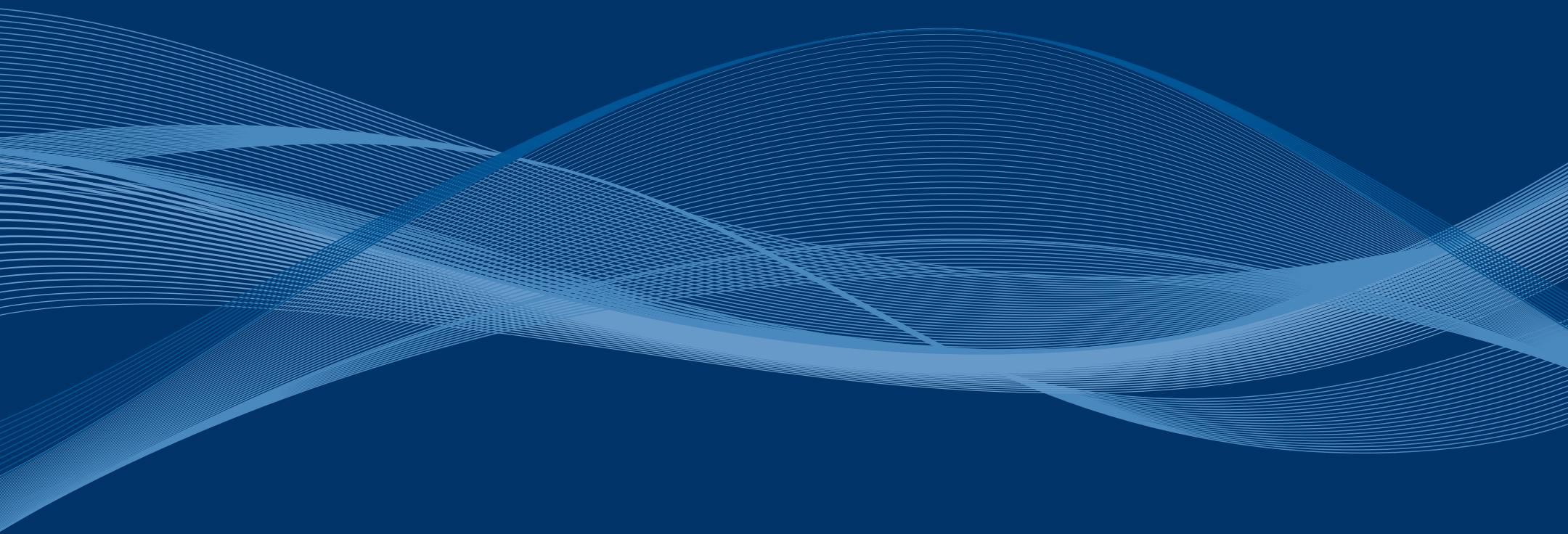
Second, the investigation showed that violent extremism can incubate even in a peaceable and pluralistic country such as Canada: seemingly ordinary young men who grew up in Canada came to reject the Western, liberal and democratic values that underpin Canadian identity, instead replacing them with the violent, anti-Western ideology of Al-Qaeda.

It is the view of CSIS that the culmination of an investigation in the form of criminal charges is never an occasion for celebration. Many of the accused at the centre of the Toronto 18 investigation had promising futures. One was a successful computer engineer. Of course one's primary thoughts are with the potential victims of terrorism, but losing a son or daughter to violent extremism is still losing a child.

Many CSIS teams from across the organization worked on the investigation, some around the clock for weeks at a time. It was a period of high tension; the time between the planning and execution of a terrorist attack can be dangerously short.

The mandate of CSIS is to protect Canada's security interests. In the case of the Toronto 18 this meant protecting the most fundamental of all interests: the right to life and to physical security.

SECURITY SCREENING PROGRAM



SECURITY SCREENING PROGRAM

The CSIS Security Screening program serves as the first line of defence against terrorism and extremism, espionage and the proliferation of weapons of mass destruction. The program is designed to prevent individuals who pose a threat to the security of Canada from entering or obtaining status in Canada or from obtaining access to sensitive government sites, assets or information.

In 2010-2011, the Security Screening program remained one of the most visible operational activities undertaken by the Service. CSIS processed more than 500 000 Security Screening cases for its clients.

Government Security Screening

The Policy on Government Security (PGS) states that security clearances are required for employees of the Government of Canada, and for persons under contract to a federal government department who have lawful access to classified government assets or information. The Service, under the authority of sections 13 and 15 of the *CSIS Act*, is mandated to investigate and provide security assessments to government departments and institutions for this purpose. However, the PGS gives these departments and institutions the exclusive authority to grant or deny such clearances.

The Service's Government Screening Section also supports several site-access programs. CSIS provides security assessments for individuals requiring access to major ports, airports, sensitive marine facilities, nuclear power facilities, the Parliamentary Precinct, as well as certain provincial and federal government departments. These programs enhance security and reduce the potential threat from extremist and terrorist groups and foreign governments seeking to exploit such access.

