Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

Public Report

2008 | 2009

Canada

© PUBLIC WORKS AND GOVERNMENT SERVICES CANADA 2009
Cat No. PS71-2009
ISBN 978-1-100-50624-1

Think recycling

This document is printed with environmentally friendly ink

FSC

Overview of the Canadian Security Intelligence Service

In 1984, the Government of Canada passed an Act of Parliament for the creation of a civilian security intelligence service. This legislation not only gave birth to the Canadian Security Intelligence Service (CSIS), it also clarified the differences between security intelligence activities and law-enforcement work, bringing to an end the 120-year interlocking of Canada's security intelligence service with the Royal Canadian Mounted Police (RCMP). CSIS came into existence on July 16, 1984, and marked its 25th year of service in July 2009.

The Service is at the forefront of Canada's national security establishment and as such, its programs are proactive and pre-emptive. Its role is to investigate and assess threats to Canada and its interests, analyse information and produce intelligence. CSIS then reports to and advises the Government of Canada, so as to protect the country and its citizens. Key threats include terrorism, espionage, foreign interference, the proliferation of weapons of mass destruction and cyber-tampering affecting critical infrastructure.

Table of Contents

OVERVIEW OF THE CANADIAN SECURITY INTELLIGENCE SERVICE 1

MESSAGE FROM THE DIRECTOR 4

CSIS OPERATIONAL ACTIVITIES IN 2008-09 7

- National Requirements for Security Intelligence 7
- The Threat Environment 8
  - Terrorism 8
  - Terrorist Financing 12
  - Espionage and Foreign Interference 13
  - Chemical, Biological, Radiological, Nuclear and Explosive Weapons 14
  - Cyber-Security 15

LEGAL ENVIRONMENT 16

SECURITY SCREENING PROGRAM 19

- Government Screening 20
- Foreign Screening 20
- Immigration Screening 20

DOMESTIC AND INTERNATIONAL COOPERATION 22

- Domestic Cooperation 23
- CSIS Intelligence Assessments Branch (IAB) 23
- Integrated Threat Assessment Centre (ITAC) 26
- Foreign Operations and Cooperation 27

INSIDE CSIS 30

- Our People 30
- Employee Recruitment 31
- CSIS National Headquarters 33
- Regional Profile: Atlantic Region 34
- CSIS Financial Resources 35

REVIEW AND ACCOUNTABILITY 36

- The Inspector General (IG) 37
- The Security Intelligence Review Committee (SIRC) 37
- Access to Information and Privacy 38
- CSIS Internal Audit Branch 39
- Treasury Board Secretariat—Management and Accountability Framework 39
- Resource Planning 40

PUBLIC COMMUNICATIONS 41

- Academic Outreach 42
- CSIS 'Youth Day' 44
- Government of Canada's Workplace Charitable Campaign 44
- CSIS on the Internet 44
- CSIS—25 Years of Service 45

ANNEXES 62

- CSIS Organization 62
- Contact Us 64

Message from the Director

In June 2009, I began my term as the Director of CSIS just before the Service marked its 25th anniversary. I accepted this new challenge because I believe that CSIS is a critically important institution.

CSIS has been buffeted by enormous change over the past few years as it tracks and adapts to myriad global threats, a rapidly evolving legal landscape and a technological revolution that demands constant vigilance and ingenuity.

As described in the *Threat Environment* portion of this report, counter-terrorism remains the Service's major priority. The world is more dangerous and unpredictable in 2009 than when CSIS was born, in part because of the number of failed states and the strong emergence of violent and aggressive groups, such as Al Qaeda, that owe allegiance to no community. A global system in which many players are in a state of near-collapse or anarchy makes intelligence work infinitely challenging.

Canada remains at risk for the types of serious terrorist violence which other countries have experienced. Recent criminal convictions and sentencing of terrorists in Canada demonstrate this fact. We continue to be mentioned by Al Qaeda and its supporters as a legitimate target, and these threats have been directed not only within our borders, but to our interests abroad.

While terrorism garnered most of the headlines since the tragic 9/11 attacks in the United States, other threats also remain prevalent. Espionage against Canada or Canadian firms is an ongoing and substantial concern, as Canada - a leader on many industrial fronts - remains an attractive target for foreign governments. CSIS continues to investigate and advise the government about foreign intelligence agencies that attempt to conduct covert operations or collect information against Canada.

Interference in Canadian society by foreign governments or groups also remains a concern. This includes exerting undue pressure on Canadians to raise funds or support a terrorist cause in a foreign homeland, or monitoring dissent voiced by diaspora communities in Canada against their countries of origin.

Canada and other countries have also been the victims of cyber-related attacks against public and private sectors. Preventing these attacks, which are undertaken for criminal or political reasons, is a strong government priority. The proliferation of chemical, biological, radiological, nuclear and explosive weapons is also a disturbing reality for both Canada and our international allies. Financial intelligence is growing in importance as an element of all these investigations as a number of countries attempt to piece together the fragments of terrorism's elusive trail.

The Service's foreign role has continued to grow and develop, including our security intelligence support of Canadian Forces in Afghanistan and our work to help locate and free Canadians kidnapped abroad by terrorist groups. CSIS continues to find new and innovative ways to work with its partners to get the best intelligence possible for the Government of Canada.

In recent years, CSIS has most often been cited in the media with respect to court cases and decisions emanating from them. Various court rulings have resulted in CSIS having to both disclose and retain more information. In some cases, we have withdrawn especially sensitive information because of our commitment to our sources or allies, or because release would compromise operations.

As described in the *Legal Environment* portion of this report, this shift has been a major challenge for our organization as it involves policy changes, evolution in our training, and hard decisions on where to devote precious resources. It is critical that CSIS be able to protect sensitive information because an intelligence agency that reveals information about its tradecraft or sources can no longer operate credibly or effectively, but it is also clear that we must adapt to meet the requirements of the courts.

While CSIS is primarily known for its intelligence work, it is also a workplace with a strong internal culture and sense of pride. Our employees supported many charitable causes over the past year, including raising more than $293,000 nationally in support of the Government of Canada Workplace Charitable Campaign.

We also continue to recruit a new generation of professionals who have the knowledge, skills and dedication to work in the intelligence business.

Our workforce is more diverse than ever before, and those employees of different backgrounds and life experiences bring new ideas and make us stronger as an organization. I am enormously impressed and gratified that we continue to attract high-calibre employees, often from other careers. We work hard to attract good people.

In 2008, CSIS also launched its Academic Outreach Program to promote a dialogue with experts from a variety of disciplines, academic institutions and think tanks in Canada and abroad. This new program is building important links that are helping to make CSIS an organization which is more broad-minded and aware.

The 2008-09 period also brought about a "greener" CSIS, as the Service created a Green Committee and launched a campaign to help create a more environmentally friendly workplace. The committee is helping to save energy, reduce the Service's carbon footprint and generate enthusiasm toward this important issue, particularly among younger employees who are demanding that their workplace respect the environment and reflect their values.

The positive changes charted out above contributed to CSIS being recognized as one of Canada's top 100 employers and one of the National Capital Region's top 25 employers in the annual competition sponsored by Mediacorp Canada Inc., a specialty publisher of employment-related periodicals.

Over the past 25 years, CSIS has accomplished a great deal. We celebrate our Silver Anniversary a little older, a great deal wiser, and proud of how we have come together to protect the security of Canada. Since becoming Director, I have noticed a special esprit de corps and sense of purpose at CSIS.

As part of the Service's ongoing commitment to public accountability, we welcome the tabling in the House of Commons of this 18th annual CSIS Public Report, which provides the Service with an opportunity to report on its priorities, activities and corporate issues for the 2008-09 fiscal year.

Richard B. Fadden
Director
Canadian Security Intelligence Service

CSIS Operational Activities 2008-2009

National Requirements for Security Intelligence

The Minister of Public Safety issues 'National Requirements for Security Intelligence' which contain general direction from government regarding where CSIS should focus its investigative efforts, as well as guidance on the Service's collection, analysis and advisory responsibilities.

Today's complex threat environment is increasingly international and transnational in nature, and intelligence collection remains key in countering threats to the security of Canada posed by states, terrorist groups, foreign intelligence agencies, or other individuals or entities. Consistent with the government's priorities, CSIS continues to investigate threats to the security of Canada, both domestically and abroad, and advise the Government of Canada in accordance with those priorities.

CSIS continues to refine the process of identifying rapidly evolving security intelligence requirements. Working in close cooperation with a range of Canadian officials and departments, the Service strives to constantly improve the collection of security intelligence to ensure that analysis and advice provided to the Government of Canada are accurate, timely and effective. However, this has become an increasingly complex endeavour as the issues impacting national security and domestic and foreign policy are becoming more intricately linked to international developments. Furthermore, many of those issues have spread into non-traditional areas, thus requiring broader and more interactive cross-government specializations and consultations.

The Threat Environment

Terrorism

Terrorism remains a real threat to the safety and security of Canadians, both within Canada and internationally. While Canada has remained free of major terrorist incidents over the past two decades and no significant acts of terrorism originated from this country in 2008-2009, this is not an indication that Canada is immune from the threat which many other countries have experienced with tragic consequences. Some incidents did occur domestically, such as the multiple bomb attacks against the EnCana gas pipelines and wellheads in northern British Columbia, but such acts were noteworthy for their rare nature.

However, recent criminal convictions of individuals in Canadian courts on terrorism charges have underscored the reality of terrorist activity within our borders. The conviction of several individuals involved in the 2006 bombing plot in Toronto and the Momin Khawaja case are prime examples of Canadians willing to carry out or assist in violent acts supporting an extremist ideology. These cases have also demonstrated the ability of CSIS and law enforcement to work within the framework of existing legislation to investigate and prosecute these complex offenses.

These investigations have also exemplified the transnational elements of international terrorism and the need for an equally international response to counter it. It is important to understand the extent to which the security of the international community depends upon mutual vigilance and assistance. Through active support of the international community in counter-terrorism efforts, CSIS ensures the reciprocal cooperation of allied nations in the interests of the security of Canada.

CSIS also continues to work closely with the various communities within Canada to ensure that conflicts occurring outside of our borders do not spill over into our own local communities, where some individuals may be pressured to support a terrorist cause financially or logistically, while others may be persistently targeted for recruitment by extremist groups.

Investigating possible terrorist threats to Canada and Canadians - both domestically and abroad - remained the primary (but not exclusive) focus of the Service's operational activities in 2008-09. The threat from Islamist extremism continued to be the priority concern of most of the international community, including Canada. The greatest international terrorist threat to Canada and Canadian interests continues to emanate from Al Qaeda and its affiliates such as Al Qaeda in the Islamic Maghreb (AQIM). Al Qaeda has demonstrated a capability for conducting mass-casualty attacks using a variety of methods. Moreover, Al Qaeda is directly involved with the wars in Afghanistan and Iraq, and supports Islamist extremists in other areas, including the Maghreb, Somalia, and Yemen.

Canada remains a target for the types of serious terrorist violence which other countries have recently experienced. Canadians also run the risk of being specifically targeted while working or travelling abroad, or simply having the misfortune of being in the 'wrong place at the wrong time'. For example, in 2008-09, several Canadians were kidnapped in Somalia, Niger, Afghanistan and Pakistan by militant groups. In some cases, the groups believed to be responsible were affiliated with, or inspired by, Al Qaeda. Elsewhere, in Algeria, a bus belonging to a Canadian oil company was targeted, while attacks were also carried out near facilities belonging to the Canadian company Nexen in Yemen.

