Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

PUBLIC REPORT 2007-2008

Canada

Public Contact

For more information, please contact:
Canadian Security Intelligence Service
Communications Branch
P.O. Box 9732
Postal Station T
Ottawa, Ontario
K1G 4G4

(613) 231-0100 (Communications)
Internet: www.csis-scrs.gc.ca

Nº de cat. PS71-2008

ISBN 978-0-662-06366-7

Think recycling

This document is printed with environmentally friendly ink

The CSIS mandate

The Canadian Security Intelligence Service (CSIS) plays a leading role in protecting national security by investigating and reporting on threats to the security of Canada and its interests. Guided by the rule of law and the protection of human rights, CSIS works within Canada's integrated national security framework to provide information and advice to the Government of Canada on such threats.

Table of contents

Message from the Director

The 2007-08 fiscal year remained a busy period for CSIS on many fronts as we continued to provide the government with information and advice linked to threats to the security of Canada and its interests.

As described in the 'Threat Environment' portion of this report, counter-terrorism remained the Service's number one priority in 2007-08. Terrorism has existed for generations and is certainly not a recent phenomenon. In the past decade or so, and certainly since the September 11, 2001 attacks in the United States, most Western intelligence services have - not surprisingly - shifted their attention and resources to the threat of terrorism.

In particular, we have focussed our attention on the threat posed by those individuals who either follow - or are inspired by - Al Qaeda's ideology. Al Qaeda and its affiliated groups attract supporters from countries throughout the western world, including Canada. This threat is global in scope, unlike most other terrorist movements of the past which tended to be more nationally or regionally focused. Its international reach and operations, combined with its largely decentralized structure, complicate an already difficult operational challenge for counter-terrorism investigations by intelligence and security agencies.

Since the 9/11 attacks in the U.S., other plots have either been launched or disrupted in countries on several continents. Fortunately, to date nothing has matched the casualties inflicted in the 9/11 attacks, but this does not mean that the threat is disappearing. To become complacent or to spread a belief that Canada is immune from such threats could potentially have a tragic, devastating outcome.

The vast majority of people in Canada are law-abiding individuals who abhor the use of violence to achieve political or ideological goals, and who also believe that there should be no sanctuaries for terrorists. However, some individuals - even if they represent only a small fraction of a percentage of our population - are involved in activities that pose a security threat to Canada and its interests. The goal of CSIS is to provide the Government of Canada with the intelligence it needs to thwart such threats before they reach fruition.

While investigating the terrorist threat will remain the operational priority for CSIS in the foreseeable future, other issues continued to compete for operational resources in 2007-08. The threat posed by the proliferation of weapons of mass destruction and ongoing efforts by several countries to develop nuclear weapons continued to be a reality. Foreign espionage - the primary preoccupation of intelligence agencies right up until the 1990s - continued unabated after 9/11. It is in fact growing and becoming even more sophisticated and aggressive through the application of new technologies.

Foreign interference in domestic affairs, especially in multicultural societies with large immigrant communities such as ours, also remains an issue of concern. Cyberattacks on computer networks and other critical information technology systems - which used to be seen as largely the work of 'lone hackers' - are increasingly becoming an attractive option for certain foreign governments or groups seeking to disrupt a country's infrastructure or economy.

CSIS, like its counterparts, continues to face all these challenges while carrying out its mandate within today's threat environment. From an international perspective, the Service's increased role abroad, such as supporting the Canadian Forces in Afghanistan, represents a departure from pre-9/11 CSIS operations. We must continue to enhance our foreign presence to effectively counter threats to Canada which originate from outside of our country's borders.

We worked diligently in 2007-08 to address some of these issues, and we continue to identify ways to meet other challenges that lie ahead. We must continue to recruit new staff, acquire new technologies, and meet new demands from clients. The combined impact of growth and rapid demographic change continues to have an effect on the workforce of intelligence and security agencies, and CSIS is no exception.

We need to ensure that the transfer of knowledge, solid training and development programs for new recruits continue while this transition takes place. Looking at the CSIS experience to date, the infusion of youth has been working well given the dedication, education, technological skills, and fresh perspectives which our new recruits bring to the table. Our workforce is also more diverse than ever before, one of the positive aspects of the generational change.

On the public front, more is now known about the world of intelligence than in the past. Due to the nature of its work, CSIS must continue to protect its classified information and activities for reasons of national security, privacy and confidentiality. We cannot publicly discuss in detail our successes, nor our

mistakes. The protection of classified information, methodologies, and sources will always remain a crucial requirement for an intelligence service wishing to have any measure of success in carrying out its mandate.