Some examples of the Service's work include security assessments provided to the Canada Border Services Agency (CBSA) for commercial drivers who apply for a border pass under the Canada-US Free and Secure Trade program (FAST); and assessments on certain locally engaged staff (foreign nationals) at Canadian missions abroad. The latter are provided to the Department of Foreign Affairs and International Trade.

Foreign Screening

Under reciprocal screening agreements, CSIS provides security assessments to foreign governments and international organizations (such as NATO) concerning Canadian residents who reside abroad and are being considered for positions requiring classified access in a foreign country. Canadian citizens about whom information is being provided must give their consent in advance. All screening arrangements with foreign entities are approved by the Minister of Public Safety after consultation with the Minister of Foreign Affairs and International Trade Canada.

Government Screening Programs

Requests received *	**2009-2010**	**2010-2011**
Federal Government Departments	64,300	54,400
Free and Secure Trade (FAST)	7,700	31,800
Transport Canada (Marine & Airport)	34,900	35,100
Parliamentary Precinct	1,100	1,400
Nuclear Facilities	9,500	12,500
Provinces	850	260
Site Access-Others	3,400	2,500
Special Events Accreditation	200,800**	24,200
Foreign Screening	490	500

* Figures have been rounded
** Increase largely due to the 2010 Winter Olympic Games

Screening in action I

In 2010, the Service received Permanent Resident applications from Citizenship & Immigration Canada (CIC) for a group of seven foreign nationals who were sponsored and being considered for status and re-settlement in Canada. Service investigation revealed that all seven applicants were either under investigation or under arrest for links to or membership in extremist organizations which were also listed terrorist entities in either the US or Canada. The Service provided advice to the Canada Border Services Agency (CBSA) in accordance with section 14 of the *CSIS Act*, indicating that all seven individuals had either links to or membership in an extremist cell. All seven applicants were subsequently deemed inadmissible and refused Permanent Resident status in Canada.

Immigration and Citizenship Screening

While Canada's long and valued tradition of welcoming immigrants and visitors continues, Canada and its allies must continue to remain vigilant in countering acts of political or religiously motivated violence and espionage. Maintaining the integrity of the immigration system is essential to strengthening Canada's security environment.

The objective of CSIS's Immigration and Citizenship Screening Program is to assist the Government of Canada in preventing non-Canadians who pose a threat to national security from entering or obtaining status in Canada. CSIS, under the authority of sections 14 and 15 of the *CSIS Act*, provides advice to CBSA and to Citizenship and Immigration Canada (CIC) based on the security-related criteria contained in the *Immigration and Refugee Protection Act (IRPA)* and the *Citizenship Act*.

This program includes the following essential screening components: applicants for permanent residence from within Canada and abroad; refugee claimants (Front End Screening); applicants for Canadian citizenship; and the screening of visitors from countries of terrorism, proliferation, and espionage concern.

CSIS strives to provide quality advice to partner departments, on time. While the total number of immigration screening requests received in 2010/11 remained at approximately the same levels as the previous year, processing time for these requests were in many cases halved. The median number of calendar days required to process permanent resident applicants living in Canada dropped from 78 days to 38 days. Processing times for refugee claimants dropped from a median of 74 to 48 days. For regular permanent resident applicants, from Canada, the US or overseas, the combined median processing time was 29 days - eight fewer than in 2009/10.

Spotlight: Screening of Refugee Claimants (Front End Screening)

Canada's refugee determination system is recognized around the world for its fairness in offering protection to genuine refugee applicants. However, without proper safeguards, the system is vulnerable to criminals or terrorists posing as refugees. The Government of Canada's Refugee Determination Program is Canada's first line of defence, with a mandate to screen all refugee applicants in order to determine their admissibility to Canada.

The CSIS Security Screening program supports the Refugee Determination Program. By conducting security screening investigations, CSIS provides security advice regarding refugee applicants to CBSA and CIC. The program's goal is to ensure that individuals deemed inadmissible to Canada for security reasons under the *IRPA* are identified as early as possible in the refugee determination process and prevented from taking up residence.

Immigration and Citizenship Screening Programs

Requests received *	2009-2010	2010-2011
Permanent Residents Within and Outside Canada	77,600	79,600
Front End Screening**	23,500	17,400
Citizenship Applications (Marine & Airport programs)	175,500	198,800
Visitors Visa Vetting	67,800	71,400