While there were no significant attacks against the Western world in 2008-09 outside of current conflict zones, citizens of countries such as Afghanistan, Colombia, India, Iraq, Pakistan, Somalia, Sri Lanka, Yemen and several other regions were killed or wounded in terrorist attacks. Several terrorist incidents in 2008-09 point to an increase in the use of less sophisticated methods for such attacks. For example, the 2008 terrorist attacks in Mumbai, India, by Pakistani extremists were relatively low-level operations using guns and grenades, rather than major explosives. However, despite the methods used by the extremists, the terrorist campaign in Mumbai

lasted several days before the perpetrators were killed by Indian security forces and had caused 179 deaths and over 300 casualties. The targets chosen - hotels, train stations and cultural centres busy with both locals and foreign tourists - indicate that government, military and law enforcement officials are not the only groups targeted by terrorists. Extremist websites immediately touted the Mumbai attacks as a model for others to follow.

Somalia, already a failed state under any definition, became a magnet for international terrorists in 2008-09. Radical ideologues called upon "true believers" to travel to engage in jihad in the country or support the fight in other ways. The withdrawal of Ethiopian troops from Somalia was interpreted as a great victory for the Islamist extremists, who are now endeavouring to create a Taliban-like state in the region.

The lack of state infrastructures also contributed to a rise in piracy in the Red Sea and Indian Ocean, activities largely driven by Somali youths. The impact on Canada was felt both by merchant ships and crews, and by Canadian Forces' ships contributing to anti-piracy efforts in those waters.

The 2008-09 period also saw a further deterioration in the situation in Pakistan. Islamist extremists continued their campaign to increase their presence in several of the country's states and regions. Despite several successful strikes on terrorists in Pakistan and along the Pakistani-Afghan border, militants along the border continued to carry out attacks against international forces and civilians in both countries. The governments of Pakistan and Afghanistan have vowed to work more closely together to fight the insurgency by militants, which has severely affected both countries, by rooting out insurgents and increasing border patrols and security in the mountainous border regions.

In the Middle East and North Africa regions, violence increased in the latter stages of 2008 and early 2009, with bombings and assassinations again on the upswing. The situation in Iraq, while appearing to stabilize somewhat during this period, remains tenuous, while Yemen also saw an increase in attacks linked to an Al Qaeda-affiliated group and the rekindling of a long-standing civil conflict in the north. Additionally, the rise of Al Qaeda-affiliated groups such as AQIM continues to pose a threat to domestic and foreign interests in North Africa.

CSIS's current counter-terrorism priority remains focussed on investigating the threat posed by individuals and groups inspired by the ideology of Al Qaeda. Despite the successes by intelligence and security forces in targeting and neutralizing much of the group's pre-9/11 leadership, the Al Qaeda threat has not disappeared. The Al Qaeda 'core' is still keen to attack

Western nations, including Canada, and there remain credible reports of Westerners travelling to the Afghanistan/Pakistan region to receive training and tasking for acts of terrorism.

The example set by violent jihadists and their ideological pronouncements continues to provide direction to Islamist extremists living in the West, including in Canada. Al Qaeda, its affiliated groups and individuals inspired by similar ideologies continue to spout propaganda of a conflict between the West and Islam and of attempts by the 'infidels' to overtake their lands. This strategy is used in an attempt to gain support and recruit impressionable and ill-informed followers. It also masks the true nature of their extremist objectives and grossly misrepresents the many people worldwide who follow the actual religion of Islam.

Events in recent years have emphasized the impact of shifting demographics, particularly in Europe. Incidents and conflict between elements of Islamic and non-Islamic communities have been on the rise. Extensive riots in the suburbs of Paris and similar inter-community conflicts in Australia and the United Kingdom underscore the need for governments to anticipate and counter potentially disruptive and violent conflicts. To some extent, these tensions have also hardened opinions and political positions in a number of countries.

The development of what has been referred to as "homegrown Islamist extremism", a threat which refers to the indoctrination and radicalization of young Canadians into the violent ideology espoused and inspired by Al Qaeda, also continued to be a concern in 2008-09. While demographically small, Canada remains home to certain individuals and groups that support the use of violence to achieve political or ideological goals. These individuals and groups work outside the legitimate political and democratic system.

Furthermore, the Internet continues to be a popular tool used by those who espouse extremist views. It remains a key component for planning, organizing, and executing terrorist activities, as well as in recruiting participants and disseminating propaganda. CSIS is aware that certain websites based in Canada continued to support or incite terrorist violence in 2008-09. CSIS continued to develop its capacities to investigate and understand how terrorists use the Internet to support their ideology and plan their objectives.

CSIS has been working closely with partners around the world and across Canada to identify and adopt best practices used in various counter-radicalization programs implemented in recent years. In some countries such as the United Kingdom, the counter-radicalization strategy includes a broad cross-government strategy designed to identify and address relevant concerns within all communities in the interest of national security.

Experience has also shown that conflicts abroad can be expected to influence affected immigrant communities residing in Canada. Some individuals within Canada's immigrant communities are also forced, through tactics of threats or intimidation, to support a violent cause abroad. Financial and other support sent to assist communities abroad can at times be diverted by those interested in advancing a conflict in their homeland, and funding intended for medicine and food is instead used to purchase arms and other equipment in support of violent conflict.

Others residing in Canada have returned to their country of origin and become actively engaged in the conflict. For example, in the case of Somalia, individuals involved in the conflict are motivated by the desire to establish a sharia state and may be drawn into global jihad circles, where they are subsequently recruited to carry out attacks against perceived enemies of Islam. Related developments in Australia, the United States, Europe and Africa support assessments that the regional conflict in Somalia and the region represents a direct threat to Canadian and international security.

Terrorist Financing

In 2008-09, CSIS continued to investigate and assess terrorist financing activities through its Financial Analysis Unit, which is mandated to conduct financial analysis on investigations linked not only to terrorism, but also to counter-proliferation and counter-intelligence concerns. CSIS continued to work 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), as well as with international counterparts, in order to share information and discuss issues of mutual concern in these areas.

Financial intelligence continues to grow in importance as an element in the interdiction and prevention of terrorist financing. As has been the case with so many other criminal activities, investigating and piecing together the financial trail has become an essential and international step in fighting terrorism.

Canadian legislation designates terrorist entities and freezes their assets. FINTRAC, under its legislated mandate, acts as the financial intelligence agency. The CRA reviews the charitable status of non-profit entities which may be implicated in terrorist-related funding. Increasing co-operation has become standard practice amongst government agencies, both domestically and internationally.

As the intelligence and law enforcement communities work to disrupt or shut down their activities, terrorist networks continue to seek new ways to raise, move and store the resources used in their recruitment, training and terror attacks. Some networks profit from sponsors and donors, and most also engage in traditional criminal activities such as theft, forgery and kidnapping to fund their extremist agendas.

Certain terrorist networks manage their financial operations much like multinational corporations, complete with bank accounts in different countries. Some make global investments in an effort to launder and legitimize their funds. However, governments such as Canada's are making it increasingly difficult for such groups to move funds through financial institutions as financial intelligence units become more vigilant. In March 2009, the Canadian government implemented amendments to the *Investment Canada Act* allowing for government review of foreign investments on national security grounds in order to counter this increased threat.

Espionage and Foreign Interference

While counter-terrorism continues to be a priority for CSIS in the post-9/11 world, CSIS also plays an active role in investigating and advising government on other threats such as espionage and interference in Canadian society by foreign intelligence services.

Canada remains an innovative leader in areas such as agriculture, biotechnology, communications, oil extraction from bituminous sands, mining, the aerospace industry and control systems engineering. Our country has a diverse population and a range of international, defence and economic partnerships. Canada is also a founding member of the North Atlantic Treaty Organization (NATO), and a signatory to a number of other multilateral and bilateral defence agreements. Such international connections, coupled with our close economic and trade relationships with the United States, give the country a unique position in the world.

These advantages attract business and investment opportunities to Canada. At the same time, precisely for these reasons, Canada is attractive to foreign intelligence agencies, and the threat of espionage against Canada and Canadian firms is an ongoing and substantial concern. In past years, foreign intelligence officers have been found operating clandestinely in Canada for the purpose of gathering intelligence. Some of their activities have also included source recruitment and handling, and monitoring or interference within certain immigrant communities in Canada, which certain governments perceive to be of concern to their own domestic security or political agendas.

Increasing global economic competition is leading many governments—both those representing traditionally "hostile" countries as well as ones considered "friendly" to Canada—to shift the focus of their intelligence collection from traditional political and military matters to the illicit acquisition of economic and technological information. Such information can include trade and pricing information, investment strategies, contract details, supplier lists, planning documents, research and development data, technical specifications and drawings, as well as computer databases.

While espionage can occur on Canadian territory, Canadian business people travelling abroad may also be vulnerable. A foreign government can operate more easily and with greater impunity within its own borders, making hotel rooms, restaurants, offices, and telecommunications systems vulnerable to espionage activities. Over time, these efforts damage Canadian society and undermine its competitive advantages. CSIS will continue to work with domestic partners and allied agencies to identify and address the threat that espionage poses to Canada's national interests.

Chemical, Biological, Radiological, Nuclear and Explosive Weapons

Chemical, biological, radiological, nuclear and explosive (CBRNE) weapons are an ongoing concern for the Service. In 2008-09, CSIS investigated and assessed the threat to Canada and Canadian interests posed by the proliferation of such weapons. Terrorist organizations such as Al Qaeda and affiliated groups continue to explore ways to obtain, manufacture and use such materials or weapons.

Information on how to use chemical, biological and radiological (CBR) weapons has become more readily available through open sources such as the Internet. While it remains very difficult for groups to use CBR materials in a large-scale attack without state assistance, even a small attack could have a deep psychological impact on society.

Many countries possess weapons of mass destruction, or have the capacity to produce them. Political or economic instability may increase the risk that such weapons or expertise may fall into the wrong hands, either inadvertently or by design. The International Atomic Energy Agency (IAEA) previously warned that as many as thirty countries could have the capacity to develop nuclear weapons in the next several decades. The proliferation of nuclear weapons, technology and expertise—particularly to less stable or conflict-ridden regions—presents a security threat to Canada and the wider international community.

It is very unlikely that a terrorist group could develop a nuclear weapon without state assistance, unless it obtained sufficient weapons-usable material, technology and expertise. No terrorist group is believed currently capable of independently producing the fissile material needed for a nuclear weapon. However, the possibility that a weapon of mass destruction could be obtained and improvised by a terrorist group cannot completely be discounted.

Cyber-Security

Media reporting during 2008-09 outlined the impacts of cyber-related attacks directed against the public and private sectors in a number of countries around the world, noting intrusions into government systems, suspected encroachment into national critical infrastructures, and the loss or theft of technological, financial, political, personal and other information.

Canada and other states have been the targets of such activity undertaken for criminal, political and other purposes. In March 2009, Canada's Public Safety Minister warned that cyber-warfare will be a "growing threat" in the foreseeable future. Canada's national critical infrastructure includes various technologies, physical and technical facilities, networks and other assets upon which the functions of government and the economy generally depend. Any compromise of these systems and networks could have serious ramifications for the health, security, safety and economic well-being of Canadians. The interconnection of sensitive systems through the Internet creates vulnerabilities which could be exploited by foreign governments, hackers, or terrorists/extremists.