However, greater public interest in national security issues, combined with various ongoing public inquiries, court proceedings, reporting from various review bodies and greater use of access-to-information provisions have resulted in greater transparency for organizations like CSIS. As a result, CSIS continued its efforts in 2007-08 for active communications and outreach initiatives, effectively explaining the Service's role, mandate and organization in general, and dispelling some myths and misconceptions which occasionally find their way in the public reporting of CSIS issues.

CSIS remains committed to a policy of public accountability. We welcome the tabling in the House of Commons of this 17th annual CSIS Public Report, which provides the Service with an opportunity to report on its priorities, activities and corporate issues for the 2007-08 fiscal year.

Finally, 2007-08 was also a positive year on the corporate front. Several CSIS employees were awarded a Public Service Award of Excellence for their work in the evacuation of Canadian citizens from Lebanon during the Israel-Lebanon conflict in the summer of 2006. Also, in November 2007, CSIS was awarded the Chair's Cup at the 2007 Government of Canada Workplace Charitable Campaign (GCWCC) Achievement Celebration, in recognition of the more than $164,000 which CSIS employees contributed to the GCWCC. And finally, CSIS was named as one of the 'Top 20 Employers in the National Capital Region' by an academic advisory board in 2007.

I am very optimistic about the future of CSIS. We have accomplished a great deal over the past few years, and as we approach our 25th anniversary, I am confident that we can do what must be done to become an even better organization and effectively meet the new challenges which lie ahead. I am proud to be part of an organization so dedicated to protecting our country and its citizens.

Jim Judd
Director
Canadian Security Intelligence Service

CSIS Operational Activities 2007-08

CSIS, like other organizations, must establish priorities to ensure the best use of its resources in fulfilling its mandate. Over time, priorities change with circumstances. For this reason, the Service's operational priorities are reviewed on an ongoing basis to ensure they reflect the current threat environment.

In the early days of CSIS, most of its operational resources were directed to counter-intelligence investigations. However, over the years - both before and after 9/11 - terrorism has emerged as the primary preoccupation of the intelligence community in Canada and abroad, and 2007-08 was no exception. The Government of Canada has identified counter-terrorism as the top priority of CSIS.

Other operational priorities for the Service in 2007-08 included investigations which focussed on: espionage and foreign interference (such as clandestine work of foreign governments in Canada); security threats against Canada's information systems and critical infrastructure (posed by hackers, terrorists and foreign countries); the proliferation of weapons of mass destruction (chemical, biological, radiological or nuclear threats); and terrorist financing. Finally, security screening also continued to be a key priority in 2007-08, as CSIS continued its work relating to security assessments of individuals as part of the Government Screening program, as well as in providing advice to Citizenship and Immigration Canada (CIC) as part of the Immigration Screening program.

THE THREAT ENVIRONMENT 2007-08

Terrorism

Unlike many nations, Canada has been fortunate that no major terrorist incidents have occurred within its borders, or originated from Canada (such as the tragic Air India bombing in 1985), in over two decades. While some incidents did occur in 2007-08 (for example, in April 2007, an explosive device was detonated outside a Jewish community centre in Montreal, causing damage but no injuries), the number of incidents of this nature have been minimal within Canada's borders over the past several years.

Terrorism, however, remains a real threat to the safety and security of Canadians. Since the 9/11 attacks in the U.S (in which 24 Canadians were among those killed), there continue to be major terrorist acts committed across the globe.

In Afghanistan, 30[1] Canadian soldiers were killed in 2007-08, most of them victims of improvised explosive devices (IEDs), or roadside bombs. Canada has the highest proportion of casualties amongst troops deployed for any North Atlantic Treaty Organization (NATO) member-states providing support to the International Security Assistance Force. Outside of Afghanistan, no major terrorist incidents were carried out against Canadians or Canadian interests in 2007-08. However, nothing exempts Canada from the threat of serious violence which other countries have already experienced. Canadians remain at risk of being directly targeted or simply having the misfortune of being in the 'wrong place at the wrong time' while travelling abroad.