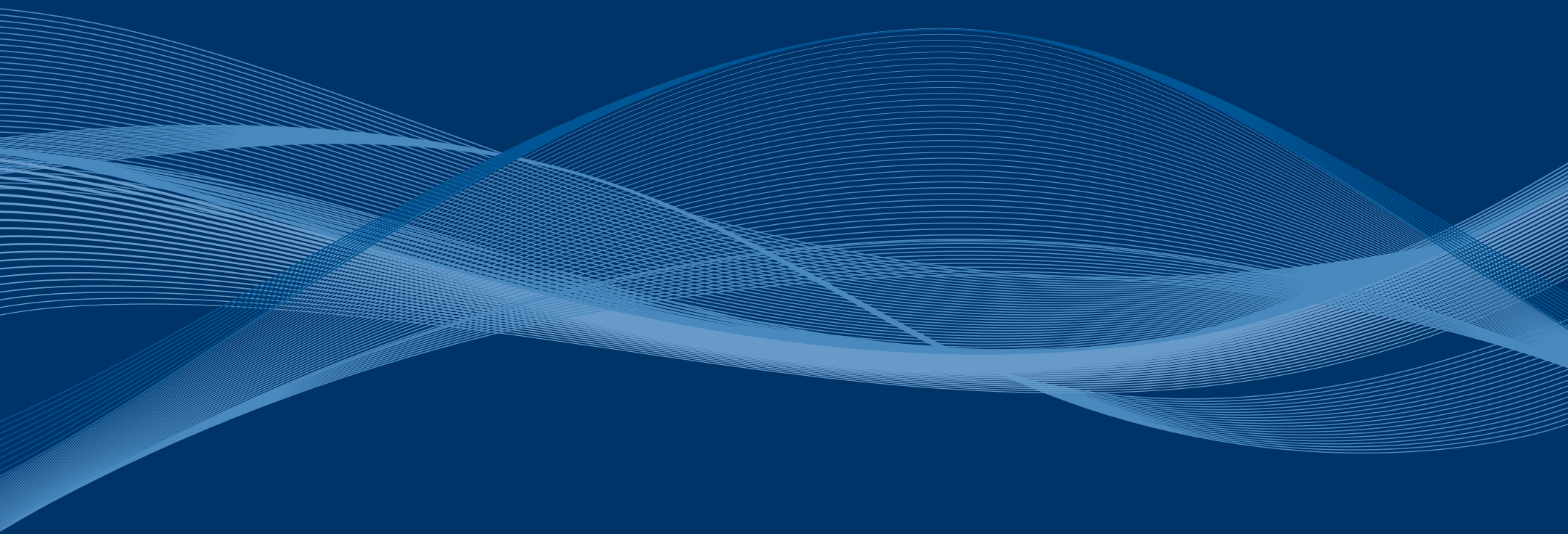
* Figures have been rounded.
** Individuals claiming refugee status in Canada or at ports of entry.

Screening in action II

Nearing the end of Canada's mission in Kandahar Province, Afghanistan, the Government of Canada initiated a Special Immigration Measures (SIM) program to support the immigration to Canada of a select number of locally engaged staff who provided valuable support to Canada's efforts throughout the preceding years. The Service, as a whole-of-government partner, was instrumental during this program in providing security advice to both CBSA and CIC in accordance with section 14 of the *CSIS Act.* CSIS advice focussed upon threats or potential threats posed by applicants from this volatile and complex environment.

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

AT HOME AND ABROAD



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 & 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.

In 2010-2011, 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 the police – the RCMP – collect evidence for criminal prosecution.

This division of labour worked well during the Cold War period but has arguably become more complicated in the post 9-11 age of international terrorism. Most notably, plotting a terrorist attack is as much a crime as carrying one out. This means that the intelligence a CSIS officer collects about a suspected plot could be legally indistinguishable from evidence – and yet the collection of evidence is normally a job for police, not the security service.

In 2010-2011, CSIS and the RCMP continued to develop a series of protocols on information-sharing. There is a growing body of Canadian jurisprudence in this area, which the Department of Justice and the Public Prosecution Service of Canada have helped interpret for CSIS and the RCMP. The goal is to ensure that both organizations work together in a way that enhances the national security of Canada while at the same time respecting their respective legislative mandates. Fortunately, there is much to build on. The Toronto 18 case, for example, is widely recognized as a model of how CSIS and the RCMP can run separate yet parallel counter-terrorism investigations.

Over the next year, CSIS will continue to work with RCMP on articulating respective roles so that an already productive and effective relationship becomes even more so.

Foreign Operations and International Cooperation

Over the past decade, the Service has increasingly focused on global issues and specifically on how they affect the national security interests of Canada. As such, the Service has enhanced its international presence.

Section 12 of the *CSIS Act* does not distinguish between domestic and foreign collection, and thus allows the Service an equal mandate to collect security intelligence abroad. CSIS has officers stationed in cities and capitals around the world, among them Washington, Paris and London. Their primary function is to collect security intelligence information related to threats to Canada, its interests and its allies.

Occasionally, the Service is obliged to send Canada-based officers abroad to respond to certain extraordinary situations. Examples of this include evacuations of Canadians from nations in turmoil and kidnapping of Canadian citizens. CSIS officers stationed abroad also provide screening support to Canada's Citizenship and Immigration (CIC) offices.

The decision to give CSIS a mandate to collect security intelligence abroad emerged from the Parliamentary debates in the early 1980s when the *CSIS Act* was being crafted. The intent was clearly to ensure that CSIS could follow the threats wherever they might materialize.

Another consequence of the transnational nature of today's security threats is the increased cooperation among governments and their security agencies.