Recent open-source reporting suggests that foreign intelligence services and others use the Internet to conduct espionage activities at little cost or risk when collecting classified, proprietary or sensitive information. Regardless of their agenda, hackers could use these computer-based networks to cause economic and other disruptions from a distance, using tools and techniques that are very difficult to detect.

In 2008-09, CSIS tracked developments in communications technologies, including the Internet, and their use by individuals and groups that pose a threat to Canada and its interests. These technologies and techniques are in a constant state of evolution, which complicates the efforts of security and intelligence services to counter the cyber-threats.

Legal Environment

CSIS's mandate is to collect intelligence and advise the government of potential threats to Canada's national security, to Canadians and to our country's interests as defined in the *CSIS Act*. The 1984 *CSIS Act* was intended for a purpose quite different and distinct from law enforcement. The Service has no powers of arrest, detention or capacity to compel cooperation. Our objective is to identify and investigate potential threats to Canada and Canadians before such threats come to fruition.

Over the past several years, various high-profile inquiries, court cases and rulings, and legal debates on national security cases have drawn attention to the use of intelligence information as evidence. The work of intelligence agencies worldwide in countering the current threat environment is under increased scrutiny. CSIS must stay on top of this ever-shifting legal landscape.

The investigative means taken on each case must be proportional to the gravity and imminence of the threat and - as per the *CSIS Act* - warrants must be approved internally by the CSIS Director, and subsequently by the Minister of Public Safety Canada, prior to applying to the Federal Court.

The power to authorize intrusive investigation techniques rests solely with the Federal Court of Canada. Before such an authorization can be made, CSIS must provide solid justification for the proposed use of these techniques in an affidavit. The objective of this judicial control is to strike the appropriate balance between Canada's security needs and the protection of individual rights and freedoms.

Increasingly, information collected by intelligence agencies is being used in court cases, leading to debates over disclosure obligations, evidentiary standards, information recording and retention practices and the need for intelligence personnel to testify before the courts. The challenge for intelligence organizations like CSIS is to strike the right balance between close cooperation with law-enforcement agencies, while maintaining the distinction of our respective mandates.

CSIS must continue to ensure the protection of its classified information, methodologies, information on its human sources and other CSIS assets such as the identification of its employees who work in a covert capacity - elements crucial to any current and future national security intelligence investigations.

This ever-evolving legal landscape and its impact on the policies and practices in national security investigations have been challenging not only for CSIS, but for many other intelligence agencies worldwide. The courts have made decisions in prosecutions, civil suits, judicial reviews and other litigation which have directly affected the Service, both in terms of disclosure obligations and existing policies and procedures.

These changes have provided CSIS the opportunity to reflect on our existing business practices and to improve how we gather and process information. It is clear that the legal environment has shifted, and that CSIS must and will adapt within the legal framework of its mandate to ensure that the work it does continues to respect Canada's rule of law.

Security Screening Program

As a vital component of Canada's national security framework, the CSIS Security Screening program in 2008-09 remained one of the most visible and primary operational responsibilities undertaken by the Service.

Government Screening

Under the Government Security Policy (GSP), federal employees, members of the Canadian Forces or persons under contract to a government department, who in the performance of their duties have access to classified government assets or information, are required to hold security clearances. The Service assists the originating department by providing security assessments to prevent anyone presenting a security concern from gaining access to sensitive government assets, locations or information.

Under the GSP, all departments have exclusive authority to grant or deny security clearances. It is under the authority of sections 13 and 15 of the *CSIS Act* that the Service may provide security assessments for all government departments and institutions. Since the RCMP conducts its own field investigations, CSIS only conducts indices checks in support of RCMP assessments.

Additionally, the Service's Government Screening Unit has several site access programs which provide assessments on individuals requiring access to major airports, ports and sensitive marine facilities, the Parliamentary Precinct, nuclear power facilities, as well as certain provincial and federal government departments. These programs enhance security and reduce the potential threat from terrorist groups and foreign governments that may seek to gain access to classified information or other assets, materials and sensitive sites.

Foreign Screening

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

Immigration Screening Program

While Canada's long and valued tradition of welcoming immigrants and visitors continues, maintaining the integrity of the immigration system is a vital part of strengthening Canada's security environment. The goal of CSIS's Immigration Screening Program is to prevent non-Canadians who pose security risks from entering or receiving status in Canada.

The program is founded on the security-related criteria contained in the *Immigration and Refugee Protection Act* (*IRPA*) and the *Citizenship Act*, and the Service provides advice to Citizenship and Immigration Canada (CIC) in order to assist the latter in its decisions, as well as to the Canada Border Services Agency (CBSA) via this program.

The program has the following essential screening components: visitors from countries of terrorist and espionage concern; refugee claimants in Canada; applicants for permanent residence from within Canada and abroad; and applicants for Canadian citizenship. The CSIS authority in this regard is provided under sections 14 and 15 of the *CSIS Act*.

Government Screening

Programs	Requests received *	
	2007–2008	*2008-2009*
Department of National Defence (DND)	8,800	15,300
Other departments/agencies	41,500	46,400
Parliamentary Precinct	1,100	1,000
Transport Canada (Marine & Airport programs)	43,100	36,600
Nuclear Facilities	9,200	11,100
Special Events Accreditation	1,300	16,300**
Free and Secure Trade (FAST)	10,700	6,400
Provinces	170	1,000
Site Access - Others	2,000	2,600
Foreign checks	800	700
TOTAL	118,670	137,400

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

Immigration Screening

Programs	Requests received *	
	2007-2008	*2008-2009*
Permanent Residents Within and Outside Canada	66,000	67,300
Front-end Screening	21,800	26,800
Refugee Determination Program	6,600	6,600
Citizenship Applications	190,000	169,500
Visitors Visa Vetting	111,300	58,900
TOTAL	395,700	329,100

* *Figures have been rounded*

Domestic and International Cooperation

Cooperation with domestic and foreign organizations is absolutely essential for any intelligence service to effectively carry out its mandate. Such cooperation allows CSIS to access a much broader range of timely information, which might otherwise not be available to Canada, and to better evaluate current and future threats to our country and its interests. CSIS works with a wide variety of partners in Canada and abroad.

Domestic Cooperation

CSIS is geographically dispersed across Canada, allowing the Service to closely cooperate with its many federal, provincial and municipal partners on security issues. The CSIS National Headquarters (NHQ) are located in Ottawa and CSIS also has Regional Offices in Halifax, Montreal, Ottawa, Toronto, Edmonton and Burnaby. Furthermore, CSIS has District Offices in St. John's, Fredericton, Quebec City, Niagara Falls, Windsor, Winnipeg, Regina, and Calgary.

Additionally, CSIS also 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 officers on potential 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 carrying out its duties, CSIS shares information with a wide variety of domestic partners. We work closely with many Canadian government departments and agencies to ensure the collective security of Canada. A key component of CSIS cooperation with its domestic partners is the production and dissemination of intelligence reports and assessments such as those drafted by the Service's Intelligence Assessments Branch (IAB) and the Integrated Threat Assessment Centre (ITAC), which is housed within CSIS Headquarters.

CSIS Intelligence Assessments Branch (IAB)

The mandate of the Service's Intelligence Assessments Branch (IAB) is to provide timely and focussed intelligence which meets the Government of Canada's stated requirements and priorities. Within the Service, IAB is responsible to prioritize and integrate intelligence requirements from all sources and to provide subject-matter expertise in support of collection programs and reporting.

IAB's responsibilities include:

- Actively engaging the Government of Canada to identify its intelligence needs and to review CSIS's performance in meeting those needs;
- Working closely with other core operational branches of the Service to prioritize and integrate intelligence requirements from all sources;
- Provide subject-matter expertise in support of CSIS operational and corporate programs;
- Produce assessments and reports which meet the strategic requirements of the Government of Canada's senior policy-makers and ensure the Service has a voice in the formulation of policy on security issues;
- Maintain open-source information services tailored to meet the operational and corporate requirements of the Service;
- Provide leadership and coordination in the delivery of the Foreign Intelligence Program;
- Deliver a number of other centralized CSIS corporate programs and services, namely:
  - the management of the Tactical Analyst Program;
  - the preparation of Security Intelligence Reports (SIRs) in support of Terrorist Listings and Threat and Risk Assessments (TRAs);
  - the management and coordination of the Service's involvement in NATO's Special Operational & Administrative programs;
  - the reception and dissemination of allied foreign agency intelligence reports.

IAB provides a range of products to the Government of Canada and certain allied foreign agencies. These publications provide concise analyses of threat-related issues and identify emerging trends or threats having national security implications for Canada. IAB analytical reports are generated by subject-matter experts from an extensive review of classified reporting, as well as open-source information. They are designed not only to explain general threat trends, but also to address more narrowly focussed issues based on particular client needs. Reports produced and disseminated by the CSIS IAB include:

- ***CSIS Intelligence Assessments (IAs):*** IAs are strategic assessments produced for the Government of Canada. Formerly known as CSIS Intelligence Briefs or CSIS Studies, IAs are relatively short, running from two to ten pages, depending on the issue. These assessments run the gamut of narrowly focussed analyses to broad threat-related trends, and are produced at the lowest classification level possible to ensure dissemination to clients with a need to know.
- ***CSIS Intelligence Reports (CIRs):*** CIRs provide non-assessed intelligence in response to established intelligence requirements. CIRs include intelligence collected within the mandates of Section 12 and Section 16 of the *CSIS Act*.
- ***Foreign Agency Reports (FARs):*** IAB's Allied Intelligence Unit (AIU) receives, reviews and processes foreign agency reports and disseminates them to appropriate Canadian government departments and to CSIS operational desks. The FAR product is the format used when sending such reporting to government departments other than to the Privy Council Office (PCO), the Department of Foreign Affairs and International Trade (DFAIT), the Communications Security Establishment (CSE) and DND.
- ***NSA Weekly Brief (NSAWB):*** This brief is produced weekly by the CSIS IAB for the National Security Advisor (NSA) and a limited group of other senior government officials. It is designed to provide the NSA with timely and relevant CSIS-specific information and assessments on events having a distinct incidence on national security.
- ***Threat and Risk Assessments (TRAs):*** TRAs are strategic, client-driven analyses which deal with long-term departmental security requirements as well as immediate threats, tactical intelligence-sharing or special events requirements. They are meant to assist clients in their risk management responsibilities.

- ***Perspectives:*** IAB produces this detailed internal assessment which is designed to situate CSIS intelligence collectors on significant developments and trends in key areas of concern. Some of the Perspectives produced in 2008-09 related to Afghanistan, Iran, Pakistan, Lebanon, Syria and the Horn of Africa. These are "all-source" products, combining classified and open-source information in a manageable format.

Integrated Threat Assessment Centre (ITAC)

ITAC was created under Canada's National Security Policy in April 2004, becoming operational on October 15th, 2004. It produces integrated, comprehensive and timely threat assessments for all levels of government with security responsibilities, as well as first-line responders such as law enforcement and, as appropriate, critical infrastructure stakeholders in the private sector.