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 2007-08. The notion of individuals or groups using violence aimed at governments and civilian populations with the intention of pressuring governments into changing policies is as old as recorded history itself. The current concept of terrorism has been enabled by several modern-day factors such as the Internet, cell phones, the proliferation of electronic media internationally, broader access to air travel, and 'homemade' improvised explosive devices. However, the objectives behind terrorist acts have remained the same throughout the centuries. Terrorism does not discriminate between its victims, with all races, religions, genders and age groups being affected. According to a report published by the U.S. National Counterterrorism Center (NCTC), it is estimated that over 50 percent of the victims of terrorist attacks in 2007 were Muslims. Additionally, 400 children were reported as either killed or injured in terrorist attacks during this same period.

> *"Terrorism is not a new phenomenon in Canada. Some Canadians have been and continue to be either victims of, or participants in, terrorist activity."*
>
> — CSIS Director Jim Judd, speaking at the Raoul Wallenberg International Human Rights Symposium.

The overall terrorist threat in 2007-08 remained of much concern to the international community, including Canada. When factoring in the terrorist incidents which occurred in Iraq and Afghanistan in 2007, the number of overall attacks reported in 2007 was virtually identical to that of 2006. In the years since the 9/11 terrorist attacks in the U.S., many countries have witnessed major terrorist incidents on their soil, both related and unrelated to Islamist extremism. Afghanistan, Algeria, Bangladesh, Colombia, Egypt, India, Indonesia, Iran, Iraq, Israel, Jordan, Lebanon, Libya, Morocco, Pakistan, the Philippines, Russia, Saudi Arabia, Somalia, Spain, Sri Lanka, Syria, Thailand, Tunisia, Turkey, the United Kingdom, the United Arab Emirates and

[1] *This figure does not include accidental deaths.*

Yemen - among others - have all suffered significant terrorist attacks resulting in the death of civilians. Such attacks demonstrate the horrific realities of today's international threat environment.

New threats have emerged, whether state-sponsored or presented by non-state actors. More recently, a new dimension to the overseas threat has surfaced in the form of homegrown radical extremism. In Europe, terrorist-related incidents and support networks remained a primary concern in 2007, as did the issue of radicalization. In East Africa, the presence of Al Qaeda and militants who support its cause continued to pose a serious security threat in the region. Additionally, ethnic violence and civil conflicts continued in a number of countries on the continent, feeding the terrorist threat and creating conditions whereby it can flourish.

In the East Asia and Pacific region, the Jemaah Islamiya terrorist network, which espouses - through violence - the amalgamation of Indonesia, Malaysia and the Southern Philippines into a regional Islamic state remained a serious threat to Western and regional interests. Militant and extremist activity was on the rise in Pakistan in 2007, with reported terrorist attacks increasing 137 percent from the previous year, culminating in the December 2007 assassination of Benazir Bhutto, former Prime Minister and Pakistani People's Party leader. Attacks in Afghanistan were also up 16 percent since 2006.

In the Middle East and North Africa regions, Iraq remained the country most affected by terrorist attacks, many attributed to Al Qaeda in Iraq (AQI) and other affiliated terrorist groups in the region. Additionally, Israel, Lebanon, Saudi Arabia, Yemen, Algeria and Morocco also suffered terrorist attacks in 2007.

The threat of transnational terrorist attacks in Central and South America remained low in 2007-08, but regional conflicts continued in several countries, particularly in Colombia, where government troops continued to battle terrorist groups such as the Revolutionary Armed Forces of Colombia (FARC) and the National Liberation Army (ELN). Peru's primary security concern remained that of preventing the re-emergence of the Sendero Luminoso (Shining Path) terrorist group, a listed entity under Canada's Anti-Terrorism Act which in previous decades was responsible for attacks against Canadian interests in the region, such as the 1991 bombing of the Canadian Embassy in Peru.

Like many other Western democracies, Canada has individuals within its borders who support the use of violence to achieve their political goals. Their activities are often linked to conflicts around the globe and typically include: planning or helping to plan terrorist attacks in Canada or abroad; providing a Canadian base for terrorist

supporters; fundraising; lobbying through front organizations; obtaining weapons and materials; and coercing and interfering with immigrant communities.

Not surprisingly, CSIS's current counter-terrorism priority is the threat posed by individuals and groups inspired by the ideology of Al Qaeda. In the foreseeable future, the primary threat to Canada and its interests will be that associated with Islamist extremism, or what has been referred to as the "Al Qaeda phenomenon". This threat to Canadian national security interests manifests itself on two levels: international and domestic.

The threat from Islamist extremism primarily originates from several groups that can be characterized as the Al Qaeda 'core', its affiliated groups, and those individuals inspired by Al Qaeda's ideology; all interpret world affairs through the prism of a perceived conflict between the West and Islam. In Canada, the relationship between the international and domestic threats is largely ideological and inspirational, rather than institutional and direct.