In 2010-2011, CSIS implemented 11 new foreign arrangements and as of March 31, 2011, had 289 arrangements with foreign agencies or international organizations in 151 countries. Of those arrangements, 41 are currently defined as dormant, meaning there have been no information exchanges for a period of one year or longer. During that same period, six existing foreign arrangements were either enhanced or altered by the Service. Additionally, eight arrangements were categorized as having restricted contact due to concerns over the reliability of the foreign agencies in question.

Exchanging information with foreign agencies remains a key component in CSIS's ability to effectively carry out its mandate. In a globalized world, security threats such as terrorism, espionage or proliferation of weapons of mass destruction, recognize no borders. (See next section "Sharing Responsibly")

Foreign terrorists continue to inspire and provide direction to individuals and groups in Canada. Some Canadians have left the country to seek training in terrorist camps in Somalia, Pakistan and elsewhere in an attempt to support or conduct terrorist operations within Canada or abroad. Additionally, over the past several years, Canadians have been kidnapped in places such as Iraq, Afghanistan, Somalia, Pakistan, Niger, and Sudan. Certain Canadian businesses and their workers abroad have been targeted or threatened.

Canadian Forces and government officials in high-risk areas such as Afghanistan also continue to operate in precarious and dangerous surroundings. The same can be said for CSIS officers. In 2010-2011, the Service continued to provide timely reporting from Afghanistan in support of Canada's mission in that country. CSIS supported allied efforts to combat extremism with a nexus to the region and provided intelligence which contributed to the safety and security of Canadians, allies and Afghan citizens within the country.

Elsewhere, Canada's national security interests are potentially threatened by illegal migration and human smuggling, which again are issues of an international scope. Similarly, weapons proliferation – chemical, biological, radiological and nuclear – is a global problem that no one country can address alone.

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

Our international allies expect Canada to assume responsibility for investigation of threats posed by Canadians abroad, just as we expect the same from our partners. As a result, CSIS has become increasingly competent in the international arena and with global issues.

Sharing Responsibly

No single idea has had a more profound impact on national security policy than the recognition that public safety is a shared effort, both domestically and internationally.

Most obviously, terrorism is a phenomenon without borders, as the 9-11 attacks dramatically illustrated. The plot was directed from Taliban Afghanistan, one of the most anti-democratic and undeveloped countries in the world; the target was the United States, one of the world's oldest and most developed democracies. The hijackers were mostly from Saudi Arabia, while the planning took place in Hamburg and other cities. Because the attacks targeted the aviation sector – a global industry – the reverberations were felt across the world, economically and in other ways.

Instability in one part of the world can directly impact the security situation in another part of the world. The permeability of borders has been hastened thanks to technology, as expressed in cyber-espionage and hacking. Foreign actors or states can disrupt our way of life in profound ways without ever coming into our country or even near our shores.

CSIS's mandate is to collect information about security threats to Canada, and to fulfill that mandate we need to exchange intelligence with allies and other partners around the world. It used to be that in the security intelligence community the catchphrase was "need to know." That is still the case in many ways, but there is a recognition that a number of situations and investigations require a "need to share."

CSIS acknowledges that information sharing carries risks, especially with regards to foreign agencies in countries that do not have the same democratic traditions as Canada. At CSIS our overriding concern is to ensure that we are never complicit, directly or indirectly, in the mistreatment of any individual. As a result, our information-sharing practices are governed by strict standards and guidelines.

Indeed, the Service has one of the most stringent processes of all intelligence services with regards to information-sharing: Each of our foreign arrangement requests must be approved by the Minister of Public Safety after consultation with the Minister of Foreign Affairs; the Service uses proper caveats or instructions when sharing information; our review bodies – the Security Intelligence Review Committee and the Inspector General – have access to all CSIS foreign arrangement files and review those relationships on an annual basis.

It is abundantly clear in the post 9-11 era that collaboration across the international security intelligence community is non-negotiable. At CSIS, we have been able to meet our domestic and international responsibilities in a way that is consistent with Canadian law and that reflects Canadian values.

A UNIQUE WORKPLACE

A UNIQUE WORKPLACE

Our People

In 2010-2011, the number of full-time staff at CSIS totalled 3,285. Our workplace is a highly diverse one, representing the rich mosaic of Canada. Collectively, our employees speak about 105 languages. With respect to age demographics, four generations of workers can be found in our offices. We are evenly split among men and women.

A large majority of our staff – more than 70 per cent – speak both of Canada's official languages. Nearly 30 per cent of employees can speak a language other than English or French. Training is available to all employees in both official languages and many informal groups exist for employees who speak, or would like to learn to speak, other languages.

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

These achievements are reflected in our ability to retain top talent. For the fiscal year 2010-2011, we recorded a consistently low resignation rate of 0.7 per cent. In fact, the resignation rate has hovered around the 1 per cent mark for the last eight years. In addition, for every four employees eligible to retire in 2010-2011, only one chose to do so.