As an essential component of the Government of Canada's efforts to build an integrated national security system, ITAC's threat assessments aim to provide Canada's security community with the information it needs to make decisions and take actions that contribute to the safety and security of all Canadians.

ITAC is a community-wide resource staffed by federal representatives from: CSIS, Public Safety Canada; RCMP; CBSA; DND; FINTRAC; CSE; DFAIT; PCO; Transport Canada; Correctional Service Canada; and, since September 2008, Public Works and Government Services Canada (PWGSC). The Ontario Provincial Police (OPP) and the Sûreté du Québec (SQ) also have members assigned to ITAC. These representatives bring the information and expertise of their respective organizations to the Centre.

The Director of CSIS is accountable for the performance of ITAC. To provide strategic direction to ITAC, the Director obtains guidance from both the National Security Advisor (NSA) to the Prime Minister and the ITAC Management Board, which consists of heads of departments and agencies contributing to ITAC.

In 2008-09, ITAC produced and disseminated over 400 threat assessments, while its unclassified 'Media Watch' report was provided to federal, provincial, law enforcement and private sector clients. ITAC also began producing integrated threat assessments supporting security efforts for the 2010 Winter Olympic and Paralympic Games. Internationally, ITAC contributes to an integrated intelligence community by cooperating with foreign integrated threat assessment centres, thus providing Canada and its partners with an international perspective on the threat posed by terrorism.

Foreign Operations and Cooperation

Increasingly, CSIS conducts security intelligence collection and operations in support of Canadians and Canada's interests in other countries, many considered to be high-risk areas.

In order to meet the Government of Canada's strategic intelligence requirements, CSIS continued to improve and increase its presence and collection efforts overseas in 2008-09. Of the Service's 2,910 employees, more than 50 CSIS Foreign Officers were located abroad in 2008-09 in approximately 30 countries, including in cities such as Washington, London and Paris. These collection efforts and the operational requirements linked to same are largely coordinated through the Service's International Region.

In 2008-09, CSIS also continued to provide security intelligence support to the Canadian Forces in Afghanistan. CSIS has had a presence in the country for the past few years and also continues to gather intelligence in the region in order to mitigate potential security threats to Canada which have a nexus to Afghanistan. Elsewhere on the international front, CSIS was also involved in providing timely intelligence as part of the Government of Canada's efforts to resolve the kidnappings of Canadian citizens abroad, many of which were carried out by groups affiliated with—or inspired by—Al Qaeda.

The Service also has information-sharing arrangements with many foreign organizations, and CSIS's increased activities abroad have led to an unprecedented level of cooperation with foreign agencies. These agreements give CSIS access to timely information linked to potential threats to Canada that have a nexus outside of our borders and allow the Service to obtain information which might otherwise not be available to this country.

In 2008-09, CSIS implemented three new foreign arrangements, and as of March 31st, 2009, had 278 foreign arrangements in 147 countries. CSIS uses appropriate caveats or instructions when sharing information with foreign agencies, and these caveats have been enhanced following recommendations made by the O'Connor Commission of Inquiry. The caveats applied by CSIS to accompanying information shared with foreign

agencies seek assurances that any Canadian citizen detained by a foreign government will be fairly treated within the accepted norms of international conventions. Those caveats also seek assurances that the detainee is accorded due process under law and afforded access to Canadian diplomatic personnel if requested.

Additionally, in 2007, CSIS and Canada's Department of Foreign Affairs and International Trade (DFAIT) implemented a new Memorandum of Understanding (MOU) which was drafted directly in response to recommendations made by the O'Connor Commission, the Inspector General and the Security Intelligence Review Committee. The MOU provides an improved framework for cooperation relating to consular cases involving Canadians detained abroad on security or terrorism-related cases. It also allows for CSIS— through its foreign counterparts—to try and facilitate consular access for DFAIT on behalf of the latter in rare instances where such access may initially be refused to DFAIT, which continues to be the lead in consular access issues for the Government of Canada.

In November 2008, the CSIS Deputy Director of Operations also issued a directive to formalize these important principles in the context of sharing information with agencies that have poor human rights records. Lastly, the Director of CSIS received specific Ministerial Direction from the Minister of Public Safety on information-sharing with foreign agencies.

CSIS shares information with foreign agencies on a number of issues. For security, privacy and confidentiality reasons, the Service does not publicly divulge details of that information nor identify the foreign agencies in question. CSIS must protect its foreign arrangements in order to keep those relationships viable and secure. Foreign agencies have an expectation that the information they provide to us will be kept confidential and CSIS has a similar expectation that any information we provide to foreign agencies will not be publicly divulged.

When CSIS enters into any type of arrangement, be it domestic or foreign, it becomes a signatory to the "third party rule" which prohibits an agency from divulging any information shared by another agency without the sender's express consent. This rule is designed to protect confidential sources of information and keep a liaison relationship secure. It is necessary to protect the identity of sources and to respect the conditions imposed on the sharing of information from foreign agencies to ensure the continued flow of such information.

The Service has one of the most stringent processes of all intelligence services worldwide with regards to implementing arrangements with foreign agencies. Strict standards and guidelines govern CSIS relationships with foreign entities and the sharing of intelligence. As per section 17(1)(b) of the *CSIS Act* and Ministerial Directives on 'Foreign Arrangements and Cooperation', prior to entering into such agreements, each of the Service's foreign arrangement requests must be reviewed by the Minister of Foreign Affairs and approved by the Minister of Public Safety. Furthermore, the Service has implemented internal policies, procedures and mechanisms to ensure sound management practices with regard to those foreign arrangements.

Also, the Security Intelligence Review Committee (SIRC) and the Inspector General (IG) carefully examine the Service's foreign arrangements and may review the exchange of information to ensure that the terms of the arrangements are upheld and that liaison and exchanges comply with Ministerial Directives, existing legislative requirements and CSIS policies.

In a prior review of CSIS foreign arrangements, SIRC found that the Service "had informed itself of the human rights situation in all the countries and agencies in question" and that CSIS "had proceeded cautiously with exchanges of information involving countries with questionable human rights records." SIRC had also observed "an improvement in the timely submission of (foreign) arrangement profiles" and that "all of the profiles reviewed by SIRC reflected the current security, human rights and political environment of the countries and agencies in question".

In 2008-09, CSIS continued to monitor and review various government and non-government human rights reports and assessments of all countries with which the Service has implemented ministerially approved foreign arrangements under s.17(1)(b) of the *CSIS Act*, an ongoing practice which is part of the Service's management and assessment of its foreign relationships.

INSIDE CSIS

Our People

In 2008-09, CSIS had 2,910 full-time equivalents (FTEs), marking the first time CSIS surpassed its previous high of 2,760 FTEs in 1992-93. The CSIS workforce consists of a wide range of individuals working in positions such as intelligence officers (IOs), analysts, surveillants, information management and technical specialists, security screening investigators, translators, interpreters, corporate management and administrative support staff.

The CSIS workforce continues to become more diverse and, in 2008-09, was also evenly split along gender lines. Sixty-five percent of our employees speak both of Canada's official languages. In addition, 44 percent of our IOs can speak a language other than English or French. Collectively, our employees speak about 103 languages.

In her 2007-08 annual certificate to the Minister, the IG stated that she "continues to be impressed by the calibre of (CSIS) employees, their dedication and their commitment to serving Canada and Canadians". The IG also noted that "the new generation of employees are very representative of the demographic and geographic diversity of Canada".

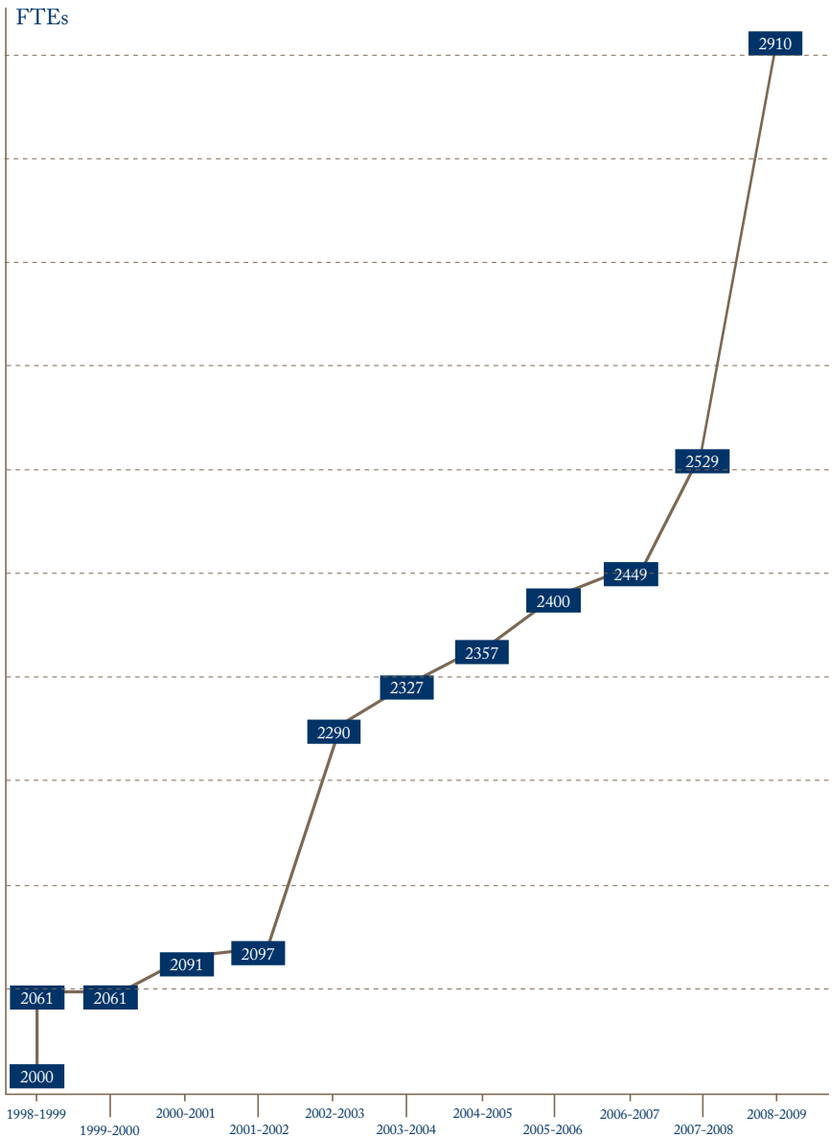
Employee Recruitment

In 2008, CSIS was recognized as one of Canada's top 100 employers and one of the National Capital Region's top 25 employers in the annual competition sponsored by Mediacorp Canada Inc., a specialty publisher of employment-related periodicals. The competition identifies the companies and organizations that lead their industries in offering exceptional working conditions and progressive human resources policies. The editors reviewed the recruitment histories of more than 75,000 employers from across Canada for the 2008 competition.

CSIS continues to make it a priority to recruit a new generation of professionals reflecting the current demographic realities of Canada. The Service is attracting more young Canadians to its ranks, people who have the knowledge, skills and initiative to work in the intelligence business, and are dedicated to protecting Canada's national security and its interests. For this purpose, CSIS participated in 70 career fairs, provided 98 information briefings on intelligence officer positions and participated in nine employee recruitment sessions held at various receptions and cultural events in 2008-09.