> *"While there are any number of terrorist organizations active in the world today, the most serious terrorist threat faced by most democracies currently is, broadly speaking, associated with the ideology of Al Qaeda. That is true for Canada as well".*
>
> — CSIS Director Jim Judd, speaking at the Raoul Wallenberg International Human Rights Symposium.

Canada has been specifically identified by Al Qaeda's senior leadership as an important ally of the U.S. and is therefore deemed a legitimate target by the group. At least three Al Qaeda propaganda releases since 2002 have explicitly threatened Canada, and warned that our country can expect attacks similar to those experienced in New York, Madrid, London and in other cities. In June 2007, a video of an Al Qaeda training camp graduation ceremony, obtained by ABC News, included footage of a senior Taliban leader encouraging suicide attacks against Canada and other countries. The video appeared to show training camps graduates being divided into groups of suicide bombers who would be dispatched to various NATO countries, including Canada, to carry out such attacks.

Additionally, Al Qaeda has identified Canada's oil industry as a target, and Canada's combat role in Afghanistan has also continued to raise its profile with groups such as Al Qaeda in 2007-08. CSIS, which continued to provide intelligence support to the Canadian Forces in Afghanistan, has had a presence in the country for the past

few years. The work undertaken by CSIS in Afghanistan has saved lives, and we will continue to do what we can to help our soldiers, as well as support Canadian interests and objectives in the region.

Al Qaeda and affiliated groups have struck repeatedly at Western interests internationally and they continue to plan and call for new attacks. The example set by global jihadists and their ideological pronouncements continue to provide direction to Islamist extremists living in the West, including in Canada. The Al Qaeda threat has not disappeared, despite the successes by intelligence and security forces in targeting and neutralizing much of the group's pre-9/11 leadership.

> *"Al Qaeda is the most technologically sophisticated terrorist threat that has been seen. This has been particularly true in terms of its reliance on the Internet as a multi-faceted facilitation tool to proselytize, to radicalize, to recruit, to communicate and to disseminate techniques and methods of operations".*
>
> — CSIS Director Jim Judd, speaking at the Raoul Wallenberg International Human Rights Symposium.

The group has evolved and new leaders have filled the gaps left by those arrested or killed. It has developed various degrees and levels of supporters and operatives that could be used as potential launching points for external attacks. Al Qaeda is also building global alliances with several groups that support its ideology. The organization has shown itself to be resilient, operationally imaginative and technologically adept. It has also proven to be a remarkable marketing machine with respect to using the international media and the Internet to disseminate its beliefs and celebrate its attacks.

Internet access is instantaneous and global, and creating a website is often possible at very minimal or virtually no cost. The Internet has become a key tool for several terrorist groups and plays a central role in the planning, organizing, and execution of terrorist activities, as well as in recruiting participants and disseminating propaganda. CSIS is aware that certain websites which support or incite terrorist violence are sometimes based in Canada.

The Internet provides those who espouse extremist violence with a multi-faceted tool which allows radicalized individuals to communicate with - and learn from - more experienced extremists and become more entrenched in a terrorist cause, often without leaving Canada. Terrorists exploit the borderless, real-time nature of the

Internet to operate in an integrated global manner that is both flexible and dynamic, thereby making effective countermeasures by intelligence and security services extremely difficult. In 2007-08, CSIS continued to enhance and develop its capacities to investigate and understand how terrorists are using the Internet to promulgate their ideology and plan their objectives.

The development of what has been referred to as "homegrown Islamist extremism" also continued to be a concern in 2007-08, a threat which refers to the sometimes rapid indoctrination and radicalization of young Canadians into the violent ideology espoused and inspired by Al Qaeda. Canada is home to certain individuals and groups that support the use of violence to achieve domestic political goals. These individuals and groups work outside the legitimate lawful, political and democratic system.

Homegrown extremists are influenced and motivated by perceptions that Western foreign policies and culture pose a direct threat to Islam. They have access to information and ideology via the Internet that feed their radicalization and lead them to embrace violence in the perceived defence of their community. Individuals now living in Canada who have undertaken terrorist training abroad could recruit participants to fight against the West, either overseas in places such as Afghanistan and Pakistan, or to carry out attacks in Canada or elsewhere. The Canadian experience has shown individuals involved in extremism to be of varied ethnic and socio-economic backgrounds. This makes their detection challenging and tracking their activities difficult to achieve. It is assessed that homegrown cells will continue to develop and that attacks using a variety of tools, from firearms to explosives, will be planned in the hopes of executing such attacks within Canada.