In addition the Service has adapted its training and development programs to ensure that all personnel are sensitive to the experiences and expectations of new Canadians. This training has become part of the formal learning curriculum, delivered by CSIS staff who can speak personally about different cultures and faiths as well as external experts representing religious or cultural communities.

Recruitment

CSIS has made it a priority to recruit a new generation of professionals who reflect the current demographic realities of Canada. The Service continues to attract bright, young Canadians to our ranks – people who have the knowledge, aptitude, skills and passion for modern intelligence work and the desire to protect Canada's national security. We continue to hire individuals who wish to pursue significant careers with CSIS in fields as varied as engineering, computer science, technology, communications, finance, and human resources, to name a few.

This past year, an unprecedented shift has taken place in the way CSIS recruits. Consistent with the Public Service Renewal initiative, the Service has transformed its recruiting approach from an informal word-of-mouth practice to a modern, branded, forward-looking one with the creation of a proactive recruiting and marketing strategy. This new direction was essential for the organization to remain current in industry-best recruitment practices. While much of the informal recruiting focus and attention of the past had been directed at Intelligence Officer (IO) positions, the need to find qualified applicants to fill non-IO positions, such as IT and engineering, is now greater.

Our accelerated recruiting needs also meant that the Service had to reach out to specialized sectors more aggressively. The Service had to be more creative and innovative – beyond traditional job fairs – in order to deliver its strategic recruiting message and raise the profile of the Service. Accordingly, CSIS became more visible to the public in 2011 as it attended high-profile events to promote jobs in the organization.

When attending recruiting events, many people are surprised to meet and chat one-on-one with actual employees of the Service. Just as importantly, the messaging over the past few months has been solid and constant: that CSIS is a smart career choice. Those who meet the basic requirements can apply on the micro site at www.intelligencematters.ca.

Financial Resources

CSIS's final expenditures for 2010-2011 totalled $515 million.

The Service's financial resources have increased since 2001-2002, 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.

In 2010-2011, additional funding was allocated through the Federal Budget to address CSIS's most acute program integrity needs. In addition, Federal Budget 2010 committed $3 million over three years to assist Citizenship and Immigration Canada and other partners, such as CSIS, in the implementation of a three year immigration backlog reduction strategy.

Incremental funding was approved to allow CSIS to meet its security-related planning roles and operational responsibilities for the 2010 Muskoka G8 Summit and G20 meeting. Over a period of two fiscal years (2009-2010 to 2010-2011), CSIS received a total of $3.1 million in support of the Service's role and requirements related to the security of the Summits.

Finally, CSIS was required to rationalize operations and ensure alignment with organizational needs as part of the Government of Canada's strategic review process in 2009-2010. As part of this strategic review the Service's budget will be reduced by $15 million effective 2012-2013.

Integrated Planning and Accountability

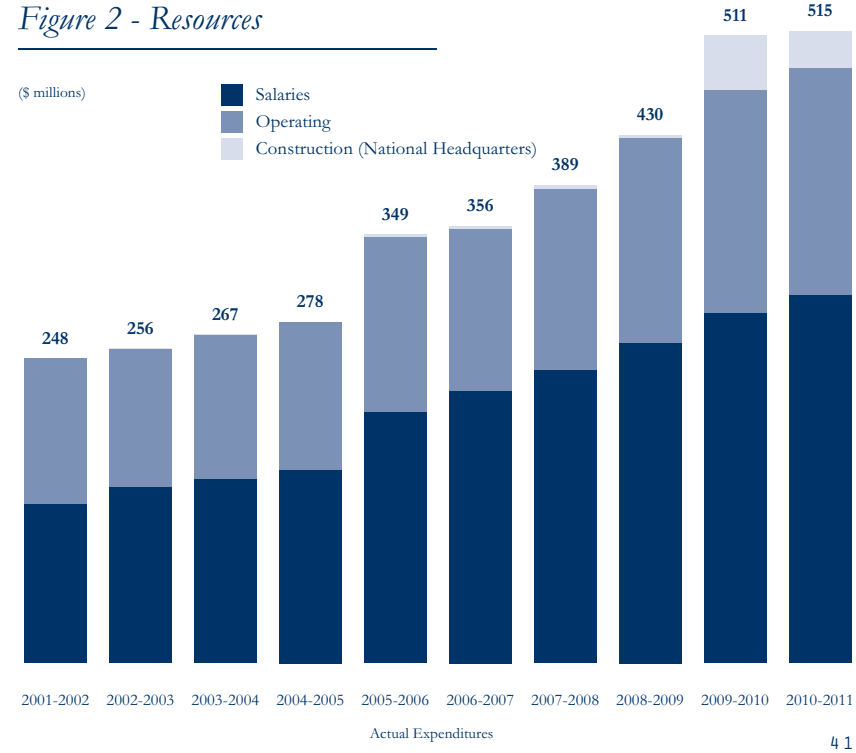
The Service has completed its second year of the Integrated Planning and Accountability initiative. In 2010, it successfully completed the first CSIS Integrated Business Plan (the Plan) and implemented a new mid-year review mechanism. These processes help CSIS to make critical and informed decisions about resource allocation in keeping with its top priorities, mandate and mission.