CSIS Workforce 2008-09

No. of FTEs	2910
Average age of CSIS employees	41
% of bilingual employees (English and French)	65%
% of IOs who speak a language other than English or French	44%
% of women	49%



CSIS National Headquarters

The Service's National Headquarters (NHQ) is located in Ottawa, Ontario. In 2008-09, ground preparations began for the construction of a five-storey tower expansion to the CSIS NHQ building. While the CSIS NHQ is a fairly recent construction (1995), factors such as the increase in personnel, the addition of new security programs such as the ITAC, enhancements to the Service's foreign collection program and new technical equipment have created space issues at NHQ.

CSIS, in partnership with Public Works and Government Services Canada (PWGSC), has been planning the NHQ expansion program (known as 'Phase III') for approximately five years to solve accommodation problems. CSIS received the 'Effective Project Approval' on October 18, 2007, from Treasury Board Secretariat (TBS), finalizing the funding to proceed with the 'Phase III' initiative. The Government of Canada awarded the Phase III construction contract to EllisDon Corporation for the CSIS building addition, as a Major Crown Project, at a value of just under $69.5 million. Estimated completion of the tower is forecast for late 2011.

Photo : Mark McNulty, Phase III

Regional Profile: Atlantic Region

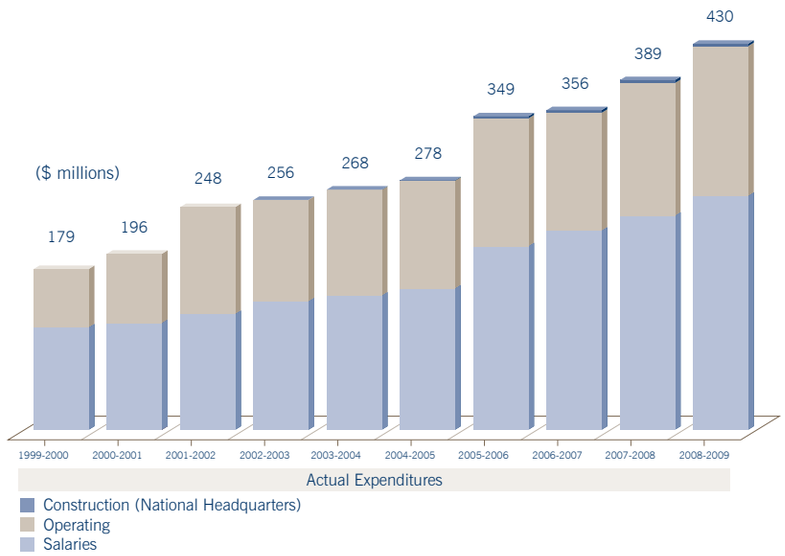
- Atlantic Region is the smallest of CSIS's Regional operations. Its main office is located in downtown Halifax, Nova Scotia, with District offices in Fredericton, New Brunswick and St. John's, Newfoundland and Labrador.
- The geographic area of responsibility includes the four Atlantic Provinces: New Brunswick, Nova Scotia, Newfoundland and Labrador and Prince Edward Island. Canada's Maritime region has a long coast line with a number of significant international sea ports (both for cruise and cargo ships) and international airports, which provide operational challenges and opportunities.
- In May 2008, CSIS's Atlantic Region was restructured to strengthen its support to CSIS operations and its administrative capacity.
- In 2008-09, over 60% of all Atlantic Region operational activities focussed on counter-terrorism issues.
- The Service's Atlantic Region has a vibrant liaison program with the federal, provincial, municipal and private-sector departments and agencies in the area. These relationships extend from working-level contacts and cooperation to those at senior executive levels.
- Canada's Atlantic provinces are well-known for their strong post-secondary programs. In 2008-09, CSIS's Atlantic Region Human Resources officers took full advantage of this situation by actively participating in nine career fairs 2008-09. Additionally, they held two employee recruitment information sessions during this period to inform potential new recruits from diverse cultural backgrounds of the rewarding work and career opportunities offered at CSIS.
- Additionally, Atlantic Region representatives maintain a regular and constructive dialogue with the various ethno-cultural communities to inform them about the Service's role and mandate, dispel misconceptions they may have about CSIS and continue building bridges and forging strong relationships with those various communities.

CSIS Financial Resources

CSIS's final expenditures for 2008-09 totalled $430 million.

The Service's financial resources have increased since 2001-02, partly as a result of new funding for public security and anti-terrorism initiatives allocated in the December 2001 Federal Budget. In addition, CSIS received resources for its part in the Government of Canada's Marine Security Initiatives and the Canada–U.S. Smart Borders Declaration. In the past few years, additional funding was also provided to augment the Service's foreign collection capabilities, to administer the ITAC, and to help CSIS maintain its operational capacity and expand its National Headquarters.

Finally, incremental funding was approved for the planning and operations related to policing and security of the 2010 Winter Olympic and Paralympic games in Vancouver. Over three fiscal years, CSIS will receive a total of $11 million for funding in support of the Service's role and requirements related to the security of the Games.



Construction costs shown are for the expansion of the CSIS NHQ. Costs incurred from fiscal year 2002-03 to 2006-07 represent expenditures associated with the project definition stage. In 2007-08 and 2008-09, costs incurred were mainly attributable to the building's site preparation. The contract for the construction of Phase III was awarded in March 2009.

Review and Accountability

The CSIS Director is accountable to the Minister of Public Safety, who is responsible for providing Ministerial Direction to the CSIS Director on the policies, operations and management of the Service. CSIS is bound by the legislation spelled out in the *CSIS Act*. Certain CSIS activities are also reviewed by the Office of the Auditor General and the Canadian Human Rights Commission. The operational activities of the Service are reviewed on an ongoing basis by two review bodies established by Parliament in the *CSIS Act* - the Inspector General (IG) and the Security Intelligence Review Committee (SIRC).

The Inspector General (IG)

The mandate of the Inspector General for CSIS is to support the Minister of Public Safety in exercising ministerial responsibility for the Service. The IG is responsible for monitoring CSIS compliance with operational policies, reviewing its operational activities, and reviewing and issuing a certificate indicating the degree of satisfaction with the Director's Annual Report on CSIS activities, which is provided to the Minister of Public Safety under section 33 of the *CSIS Act*.

The Security Intelligence Review Committee (SIRC)

The Security Intelligence Review Committee was established in 1984 as an independent, external review body which reports to the Parliament of Canada on Service operations. Each year, SIRC undertakes a series of reviews of operations and activities conducted by CSIS, and publishes an annual report that is tabled by the Minister in Parliament and available to the public. The SIRC Annual Report provides an unclassified overview of its various studies of CSIS issues conducted during the fiscal year. Following each review, SIRC provides its observations and recommendations pertaining to the CSIS policies, programs or operations under review. While CSIS is not required by law to implement SIRC recommendations, the Service always gives them careful consideration. In fact, many of SIRC's recommendations are implemented by CSIS.

The Service's interactions with SIRC (and with the IG) are primarily managed by the CSIS External Review and Liaison (ER&L) Unit. This includes coordinating requests or questions relating to reviews, and providing advice to CSIS employees during reviews or briefings. Additionally, ER&L serves as the primary liaison point regarding complaints against CSIS filed with SIRC under sections 41 and 42 of the *CSIS Act*. The ER&L Unit works with all branches of the Service to coordinate the Service's response to the complaint.

The combined efforts of SIRC and the IG for CSIS over the years have made the Service a more effective and professional organization. The Service remains committed to working with its review bodies and to maintaining a productive and professional relationship with them.

Access to Information and Privacy

The Access to Information and Privacy (ATIP) Unit is located within the Service's Secretariat Branch. The ATIP Unit currently has an establishment of 15 employees to fulfill the Service's obligations under the *Access to Information* and *Privacy Acts*. The CSIS ATIP Coordinator has the delegated authority from the Minister of Public Safety Canada to promote the program, enforce compliance with legislation, regulations and government policy, and create departmental direction, including standards and employee training in all matters relating to the *Access to Information Act* and *Privacy Act* within CSIS.

In 2008-09, the ATIP Unit continued to conduct ATIP awareness sessions for all new CSIS employees. A number of briefing sessions were also given to managers and other specialized functional areas. Twelve sessions were given to 240 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. This right of access is balanced against the legitimate need to protect sensitive information and to permit effective functioning of government while promoting transparency and accountability in government institutions.

In addition, the *Act* protects an individual's privacy by preventing others from accessing his or her personal information, and speaks to the collection, retention, accuracy, disposal, use and disclosure of personal information.

During the 2008-09 fiscal period, the CSIS ATIP Unit received a total of 390 requests under the *Privacy Act*. The CSIS ATIP Unit also received 153 new access to information requests under the *Access to Information Act* during this period.

CSIS Internal Audit Branch

The Internal Audit function of CSIS advises the Director and senior managers on the Service's risk-management strategies and practices, management control frameworks, systems and governance processes.

In 2008, the CSIS Director established an independent Audit Committee comprised of three external members jointly selected with the Comptroller General and of four ex-officio members from within CSIS. The Director of CSIS also designated an external member as Chair of the CSIS Audit Committee. Pursuant to the Policy on Internal Audit issued by the Treasury Board Secretariat, a new Audit Committee Charter, an Internal Audit Charter and an Internal Audit Policy were approved by the Director.

The Internal Audit Branch developed a 'Risk-Based Audit Plan' covering the period of 2008-2011 to meet the Service's requirements relating to Treasury Board Secretariat's policy on internal audits with the federal government and the implications of the *Federal Accountability Act*. The three-year plan encompassed all CSIS branches and programs, and demonstrated a strong and credible audit regime addressing effective risk management, sound resource stewardship and good governance. The plan also enabled the Internal Audit Branch to ensure the coordination of assurance services with the Office of the Auditor General, the Office of the Comptroller General, SIRC and the IG.

Treasury Board Secretariat's 'Management Accountability Framework'

To strengthen accountability across the Federal Public Service, the Treasury Board Secretariat (TBS) developed a tool entitled the *Management Accountability Framework (MAF)*. This provides all public service managers, including those at CSIS, with a list of management expectations and suggests ways for federal departments and agencies to move forward with—and measure the progress of—its business operations. Treasury Board Secretariat also conducts an annual assessment of management capacity and good practices across government through its MAF program.

The MAF Round VI (2008-2009) observations of CSIS were very positive and a marked improvement from the previous round. TBS acknowledged that CSIS has undergone an increase in the size of the organization and the scope of its activities, and that, during this period of expansion and change, the Service has invested in measures to strengthen corporate management capacity. TBS also recognized the Service's management improvement efforts in a number of areas since the previous fiscal year, including Corporate Management Structure, Corporate Risk Management, Information Technology Management, Internal Audit and—in particular—significant work to strengthen its 'Corporate Performance Framework'. In its 2008-2009 assessment, TBS also recommended that CSIS review how it develops and disseminates audit assessments to managers. TBS also recommended that CSIS clarify its system of governance used to evaluate those programs.

Resource Planning

To strengthen its corporate management, CSIS created a new Resource Planning Branch. In 2008-09, the Service made progress in developing a new multi-year corporate planning process that integrates human and financial resources with equipment, infrastructure and operational requirements.

As highlighted in its MAF assessment, the Service also undertook significant work to strengthen its Program Activity Architecture (effective April 2009) and to develop the supporting Performance Measurement Framework. In addition, the CSIS Risk Management Unit has also made strong progress in building a corporate risk-management program.