> *"What has been especially troubling about this has been (Al Qaeda's) capacity to expand its roster of activists to include citizens or residents of many democratic societies, at times through a process of what has come to be referred to as 'self-radicalization'. Canada, unfortunately, has not been an exception to this trend".*
>
> — CSIS Director Jim Judd, speaking at the Raoul Wallenberg International Human Rights Symposium.

Furthermore, the speed with which radicalization appears to be occurring makes it more difficult for security and law enforcement agencies to investigate such cells. It is also worth noting that the radicalization process appears to be beginning at a much younger age. Canada has adopted a "whole of government approach" to

better understand radicalization and develop measures to counter it. The threat in the current global context extends to non-state actors as well, specifically when dealing with Islamist extremism and radicalization within domestic expatriate communities. This threat exists not only in large urban centres, but also in suburban communities and smaller towns where globalization contributes to radicalization within isolated communities. The international and domestic threats from Islamist extremism are virtually indistinguishable, as the homegrown variety typically draws inspiration from the global jihadist movement. It is therefore impossible to separate the two when considering the implications for Canadian national security interests.

Espionage and Foreign Interference

While the terrorist threat remains the primary preoccupation for CSIS and its domestic and international counterparts, intelligence-gathering activities conducted by foreign intelligence agencies have not decreased. In the recent past, some foreign intelligence officers - through covert means - obtained status in Canada with the intention of gathering intelligence and stealing technology and intellectual property.

> *"Foreign espionage is growing and, in fact, becoming more sophisticated than ever through the application of new technologies. Foreign interference in domestic affairs is more prevalent than ever before".*
>
> — CSIS Director Jim Judd, speaking to the Canadian Association for Security and Intelligence Studies (CASIS).

State-sponsored agents and non-state actors are well-educated in the intricacies of Western immigration and refugee programs and policies. Forged and false documentation, identity legends and fronts are all used to gain a form of legitimate status within Canada, after which their clandestine activities begin. These include covert theft, source recruitment and handling, and intimidation of immigrant communities within Canada. They also cause financial loss to Canadian businesses, which can reduce the confidence in Canada's economic and national security.

Canada enjoys a unique position in the world through its economic, defence and international partnerships. As a resource-rich, high-technology nation, Canada is an industry leader in many areas such as agriculture and bio-technology, communications, oil exploitation, mining, the aerospace industry and control systems engineering. This favourable position of abundant resources and technological expertise is furthered through our access to the U.S. market and the fluidity of free trade across the border. As a committed member of NATO and a signatory to numerous bilateral and multilateral defence agreements, Canada has access to defence and military

technologies through its allies. All of the advantages found in our open and prosperous industrial and private sectors that attract business and investment opportunities are also the same attractive attributes sought by foreign intelligence agencies, international criminal gangs and global terrorist organizations.

Cybersecurity

Potential attacks against Canada's critical infrastructure continued to be a concern in 2007-08. For some time, Canada has been the target of cyber-related attacks for criminal, political or other motives. Canada's critical infrastructure includes physical and information technology facilities, networks and assets. The effective functioning of industry and government in Canada would be significantly affected should they be compromised. Such attacks could also have a serious impact on the health, safety, security and economic well-being of Canadians should these critical infrastructures be disrupted or destroyed.

> *"Attacks on computer networks and other critical information technology systems used to be seen as being largely the work of energetic but often strange young men sitting at their computers. It has become evident, however, that some of these young men have graduated to the payrolls of governments, bringing espionage into the highest levels of utilizing new technologies".*
>
> — CSIS Director Jim Judd, speaking to the Canadian Association for Security and Intelligence Studies (CASIS).

Politically motivated cyber-related attacks can originate from a variety of groups, including foreign governments, domestic hackers with an extremist political agenda, or terrorist groups. Open-source reports have also suggested that foreign intelligence services use the Internet to conduct espionage operations as a simple, low-cost, and relatively risk-free way to collect classified, proprietary or sensitive information.

Due to the seamless connectivity of global cyberspace, a domestic-based or foreign perpetrator could also stage an electronic attack against a Canadian target site in seconds. Terrorist groups could use such means to cause economic damage and serious disruptions to society without bloodshed and without the risk of being easily detected or captured. CSIS continued its work in 2007-08 to keep abreast of the changes in telecommunications and the Internet and - more specifically - their use by individuals and groups posing a security threat to Canada and its interests.