Integrated planning serves to create a roadmap which management and all employees can follow to fulfill their responsibilities. This is particularly important in times of global instability and of fiscal restraint. Using the Plan as a tool to improve the management of resources, mitigate risk and achieve better results for Canadians, the Service sets it priorities in response to both the evolving threat environment and domestic economic imperatives. Moving forward, the Service will build on the planning and mid-year processes, while continuing to develop a more integrated and rigorous performance and reporting framework.

Construction costs shown are for the expansion of CSIS National Headquarters. Costs incurred from fiscal year 2002-2003 to 2006-2007 represent expenditures associated with the project definition stage.

In 2007-2008 and 2008-2009, costs incurred were mainly attributable to the building's site preparation. The construction of Phase III began in the summer of 2009, with total expenditures of $30 million in 2010-2011. The building was officially opened by the Minister of Public Safety on 27 October 2011.

Figure 2 - Resources



REVIEW & ACCOUNTABILITY

REVIEW & ACCOUNTABILITY

CSIS is on occasion permitted to use what can be intrusive investigational techniques, and accordingly CSIS requires a strong system of accountability. The men and women of CSIS welcome the scrutiny. They understand they are expected not just to keep Canada safe but to do so in a way that is consistent with Canadian values.

CSIS is among the most reviewed intelligence agencies in the world. Fully two-thirds of our enabling legislation,

the *CSIS Act*, is dedicated solely to ensuring that the Service is subject to proper reporting and accountability mechanisms. The activities of CSIS are subject to review by the Security Intelligence Review Committee (SIRC), the Inspector General (IG) for CSIS, the Federal Court, as well as by various officers of Parliament, including the Auditor General and the Privacy Commissioner. The nearly three decades of interaction between CSIS and its review bodies have allowed the Service to develop and work with a robust set of operational policies, and to mature greatly as an organization.

The observations, recommendations and even occasional criticisms provided by our review bodies have made CSIS 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 under what circumstances and to what extent, the Service is to inform the Minister of its operations.

CSIS requires the approval of the Minister of Public Safety before entering into formal *CSIS Act* section 17 arrangements with domestic partners (s.17.(1)(a)) and foreign agency partners (s.17(1)(b)). This ensures 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 33 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, established in the *CSIS Act*, is an independent, external review body which reports to the Parliament of Canada on Service operations.

Every year, SIRC undertakes a set of reviews of CSIS operations. SIRC also investigates complaints surrounding Service activities. Individuals who have had a security clearance denied or revoked can similarly file a complaint before SIRC. Following each review or complaint investigation, SIRC provides observations and recommendations pertaining to the CSIS policy, program or operation in question.

While CSIS is not required by law to adopt SIRC recommendations, they are carefully considered. In fact, the Service has implemented most of SIRC's recommendations over the years.

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

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

The Inspector General (IG)

CSIS's second review body, the Inspector General (IG), is accountable to the Minister of Public Safety. The IG's work assists the Minister in exercising responsibility for the Service.

The IG monitors CSIS for compliance with operational policies, and issues a yearly certificate indicating the degree of satisfaction with the Director's Annual Report on CSIS activities that is provided to the Minister of Public Safety under section 33 of the *CSIS Act*. An unclassified version of the IG's annual certificate is available on the Office of the Inspector General's web page, via the Public Safety Canada website.

CSIS Internal Audit Branch / Disclosure of Wrongdoing and Reprisal Protection

The Internal Audit function is headed by the Chief Audit Executive (CAE), who reports to the CSIS Director and to an external Audit Committee. The CAE provides the Director, Senior Management and the Audit Committee with independent, objective advice, guidance and assurance on the Service's risk management practices, management control frameworks, and governance processes. The CAE is also the Senior Officer for Disclosure of Wrongdoing.

In 2010-2011, the Service implemented an 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.

With respect to Internal Audit, the professional standards of the Internal Audit function were acknowledged in 2010-2011. First, Treasury Board rated the function as "Strong" during its annual Management Accountability Framework assessment. Second, two self-assessments addressing the requirements of the Institute of Internal Auditors and the Office of the Comptroller General were externally validated. As a result, the Internal Audit function can confirm that it complies with internationally recognized auditing standards.

The CSIS Audit Committee continued to bring about improvements to the delivery of assurance services. The Audit Committee focused on examining CSIS activities and performance in the five key areas in the Committee's mandate, namely risk management; management control framework; financial reporting; values and ethics; and the internal audit function. The Audit Committee continued to contribute to the independence and stature of the Internal Audit function by maintaining high standards in their review of work performed by the function. The Audit Committee also rigorously monitored the implementation of management action plans following internal audit reports.

Over the past year, CSIS demonstrated that it is an organization willing to listen to advice from a variety of sources and to create action plans accordingly. The Internal Audit function remains committed to supporting CSIS and improving its operations by maintaining a disciplined approach to assessing and improving the effectiveness of the Service's risk management, control and governance processes.