In 2009-2010, CSIS will further improve its management practices by continuing to implement integrated, multi-year corporate planning programs and processes and by furthering the Service's progress on corporate risk management.

Public Communications

In 2008, CSIS's public profile was higher than usual, with over 3,840 media reports referring to the Service. The majority of references to CSIS in the media were in news items pertaining to legal cases such as those linked to security certificates before the courts.

In most instances, CSIS cannot publicly confirm what is reported in the media nor refute any erroneous or misinformed allegations or criticisms levied against the Service in the public domain. However, where and when it can, CSIS does reach out to the public to keep Canadians informed within those parameters in order to explain the Service's role, mandate and organization. For example, in 2008-09, CSIS:

- responded to over 240 media queries;
- responded to more than 790 public calls;
- provided testimony by the Director or other high-level managers before various Parliamentary and Senate Committees;
- continued to distribute information through its Public Report, backgrounders and brochures;
- continued to provide updated information relating to CSIS on its public website.

Aside from its public and media communications program, the Service continues to participate in outreach initiatives so as to inform various communities about the role and mandate of CSIS, and to dispel some myths about who we are and what we do. In 2008-09, CSIS offered more than 40 corporate briefings to government, law-enforcement, private-sector and public audiences and participated in more than 80 community outreach events. CSIS also continued its efforts in this regard by providing briefings and presentations to:

- academic and ethno-cultural communities;
- Canadian business leaders;
- non-governmental organizations;
- universities.

CSIS also participated in regional events of the federal Cross-Cultural Roundtable on Security, in career fairs, employee recruiting events at universities and community festivals. The CSIS Director also participated in the Canadian Association for Security and Intelligence Studies (CASIS) Conference in October 2008, which was held in Ottawa, and delivered a keynote speech at the Global Futures Forum Conference in Vancouver in April 2008.

Academic Outreach

In September 2008, CSIS launched its Academic Outreach Program. The purpose of the program is to promote a dialogue with experts from a variety of disciplines working in academic institutions and think tanks in Canada and abroad. Government is confronted with an increasingly complex and unpredictable environment. CSIS is turning to experts in the field to provide it with the context, different perspectives and a longer-term view of the changes that may affect national security.

The program also allows CSIS to improve its analytical capacity and the quality of the assessments it prepares for government decision- and policy-makers. It also seeks a more interactive relationship with academia in order to share insights on issues and developments, and provide a better understanding of government priorities. During the eight months following the program's creation, there was significant interest on the part of experts to participate in activities sponsored by the CSIS program. These events included two international conferences, several seminars and roundtable discussions, and 'Lunchtime Theatre Presentations' at the Service's National Headquarters. Speakers from a number of both Canadian and international academic and research institutions have taken part in these exchanges.

The discussions have covered a range of issues, including: the political dynamics in Afghanistan; the prospects for security in Pakistan; stability of the Iranian regime and its regional ambitions; the proliferation of WMDs; the potential impact on China's economic development from its demographic change; and Canadian Arctic security and sovereignty.

As the Academic Outreach program develops, CSIS anticipates that exchanges with the academic and think-tank communities will assist the Service in asking the right questions and avoiding surprises. Such exchanges will also allow CSIS to take a more holistic approach when reviewing and assessing national and international issues of interest.

The Academic Outreach program has also solidified partnerships with other government departments. DFAIT, DND, PCO and Public Safety were co-sponsors along with CSIS of two international conferences on issues of mutual interest to several government stakeholders, which drew representatives of all departments and agencies from the intelligence community. Likewise, Academic Outreach presentations at the CSIS 'Lunchtime Theatre Series' presentations are open to members of the intelligence community.

Through the program, CSIS has also increased its support and participation in international outreach efforts which touch upon emerging issues of broad concern. The results of some of the Service's academic outreach activities are released on the CSIS website as part of the *World Watch: Expert Notes* series. We hope in this way to share the findings and stimulate debate about issues that interest all Canadians.

CSIS 'Youth Day'

In November 2008, CSIS hosted its 13th Annual 'Youth Day' at its NHQ, where 52 Grade 9 students who are children of Service employees participated in presentations and activities designed to provide them with a better insight as to what CSIS does, and the various types of work undertaken by its employees. The 'Youth Day' event is sponsored by the Learning Partnership, a non-profit organization of business people, educators, labour and community leaders committed to creating learning and career opportunities for young people. The event also shows participants how learned skills, training and education are critical to their future success.

CSIS Participation in the Government of Canada's Workplace Charitable Campaign

In 2008, CSIS also continued its strong support of the Government of Canada's Workplace Charitable Campaign (GCWCC), as Service employees in Ottawa contributed more than $222,500 to the 2008 GCWCC—well above its $175,000 target—while those in other CSIS Regions raised over $71,000 for the cause. Following the 2007 GCWCC campaign, for which CSIS was awarded the Chair's Cup in recognition of its overall campaign excellence, the Service was also recognized for its 2008 campaign. In May 2008, United Way/Centraide Ottawa honoured and celebrated those who demonstrate and encourage leadership, cultivate connections and exemplify engagement within our community. At the event, CSIS received the 2008 Community Builder Award for the 'Best GCWCC'.

CSIS on the Internet

The CSIS website (www.csis-scrs.gc.ca) continues to be a popular Internet destination for those seeking official information about the Service. The following chart provides approximate figures on the number of times various pages on the CSIS site were viewed in 2008-09:

*CSIS website 2008-09**

Item(s) viewed	Number of views
Website (total views of all pages)	6,340,723
Backgrounders	57,112
Integrated Threat Assessment Centre	94,649
Commentary	159,453
Perspectives	38,984
Public Report (all years)	57,000
Recruitment information and job postings	3,354,192

** Numbers are approximate and do not include views of graphics on the site.*

CSIS—25 Years of Service

On July 16th, 2009, CSIS marked its 25th anniversary. The Service - along with the national and international threat environment in which it operates - have undergone significant transitions during the past quarter century. The following is a retrospective outlining several key CSIS corporate facts and figures over its history to date, as well as high-profile national and international security incidents* which have occurred since the Service's inception:

1984

Bill C-9, which led to the creation of CSIS, comes into effect as the Service begins its work on July 16th. Ted Finn is the first CSIS Director. 80% of CSIS operational resources are committed to counter-intelligence investigations. The CSIS Headquarters are located in Ottawa's East Memorial Building on Wellington Street, but due to space limitations, CSIS HQ Branches are actually scattered throughout eight buildings around Ottawa. Major international security incidents include the bombing of the U.S. Embassy Annex in Beirut, Lebanon, killing 20 people. Indian Prime Minister Indira Ghandi is assassinated by her Sikh bodyguards.

1985

CSIS has 1,968 positions, most filled by former RCMP Security Service members and employees. In March, the Turkish Embassy in Ottawa is attacked by men claiming to be members of the Armenian Revolutionary Army. A Canadian security guard is shot to death during the attack. After bombing the embassy and taking hostages for a brief period, the men surrender to police. Less than a year into CSIS's existence, the Air India Flight 182 tragedy occurs on June 23rd. Among the 329 victims killed are 280 Canadians. At the time, it is the deadliest terrorist attack involving an aircraft. Elsewhere, four Palestinian Liberation Front terrorists seize the Italian cruise liner 'Achille Lauro' in the eastern Mediterranean Sea, taking more than 700 hostages and killing one U.S. passenger. Four gunmen belonging to the Abu Nidal Organization attack the El Al and Trans World Airlines airport ticket counters in Rome and Vienna, killing 16 people and injuring more than 100. In the U.S., John Walker Jr., a former warrant officer and communications specialist for the U.S. Navy, is convicted of spying for the Soviet Union.

1986

CSIS's workforce numbers 1,964 and remains 82% comprised of former RCMP Security Service members and employees. Of those, 131 employees return back to the law-enforcement work of the RCMP in accordance with a 'bridge-back' arrangement offered when CSIS was established in 1984. CSIS has a budget of just under $116 million. In April, two U.S. soldiers are killed and 79 American servicemen injured following a bomb attack on a nightclub in West Berlin, West Germany. Libyan terrorists claim responsibility.

1987

The Solicitor General of Canada tasks former Clerk of the Privy Council, Gordon Osbaldeston, to review certain concerns raised by the Security Intelligence Review Committee (SIRC) about the Service's structure and certain programs. Osbaldeston's subsequent report includes several recommendations, including changes to the CSIS Executive Committee, a new support infrastructure, and the elimination of the CSIS Counter-Subversion Branch. All of these recommendations are eventually implemented. In September, CSIS Director Ted Finn announces his resignation. Reid Morden is appointed as the new CSIS Director. The number of CSIS employees rises to approximately 2,153. Korean Airlines Flight 858, en route from Abu Dhabi to Bangkok, explodes and crashes into the Andaman Sea, killing all 155 passengers and crew after a bomb was planted on the aircraft by North Korean terrorists. Elsewhere, 11 people are killed and 66 injured following an IRA bomb attack at a Remembrance Day parade in Northern Ireland.

1988

Counter-intelligence investigations remain the operational priority for CSIS, but counter-terrorism requirements begin to increase as the worldwide number of terrorist incidents rises to a record high (at that time). CSIS has 2,319 employee positions. In December, Pan-Am Flight 103 is blown up over Lockerbie, Scotland, by a bomb placed onboard by Libyan terrorists in Frankfurt, West Germany. All 259 passengers and crew members are killed, while 11 people on the ground are killed by debris from the aircraft. Elsewhere, a U.S. Naval Defense Attaché is assassinated in Athens, Greece, by the Marxist terrorist group 'Revolutionary Organization 17 November' via a remote-controlled car bomb.

1989

CSIS marks its 5th anniversary. Cabinet approves the 'National Counter-Terrorism Plan'. CSIS's employee base remains at just over 2,300 and, for the first time, CSIS publicly advertises in newspapers for new recruits. The CSIS budget is approximately $165 million. In September, UTA Flight 772 explodes over the Sahara Desert in southern Niger during a flight from Brazzaville to Paris. All 170 persons aboard were killed. Six Libyans were later found guilty in absentia and sentenced to life imprisonment. In Bogota, Colombia, Avianca Airlines Flight 203 explodes shortly after takeoff, killing all 107 passengers and crew and three people on the ground. The Colombian Medellin drug cartel subsequently claims responsibility, stating it was targeting five suspected informants among the passengers onboard. Elsewhere, ten people are killed and 22 injured in an IRA bomb attack in Kent.

1990

As per the *CSIS Act*, which called for a comprehensive review of the provisions and operations of the *Act* to be undertaken after the Service's 5th anniversary, a report entitled *'In Flux But Not In Crisis'* is completed by a Special Committee of the House of Commons. The report, completed in September 1990, declares that CSIS and its legislation are essentially on course, but provides recommendations for improving certain areas. Canada's Solicitor General subsequently responds to these recommendations in a report entitled *'On Course'*, a study detailing the mandate and role of CSIS and Canada's national security requirements. Due to ongoing concerns with national and international terrorist threats and activities, CSIS continues to shift resources from its counter-intelligence program over to counter-terrorism priorities to meet increased demands. CSIS has 2,526 employees. A pipe bomb explodes on a beach in Tel Aviv, killing a Canadian tourist and wounding 20 other people. A series of car bombs in Northern Ireland attributed to the IRA kill seven people and injure 37 others.