The spread and adoption of Internet Protocol (IP)-based technologies enable greater connectivity within the public and private sectors, but also provide more exploitable opportunities for various types of attackers. These technologies are widely understood by the hacker community and the impact of successful attacks can be more severe, due to the uniformity of networks and their underlying architectures. Where new systems are connected to old ones, additional vulnerabilities can appear.

The CSIS Information Operations Centre (IOC) functions as the Service's interface on the cyber-security aspect of the critical infrastructure protection issue. It carries out its work in consultation with other Canadian government departments, including the Government Operations Centre (GOC), Canada's national strategic-level operations centre. Within the Service, the IOC provides operational assistance to all the Service's operational branches regarding targets' use of advanced technology and the Internet.

Chemical, Biological, Radiological and Nuclear Threats

Chemical, biological, radiological and nuclear (CBRN) weapons are commonly grouped as 'Weapons of Mass Destruction' (WMD). In 2007-08, CSIS continued to assess and investigate the potential proliferation of WMD and the threat they pose to Canada or Canadian interests. Certain terrorist organizations such as - but not limited to - Al Qaeda or its affiliated groups continue to explore ways of obtaining and using such materials as part of their terrorist campaigns.

Chemical and biological weapons are easier and less expensive to produce than nuclear ones, and information on how to use such materials to conduct a small-scale attack has become more readily available through open sources such as the Internet. It remains very difficult for such groups to obtain or build reliable delivery methods to use chemical, biological or radiological materials in a large-scale attack. The probability, however, of small-scale CBR attacks occurring somewhere in the world is likely to rise as terrorists increase their familiarity and expertise with such materials.

Even a small-scale CBR attack with little or no casualties would achieve the psychological impact desired by such groups as a sign that the use of such materials would now be part of the equation. Many countries already possess WMD, or have the capacity to produce such materials, increasing the risk that such weapons may 'fall into the wrong hands', either inadvertently or via illicit purchase. In 2006, the leader of Al Qaeda in Iraq reiterated the call for the organization to acquire WMD to use in its campaign.

On the nuclear front, the proliferation of nuclear weapons, technology and expertise

- particularly to less stable or conflict-ridden regions - continues to present a security threat to the international community. In November 2006, the International Atomic Energy Agency (IAEA) warned that as many as thirty countries could have the capacity to develop nuclear weapons in the next several decades, absent successful non-proliferation measures.

However, the likelihood of a terrorist group constructing and using a nuclear explosive device is extremely low, due to the complexities and expense linked to obtaining materials, and constructing and deploying a nuclear weapon. The larger nuclear threat remains that of a rogue state, or one which is a sponsor of terrorism, obtaining nuclear weapons and technology for military use.

Terrorist Financing

There have been many changes in the past several years regarding financial intelligence, primarily as it relates to terrorist financing. Since the incidents of 9/11, governments the world over are quickly realizing that "following the money" is an essential step in fighting terrorism. For the most part, governments have implemented, or are in the process of implementing, a variety of anti-terrorist financing measures such as: passing pertinent legislation; designating terrorist entities and freezing their assets; establishing or enhancing financial intelligence agencies, such as the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC); reviewing the charity status of non-profit entities implicated in terrorist-related funding; and increasing cooperation amongst government agencies, both domestically and internationally.

Many challenges remain as to how international governments can best optimize financial intelligence to disrupt or shut down terrorist networks. Motivated by their violent ideology, terrorists and their supporters will continue to find ways to raise, move and store money to sustain their recruitment and training activities, and to launch terrorist attacks. Reports indicate that while terrorist groups continue to use methods such as using front corporations or charities to raise and transfer money around the globe, they are employing an ever-expanding repertoire of methods utilizing all the advantages of modern technology. The Internet and new payment technologies provide a plethora of opportunities for exploitation by not only criminals, but terrorists as well.

While many supporters give voluntary donations and some funds are siphoned from monies raised through forms of legitimate commerce, many terrorist groups must rely, at least to a degree, on revenues generated by illegal activities. This includes: passport forgery; drug trafficking; petty crime; fraud (including charity and welfare

> *"Let there be no mistake about this fact: money is the lifeblood of these terrorist organizations. They cannot operate without it. It takes money to send recruits to training camps, to buy weapons, to purchase other materials".*
>
> — Former CSIS Deputy Director, Operations, Luc Portelance, speaking to the Canadian Association for Security and Intelligence Studies (CASIS).

fraud); and violent crimes such as kidnappings and extortion.