Access to Information and Privacy

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 *Privacy Act*. The CSIS ATIP Coordinator has the delegated authority from the Minister of Public Safety Canada to exercise and perform the duties of the Minister as head of the institution.

In 2010-2011, the ATIP Unit continued to conduct awareness sessions for all new CSIS employees. Briefing sessions were also given to managers and other specialized functional areas. Thirteen sessions were given to 331 participants who were provided with an overview of the *Privacy Act* as well as the *Access to Information Act*, and a better understanding of their obligations and the process within CSIS.

The ATIP Coordinator liaises with the Treasury Board Secretariat, the Information and Privacy Commissioners and other government departments and agencies on behalf of CSIS. In addition, the ATIP Unit processes and responds to all *Privacy Act* and *Access to Information Act* requests made to CSIS.

The *Privacy Act* came into force on July 1, 1983. Under subsection 12(1) of the *Act,* Canadian citizens, permanent residents and individuals present in Canada have the right to access their personal information under the control of the Government of Canada. As with requests under the *Access to Information Act* , the right to obtain information under the *Privacy Act* is balanced against the legitimate need to protect sensitive material. The aim is to permit effective functioning of government while at the same time promoting transparency and accountability in government institutions.

During the 2010-2011 fiscal period, the CSIS ATIP Unit received a total of 398 requests under the *Privacy Act* (representing an increase of 32 per cent over the previous fiscal year) and 263 requests under the *Access to Information Act* (an increase of 69 per cent over the last reporting period).

The ATIP Unit strives to improve its administration of both *Acts*. Considerable effort was devoted to addressing all mandatory reporting requirements, resulting in a 'Strong' rating during the last round of the Management Assessment Framework exercise as it relates to capacity and governance.

LIBRARY AND ARCHIVES CANADA PRESERVATION CENTRE IN GATINEAU, QUÉBEC

History on File

The historical record of Canada is preserved by Library and Archives Canada (LAC). By law, all government institutions must transfer to LAC records of historical importance, and CSIS is no exception.

CSIS was created in 1984 and inherited the Cold War files of our predecessor, the RCMP Security Service. Over the years, CSIS has transferred thousands of those records to LAC. The first transfer occurred in 1989 when the Service sent over its files on suspected subversives, revolutionaries and the like.

(Continued on next page)

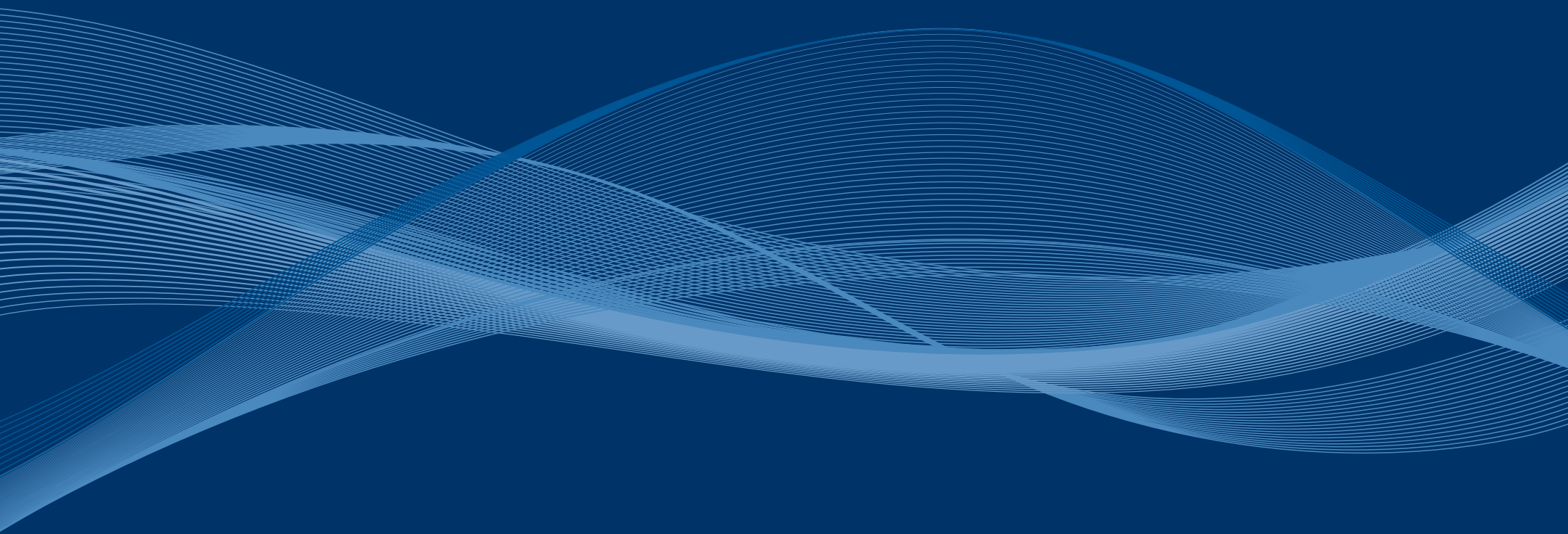
The security community recognizes that Cold War files have important cultural value and that if material can be unclassified, then it should be. This desire for transparency represents a significant attitudinal shift. The very existence of security dossiers on the Communist Party of Canada and similar organizations would never have been acknowledged a number of years ago. The default position was to protect information.