1991

CSIS increases its workforce to 2,683 employees to meet increased operational and corporate requirements. Reid Morden announces his resignation as CSIS Director. Raymond Protti is subsequently appointed as the new CSIS Director. The fall of the Soviet Union, combined with the increased terrorist threats worldwide, dramatically shift the operational landscape. The Canadian Embassy in Lima, Peru, receives minor damage following a bomb attack attributed to the Sendero Luminoso (Shining Path) terrorist group. In May, a female member of the Liberation Tigers of Tamil Eelam (LTTE) assassinates Prime Minister Rajiv Gandhi and kills 16 others by detonating an explosive vest during an election rally in India.

1992

CSIS establishes a Requirements, Technology Transfer (RTT) program. CSIS's employee base reaches 2,729 employees. For the first time, counter-terrorism investigations and resources dedicated to same surpass those dedicated to counter-intelligence requirements. CSIS's budget is just over $197.5 million. The Israeli Embassy in Buenos Aires, Argentina, is leveled in a blast which kills 29 people and wounds 242 others. Hizballah claims responsibility for the attack. In April, the Iranian Embassy in Ottawa is attacked by a group of approximately 40 Iranian exiles linked to the Iraqi-backed Mujahedin-e Khalq (MEK) group, who storm the building carrying sticks, crowbars and mallets. While no one is seriously injured in the attack, the interior of the building is ransacked and suffers major damage. Elsewhere, eight people are killed in an IRA bomb attack near an army base in Omagh.

1993

CSIS resources dedicated to counter-terrorism reach 56%, compared to 44% in counter-intelligence. The CSIS workforce reaches 2,760 employees, its highest level since inception and a mark which would not be surpassed until 2009. The World Trade Center in New York City is badly damaged when a car bomb planted by Islamist terrorists explodes in an underground garage. The bomb kills six people and injures more than 1,000. In February, a firefight ensues at the compound of the religious cult group known as the 'Branch Davidians' in Waco, Texas, when U.S. ATF agents arrive to arrest the group's leader David Koresh on weapons charges. Four ATF agents and several of the Davidians are killed while many others are injured. After a lengthy armed standoff, self-proclaimed 'angel of God' Koresh triggers his apocalyptic plan by setting the compound ablaze as authorities move in. Koresh and his 76 followers, including several children, die in the blaze.

1994

CSIS marks its 10th anniversary in July. CSIS Director Raymond Protti announces his resignation. Ward Elcock is appointed as the new CSIS Director in what would become a 10-year tenure. Federal government cutbacks due to tough economic times affect all government departments and agencies, including CSIS, as the Service's employee base drops to 2,465. CIA Counter-Intelligence officer Aldrich Ames and his wife are arrested for providing highly classified information to the Soviet KGB and its successor organization, the Russian Foreign Intelligence Service (SVR). In his plea to the court, Ames admits to compromising "virtually all Soviet agents of the CIA and other American and foreign services" known to him and to providing the Russians with a "huge quantity of information on United States foreign, defense and security policies." Elsewhere, Jewish right-wing extremist and U.S. citizen Baruch Goldstein opens fire on Muslim worshippers at a mosque in the West Bank town of Hebron, killing 29 people and wounding 150 others.

1995

Eight years after the recommendation was first made in the Osbaldeston Report, CSIS opens its new National Headquarters (NHQ) building, merging its scattered Ottawa workforce from offices previously located in eight different buildings in the city's downtown core. CSIS's budget drops to just over $180.4 million and its workforce sits at 2,366 employees. CSIS releases its report entitled '*Finding the Balance*', which looks at internal security practices within CSIS, and provides the results of the review to SIRC. On April 19th, the Alfred P. Murrah Building in Oklahoma City is bombed, killing 168 people including several children from a daycare centre inside the premises. It is the deadliest act of terrorism within the U.S. prior to the September 11, 2001 attacks. Timothy James McVeigh, a U.S. Army veteran, is later convicted of the bombing. Elsewhere, 12 people are killed and 5,700 others injured in a sarin nerve gas attack on a crowded subway station in the centre of Tokyo. A similar attack occurs nearly simultaneously in the Yokohama subway system. The Aum Shinri-kyo cult is blamed for the attacks. A suicide bomber drives a vehicle into the Egyptian Embassy compound in Islamabad, Pakistan, killing 16 and injuring 60 others. Three militant Islamist groups claim responsibility.

1996

CSIS launches its public website and Service employees number 2,244. Based on CSIS investigations, Russian spies using pseudonyms Ian and Laurie Lambert are arrested in Canada and deported back to Russia in June. Earl Edwin Pitts, a former FBI special agent, is arrested at the FBI Academy in Quantico, Virginia, and charged with several offenses including spying for the Soviet Union and its successor, Russia. In Jerusalem, a suicide bomber blows up a bus, killing 26 people including three U.S. citizens, and injures some 80 others. In June, a fuel truck carrying a bomb explodes outside the U.S. military's Khobar Towers housing facility in Dhahran, Saudi Arabia, killing 19 U.S. military personnel and wounding 515 people, including 240 U.S. personnel. Several groups claim responsibility for the attack. In Paris, France, a bomb explodes on a subway train as it arrives at the Port Royal station, killing a Canadian, two French nationals and a Moroccan, and injuring 86 others. Algerian extremists are suspected in the attack.

1997

The CSIS budget drops to $165 million, matching the 1989 figure, while its employee base also decreases to 2,077. In noteworthy security incidents, Al-Gama'at al-Islamiyya gunmen shoot and kill 58 tourists and four Egyptians and wound 26 others at the Hatshepsut Temple in the Valley of the Kings near Luxor. Elsewhere, LTTE attacks on the Hilton Hotel and the Parliament in Colombo, Sri Lanka, kill 17 people and wound more than 100 others. In Chiapas, Mexico, 46 people are killed after being gunned down by a paramilitary group during a prayer session.

1998

Counter-terrorism resources now account for 60% of the Service's overall budget. CSIS publicly confirms that approximately 50 groups and 350 individuals are being investigated by CSIS under threats to Canada's national security as defined in the *CSIS Act*. CSIS's workforce drops to 2,000 employees, its lowest total since 1986. A bomb explodes at the U.S. Embassy in Nairobi, Kenya, killing 12 U.S. citizens, 32 foreign nationals and 247 Kenyan citizens. More than 5,000 others are injured. Simultaneously, a bomb detonates outside the U.S. Embassy in Dar es Salaam, Tanzania, killing 10 people and injuring 77 others. In September, the FBI arrests five Cuban intelligence officers (later dubbed the 'Cuban Five') in the U.S., who are charged and eventually convicted of espionage, conspiracy to commit murder, and other illegal activities in the U.S. on behalf of the Cuban government.

1999

CSIS Director Ward Elcock is reappointed to a second term as CSIS marks its 15th anniversary. CSIS's employee base rises slightly to 2,061. In February, the Turkish Embassy in Ottawa is again attacked as more than 300 Kurdish rioters pelt the building with Molotov cocktails and other projectiles. Other noteworthy events include the arrest of Ahmed Ressam, who is stopped while entering the United States from Canada with explosives hidden in the trunk of his car for what was eventually revealed to be a plot to bomb the Los Angeles International Airport. Elsewhere, seven Canadian pipeline workers are kidnapped in Ecuador. A pipe bomb explodes inside a bar in Uganda, killing five and injuring 35 others. Ugandan authorities blame the attack on the Allied Democratic Forces (ADF).

2000

The CSIS budget is increased to $179 million and its employee base remains at 2,061. Ressam's foiled attack against the Los Angeles International Airport is revealed to be one of several planned to be carried out by Al Qaeda throughout the world at the millennium, including planned attacks in Jordan and against the USS warship 'The Sullivans' in Yemen. All were thwarted. However, later in the year, a small dingy carrying explosives rams into the destroyer U.S.S. Cole in Aden, Yemen, killing 17 U.S. sailors and injuring 39 others. Al-Qaeda claims responsibility for the attack.

2001

CSIS employees total 2,091. On September 11th, Al Qaeda terrorists launch attacks against the World Trade Center and the Pentagon in the U.S., using four hijacked passenger aircrafts. Two of the aircraft strike the World Trade Center towers, while another crashes into the Pentagon. A fourth hijacked aircraft fails to reach its target, crashing into a field in Pennsylvania when passengers overtake the hijackers. 2,974 victims die in the terrorist attacks in the U.S., including 24 Canadians. The worst terrorist attack in history marks the beginning of a coordinated, international effort to counter Al Qaeda and its supporters in an effort to disrupt its ability to carry out further attacks, while security and intelligence budgets are increased in order to more effectively counter the threat. The Canadian government's new *Anti-Terrorism Act* is proclaimed in force, establishing specific terrorism offences in the Criminal Code. Also in this year, FBI agent Robert Hanssen is arrested and charged with spying for the Soviet KGB and its Russian successor for more than 20 years. Hanssen later pleads guilty to 15 espionage and conspiracy charges. Elsewhere, Abu Sayyaf guerrillas seize 13 tourists and three staff members at a resort on Palawan Island in the Philippines. Some of the hostages are later found dead while others are rescued. Hamas claims responsibility for a suicide bombing of a popular Israeli nightclub that causes over 140 casualties. Five gunmen attack the Indian Parliament in New Delhi, killing six people. Indian officials blame the Lashkar-e-Tayyiba group for the attack.

2002

CSIS creates the 'Counter-Proliferation' Branch to increase the focus and information coordination on threats from weapons of mass destruction and proliferation of same. The government's 'Regulations Establishing a List of Terrorist Entities', part of the *Anti-Terrorism Act*, comes into force. CSIS's budget stands at $248 million and the number of CSIS employees rises slightly to 2,097. Armed militants kidnap Wall Street Journal reporter Daniel Pearl in Karachi, Pakistan. Authorities later receive a videotape depicting Pearl's murder by his Islamist extremist captors. In Lima, Peru, a car bomb explodes at a shopping centre near the U.S. Embassy, killing nine people and injuring 32 others. Peruvian authorities suspect either the Shining Path or the Tupac Amaru Revolutionary Movement for the attack. In Bali, Indonesia, a car bomb explodes outside the Sari Club Discotheque, killing 202 people and wounding 300 more. Most of the casualties, including 88 of the deceased, are Australian tourists. Al Qaeda claims responsibility. In Moscow, Russia, 50 Chechen rebels seize the Palace of Culture Theatre, taking more than 800 hostages. Following a three-day siege, one Russian policeman and 99 hostages are killed, as are all of the rebels.

2003

CSIS positions total 2,290. In Bogota, Colombia, a car bomb explodes outside a night club, killing 32 people and wounding 160. Colombian officials suspect the Colombian Revolutionary Armed Forces (FARC) of committing the worst terrorist attack in the country in a decade. In Saudi Arabia, suicide bombers attack three residential compounds for foreign workers in Riyadh. Seven Saudis, two U.S. citizens, and one citizen each from the United Kingdom, Ireland and the Philippines are killed as a result of the attack. In May, a team of 12 suicide bombers attacks five targets in Casablanca, Morocco, killing 43 people and wounding 100 others. In August, a car bomb explodes outside the Marriott Hotel in Jakarta, Indonesia, killing 10 people and wounding 150 others. One Canadian is among the victims. The Jemaah Islamiah group, which had carried out the 2002 bombing in Bali, is suspected of carrying out the attack. In Riyadh, a suicide car bombing occurs in the Muhaya residential compound, which is occupied mainly by nationals of other Arab countries. Seventeen people are killed and 122 are wounded. In Istanbul, Turkey, two suicide truck bombs devastate the British HSBC Bank and the British Consulate General, killing 27 people and wounding at least 450.