Certain terrorist networks still manage their financial operations much like multinational corporations, complete with bank accounts in different countries. However, governments are making it increasingly difficult for such groups to move funds through financial institutions as financial intelligence units become more vigilant. In 2007-08, CSIS continued to focus attention on terrorist financing activities through its Financial Analysis Unit (FAU), which is mandated to conduct financial analysis on investigations linked not only to terrorism, but also to counter-proliferation and counter-intelligence concerns. The CSIS FAU analysts and financial specialists are called upon to provide expert support to operational desks on issues relating to the financing of terrorists and other threats to Canada's interests. CSIS works with domestic partners such as FINTRAC, the Royal Canadian Mounted Police (RCMP) and the Canada Revenue Agency to investigate the financing of terrorists and other security threats. Additionally, the CSIS FAU forges liaison relationships with foreign allied counterparts to share information and discuss issues of mutual interest in this area.

SECURITY INTELLIGENCE ACTIVITIES

Intelligence Collection

In order to fulfill its mandate, the Service often provides advice to the Government of Canada in the form of intelligence reports about activities that may constitute a threat to the security of Canada. This information is collected from many sources, including: interviews with members of the public; liaison and cooperation with federal, provincial and municipal partners as well as foreign agencies; human sources; technical interception of communications; and the review and analysis of open sources, including newspapers, periodicals, academic journals, foreign and domestic media broadcasts and other published materials.

When CSIS has reasonable grounds to suspect that the activities of a person or an organization may pose a threat to the security of Canada, it must first establish the

appropriate level of investigation. As a guiding principle, CSIS must ensure that it applies its powers in a way that is proportional to the threat. As per the *CSIS Act,* warrant submissions must be approved internally by the CSIS Director, and subsequently by the Minister of Public Safety Canada (PS), prior to a warrant going to a Federal Court judge for approval.

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. Investigations that require the use of more intrusive techniques, such as the interception of telecommunications, are subject to a rigorous process of challenge and controls. 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.

In order to ensure a balance between security and individual rights, CSIS observes the following operational principles when considering and carrying out its intelligence investigations:

- activities and investigations are subject to Government of Canada laws and must respect the rule of law;
- the use of intrusive investigative techniques must be weighed against possible damage to civil liberties;
- lawful advocacy, protest or dissent cannot be investigated unless such activities are carried out in conjunction with specific threats to national security, as defined in the *CSIS Act*; and
- the investigative means must be proportional to the gravity and imminence of the threat.

Analysis of Information Collected

In 2007-08, CSIS analysts continued to use their knowledge of regional, national, and global issues to assess the quality of information gathered, and to convert the information into useful security intelligence that is shared within the Canadian government and with partners in the security and intelligence community. At a strategic level, CSIS produces reports on emerging trends and issues that could affect the security of Canada and that provide context about specific threats and their security implications. Strategic assessments are particularly useful to policy analysts and strategic decision-makers. On a tactical level, CSIS analyzes, publishes, and disseminates intelligence products that address current threats to the security of Canada. Additionally, the CSIS Operational Data Analysis Centre (ODAC) provides

support to the Service's operational branches by performing advanced analysis of data that is collected on subjects of investigation.

SECURITY SCREENING PROGRAM

As a vital component of Canada's national security framework, the CSIS Security Screening program is not only the most visible function undertaken by the Service, it is also one of its primary operational responsibilities.

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 also assist in enhancing security and reducing 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 or related information to the governments of foreign states, to foreign agencies, and to 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.

TABLE 1:
Government Screening

Programs	Requests received *	
	2006–07	2007–08
Department of National Defence (DND)	13,100	8,800
Other departments/agencies	38,100	41,500
Subtotal	**51,200**	**50,300**
Parliamentary Precinct	1,100	1,100
Transport Canada	39,400	43,100
Nuclear Facilities	17,900	9,200
Special Events Accreditation	0	1,300
Free and Secure Trade (FAST)	23,100	10,700
Provinces	100	170
Site Access - Others	2,400	2,000
Foreign checks	1,000	800
Subtotal	**85,000**	**68,370**
GRAND TOTAL	**136,200**	**118,670**

* Figures have been rounded

Immigration Screening Program

While Canada's long and valued tradition of welcoming immigrants and visitors continues, Canada and its allies must maintain a heightened and sustained vigilance to counter terrorist acts and espionage incidents which constitute a threat to our personal and economic security. Therefore, 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 CIC as well as to the Canada Border Services Agency (CBSA) via this program.