The approach today, however, is to release files of historical and cultural significance unless there are compelling security reasons not to. Accordingly, CSIS is working with LAC to ensure that as much material as possible can be made public. Our national narrative is contained in security documents from the Cold War, making them of legitimate interest not just to scholars and journalists but to all Canadians.

The disclosure process can be technical and time-consuming. Although LAC retains the documents, they still need to be vetted to make certain they do not contain information that holds current operational value. CSIS researchers will pore over hundreds and hundreds of old RCMP reports, laboriously separating information obtained using human sources from that obtained using technical intercepts such as wiretaps. The aim is to protect human sources while facilitating the disclosure of technical intercepts.

One of the privileges of working at CSIS is the opportunity to hold history in our hands. By working closely with the nation's archivists, we seek to give all Canadians the same opportunity.

TALKING TO CANADIANS



TALKING TO CANADIANS

Community engagement

Some people assume that a security service always needs to operate in the shadows, but that is an outdated assumption. It is true that CSIS deals in secrets but that doesn't mean we have to be a secret organization.

Canadians expect a certain transparency and openness from their institutions. CSIS cannot – and should not – seek special exemptions at every turn. Ordinary Canadians have a strong interest in issues of national

security, and CSIS, where possible, is trying to contribute to that public conversation.

We are, for example, increasingly active in what is called public "outreach", especially with respect to cultural communities. We are an enthusiastic partner of the Cross-Cultural Roundtable on Security (CCRS), an initiative championed by the Minister of Public Safety that seeks to demystify the security apparatus. The CCRS brings together security officials from several government agencies and departments and introduces them to members of ethno-cultural groups across Canada.

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

These events allow the Service to explain that our mandate is to protect all Canadians, including minority and immigrant communities. Because the Service has identified Islamist extremism as the most pressing threat to national security, many Muslim-Canadians understandably want to know what the implications are for them. Public outreach – in mosques, community halls and other places – affords the Service the opportunity to assure Muslim-Canadians that we see them as partners and allies.

CSIS itself is a remarkably diverse organization, becoming more so every year. Just as some cultural communities might worry that the security establishment harbours misperceptions about them, we at CSIS work hard to clear up misunderstandings about who we are. The multicultural character of Canada is reflected in our workforce, something that would perhaps not be widely known or appreciated were it not for our participation in public outreach.

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

Academic Outreach

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

This program allows CSIS access to leading thinkers and writers specializing in security related issues. 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, historians, psychologists – to identify new avenues of research.

Academic Outreach (AO) hosted a conference entitled "Matching Ambitions and Realities: What Future for Russia?" AO brought together a multi-disciplinary group of experts from a number of countries to imagine alternative scenarios for this former superpower as it tries to claim a leading role in a shifting world order, all the while grappling with the demands of political and economic modernization.

We also hosted an in-depth briefing on the socio-political and economic drivers in Yemen that are facilitating the expansion of Al Qaeda in the

Arabian Peninsula (AQAP). The presenter on Yemen had done extensive research in that country and was able to present unique insights into the tribal dynamics, political culture, sectarian tensions and socio-economic challenges confronting Yemen.

There is a significant interest on the part of experts to participate in activities sponsored by CSIS. Since 2008, CSIS's Academic Outreach unit has organized six international conferences, numerous seminars and workshops, and dozens of lunchtime presentations 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.

In 2010-2011, outside experts engaged CSIS staff on discussions covering a range of security and strategic issues, including: the security challenges confronting Arab states; China's evolving interest in the Arctic; the internal dynamics of the Iranian regime; technology transfers and the spread of nuclear weapons; Russia's changing role on the world stage; and the security dimensions of the global food system.

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 has helped CSIS adopt a more holistic approach when reviewing and assessing national and international issues of interest.

The Academic Outreach program has also enhanced partnerships with other government departments. Canada's Foreign Affairs and International Trade, Privy Council Office, Canadian Food Inspection Agency and the International Development Research Center have co-sponsored with CSIS some of the international conferences, providing an opportunity for members of the broader intelligence community across government to liaise and collaborate.

CONTACT US

National Headquarters

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

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

Media and Public Liaison Queries:

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

Regional Offices

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

Quebec City District	P.O. Box 10043, Station Sainte-Foy Quebec QC G1V 4C6 Tel. 418-529-8926
Ottawa Region	P.O. Box 9732, Station T Ottawa ON K1G 4G4 Tel. 613-998-1679 or 1-800-267-7685 toll-free (Ontario only)
Toronto Region	P.O. Box 760, Station A Toronto ON M5W 1G3 Tel. 416-865-1480
Prairie (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