2004

In May, Ward Elcock's tenure as CSIS Director ends after two terms, the maximum allowed under the *CSIS Act*. CSIS Deputy Director Dale Neufeld is appointed Director. In November, Jim Judd is announced as the new Director as Dale Neufeld retires after 34 years of service with the RCMP and CSIS. In January, the government announces the establishment of the O'Connor Commission to review the activities of Canadian officials in the case of Maher Arar. In March, Momin Khawaja is arrested in Ottawa and charged with offences under the *Anti-Terrorism Act* in conjunction with the arrests of eight individuals in the U.K. in relation to a terrorist plot. In April, the government publishes its National Security Policy. In Madrid, Spain, 191 people are killed and over 600 others wounded when ten bombs detonate on the train lines. The bombs are all detonated by cell phones left in backpacks. The Abu Hafs al-Masri Brigade claims responsibility on behalf of Al Qaeda. Elsewhere, a massive suicide attack against a Shiite holy shrine in Baghdad kills over 65 people and injures more than 320 others. At least 47 people are killed and 130 injured following an attack on a Shia Muslim parade in Quetta, Pakistan, as the Shia were observing Ashoura. In Iraq, suicide attackers detonate five car bombs simultaneously against police buildings during morning rush hour, killing 68 people and wounding up to 200 others. In Islamabad, Pakistan, a bomb explodes at a Shia mosque during Friday prayers, killing 30 people and injuring dozens of others. In September, Chechen rebels storm a school in Beslan, Russia, taking more than 1,100 people hostage, including almost 800 children. Over 334 hostages, including 186 children, are eventually killed. Hundreds more are reported wounded or missing. A group calling itself the Riyadus-Salikhin Reconnaissance and Sabotage Battalion of Chechen Martyrs claims responsibility.

2005

CSIS's employee base rises to 2,357 employees. In July, bombs explode on one double-decker bus and three London subway trains, killing 56 people and injuring over 700 others. Later in the same month, minor explosions occur in three other London subway stations and on a bus, but those latest bombs fail to fully detonate, precluding the casualties and devastation from the earlier attacks. Elsewhere, members of the Christian Peacemakers humanitarian group, including two Canadians, are kidnapped in Iraq. Seven people are killed and 40 are injured by a car bomb outside a hotel in southern Thailand.

2006

The Service has 2,400 employees and its 2006-07 budget is $356 million. In March, the government announces the creation of the Major Commission of Inquiry into Air India. The inquiry is tasked to review the 1985 Air India tragedy and issues relating to inter-agency cooperation and information-sharing linked terrorism investigations. CSIS also publicly confirms that, in a departure from its more traditional international role, it is conducting operations abroad, collecting security intelligence information in support of Canada and its interests. In other news, a man using the name Paul William Hampel is arrested at Montreal's Pierre Elliott Trudeau International Airport just prior to boarding a plane departing Canada. Hampel is charged with being a Russian SVR agent masquerading as a Canadian citizen. He is subsequently detained and deported under a Canadian government security certificate. In June, 18 individuals are arrested in Toronto and charged with plotting a variety of attacks against targets in Ontario. In July, a series of explosions rock commuter trains in Mumbai, India, killing 209 and wounding another 714. In August, a major anti-terrorist operation by British Police disrupts a bomb plot targeting multiple airplanes bound for the U.S. flying through London's Heathrow Airport. In September, an LTTE suicide bomber rams a truck packed with explosives into a convoy of buses carrying Sri Lankan Navy personnel returning home on leave, killing 92.

2007

The Service's staff component rises slightly to 2,449 employees. In March, the Taliban claim responsibility for the kidnapping of Italian journalist Daniele Mastrogiacomo, beheading his driver and killing his translator. Mastrogiacomo is later released in exchange for the release of five Taliban prisoners. In June, two planned terrorist attacks in the U.K. fail. A car loaded with explosives crashes into the main terminal of the Glasgow International Airport, causing minor injuries to five people and setting off a blaze, but fails to detonate. In London's West End, an attempt to set off two car bombs by suspected cell-phone triggers fails. Elsewhere, eight Spanish tourists and two Yemenis are killed while another 12 are wounded in a suicide bombing attack at the Queen of Sheba temple in Marib, Yemen.

2008

CSIS adds 80 positions and its employee base is now at 2,529, virtually equalling the number of staff it had in 1990. In Ottawa, Momin Khawaja is convicted of terrorism charges and sentenced to 10 ½ years in prison. Ten coordinated attacks consisting of shootings and bombings are carried out in India's financial capital of Mumbai, India, killing 179 people and wounding more than 300. Canadian CBC journalist Melissa Fung is kidnapped in Afghanistan. UN special envoy and retired Canadian diplomat Robert Fowler and Canadian diplomat Louis Guay, along with their driver, are kidnapped in Niger. The 'Al Qaeda in the Islamic Maghreb' (AQIM) later claims responsibility for the kidnapping. Canadian freelance journalist Amanda Lindhout is kidnapped in Somalia along with Australian photographer Nigel Brennan.

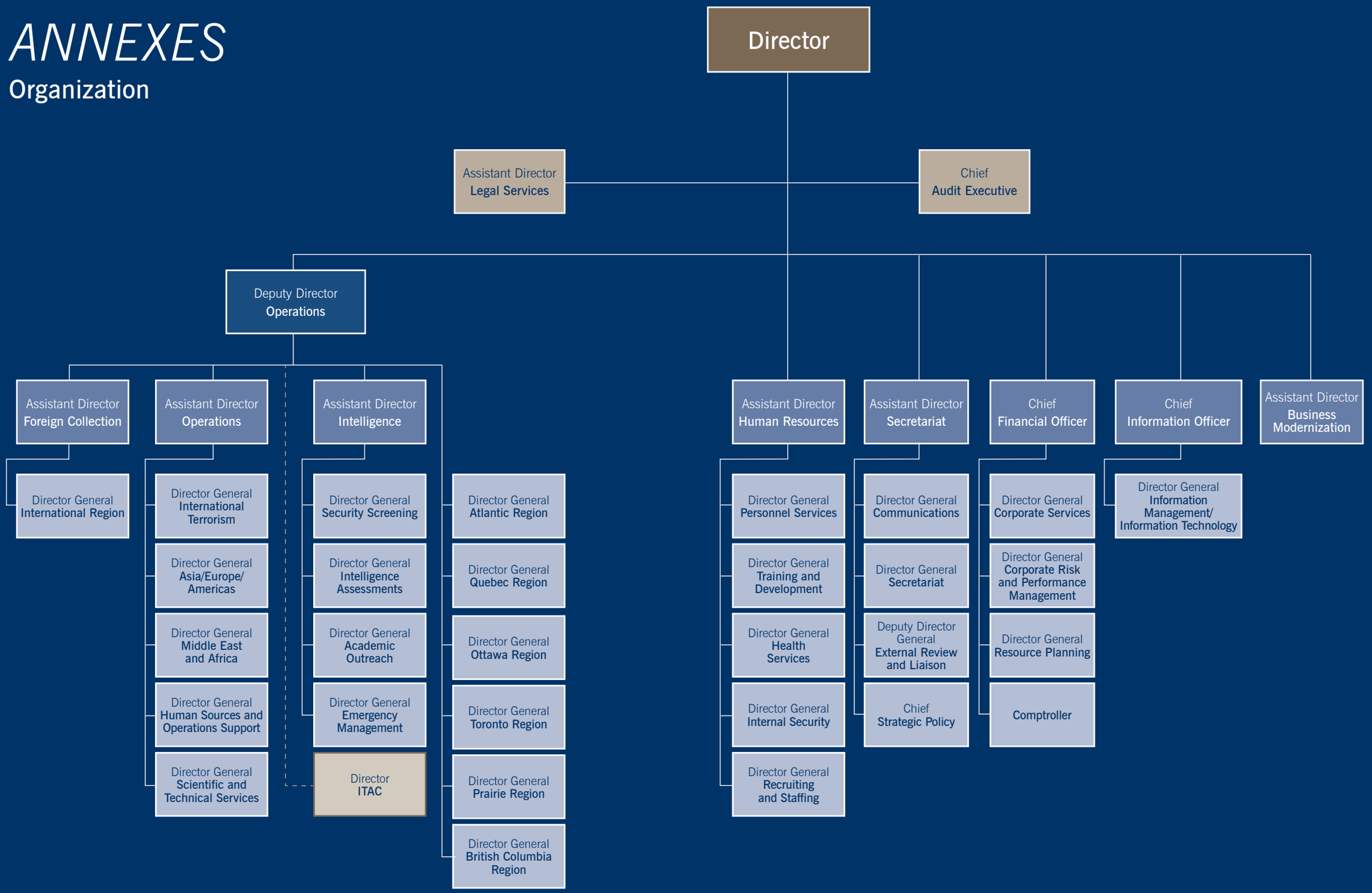
2009

CSIS has 2,910 positions, marking the first time the Service surpasses its previous high of 2,760 employees set back in 1993. The CSIS budget is at $430 million. In January, 35 people are killed and 80 injured in a suicide bomb attack in Iraq. Over 500 people are killed in the Democratic Republic of the Congo in several attacks in January suspected to have been carried out by the Christian extremist group 'Lord's Resistance Army' (LRA), based in Uganda. Elsewhere, 19 people are killed and more than 80 injured in attacks in the Gaza Strip. A car bomb explodes in Mogadishu, Somalia, killing 16 people and wounding over 30. The bomb is meant for African Union peace-keepers. In March, the Sri Lankan cricket team is attacked by armed gunmen in the streets of Lahore as it heads to a match with the Pakistani national team. Six policemen and the driver are killed while seven players, an umpire and an official are wounded in the ambush. In Northern Ireland, gunmen open fire on a military base, killing two British soldiers and injuring four people. A dissident Irish separatist group is believed to be behind the attack.

** Incidents listed are based on media reports and are not a comprehensive account of all terrorist or espionage incidents which occurred between July 1984 and June 2009. These examples reflect only those incidents which received a higher profile in media reporting.*

ANNEXES

Organization



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	P.O. Box 126, Station Central Halifax NS B3J 3K5 Tel. 902-420-5900
Quebec	P.O. Box 2000, Station A Montreal QC H3C 3A6 Tel. 514-393-5600 or 1-877-223-2265 toll-free (Quebec only)
Ottawa	P.O. Box 9732, Station T Ottawa ON K1G 4G4 Tel. 613-998-1679 or 1-800-267-7685 toll-free (Ontario only)
Toronto	P.O. Box 760, Station A Toronto ON M5W 1G3 Tel. 416-865-1480
Prairie (Alberta, Saskatchewan, Manitoba, Northwestern Ontario, Yukon and 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)
British Columbia	P.O. Box 80629, Station South Burnaby BC V5H 3Y1 Tel. 604-528-7400