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

TABLE 2:

Immigration Screening

Programs	Requests received *	
	2006-07	2007-08
Permanent Residents Within and Outside Canada	62,800	66,000
Front-end Screening	17,900	21,800
Refugee Determination Program	11,600	6,600
Citizenship Applications	227,300	190,000
Visitors Visa Vetting	114,500	111,300
TOTAL	**434,100**	**395,700**

* Figures have been rounded

DOMESTIC AND INTERNATIONAL COOPERATION

In 2007-08 and over the past decade, the Service has increased its intelligence and cooperative agreements, both at the national and international levels, to more effectively evaluate current and future threats. In doing so, CSIS works with a wide variety of partners in Canada and abroad.

Domestic Cooperation

With its National Headquarters (NHQ) located in Ottawa, Regional offices in Halifax, Montreal, Ottawa, Toronto, Edmonton and Burnaby, and District offices in St. John's, Fredericton, Quebec City, Winnipeg, Regina, Edmonton and Calgary, CSIS is geographically well-positioned within Canada. This allows the Service to continually liaise and cooperate with its many federal, provincial and municipal partners on security issues of mutual interest.

INTEGRATED NATIONAL SECURITY ENFORCEMENT TEAMS (INSETs)

One component of such domestic cooperation is the Integrated National Security Enforcement Teams (INSETs), which are operationally led by the RCMP. Strategically based in locations across the country, INSETs share and analyze information on individuals whose activities have been identified as being threats to national security. In 2007-08, CSIS continued its participation in INSETs by sending secondees from Regions and Headquarters to work alongside the RCMP and other representatives such as those from CIC, CBSA, and provincial and municipal police services. INSETs increase Canada's capacity to collect and share intelligence among partners concerning targets that threaten national security and their related criminal activities, and also create an enhanced enforcement capacity to apprehend such targets and bring them before the courts.

Another method by which CSIS cooperates with its domestics partners is by producing and disseminating intelligence reports such as those drafted by our Intelligence Assessments Branch (IAB) or threat assessments from the Integrated Threat Assessment Centre (ITAC), which is housed within CSIS Headquarters.

INTEGRATED THREAT ASSESSMENT CENTRE (ITAC)

ITAC was created under Canada's National Security Policy in April 2004 and has been operational since October 15th, 2004. Its primary objective is to produce integrated, comprehensive and timely threat assessments for all levels of government with security responsibilities, first-line responders such as law enforcement and, as appropriate, critical infrastructure stakeholders in the private sector. ITAC's assessments, based on intelligence and trend analysis, evaluate both the probability and potential consequences of terrorist threats.

ITAC, a community-wide resource, is staffed by CSIS personnel as well as representatives of the following federal organizations: PS; RCMP; CBSA; DND; FINTRAC; the Communications Security Establishment; Foreign Affairs and International Trade Canada; the Privy Council Office; Transport Canada; and Correctional Service Canada. The Ontario Provincial Police and the Sûreté du Québec also have members assigned to ITAC. These representatives bring the information and expertise of their respective organizations to ITAC.

The Director of CSIS is accountable for the performance of ITAC. In recognition of ITAC's unique mandate as a security and intelligence community-wide resource, the Director of CSIS obtains guidance on a regular basis from the National Security Advisor to the Prime Minister about the strategic direction and overall performance of

ITAC. The Director of CSIS also seeks guidance from ITAC's Management Board, a community of heads of departments and agencies that have representatives in ITAC, to provide strategic direction to ITAC.

In 2007-08, ITAC produced and disseminated 348 threat assessments to its clients. Additionally, ITAC distributed its 'Media Watch' report on a daily basis to federal, provincial, law enforcement and private sector clients across Canada.

In 2007-08, ITAC also provided presentations, briefings and training to a wide variety of audiences. For example, briefings were provided to several law enforcement training courses, to critical infrastructure stakeholders such as the Canadian petroleum industry, and to first responders such as the Canadian Association of Chiefs of Police.

Canadian security will increasingly depend on the country's ability to contribute to international security. Accordingly, ITAC contributes to a more integrated international intelligence community by cooperating with foreign integrated threat assessment centres and, in doing so, provides Canada and its partners with international perspectives on the worldwide threat posed by terrorism.

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. The Government of Canada has also identified ITAC as the primary central point for various threat assessments which will be prepared by ITAC and partner agencies linked to the 2010 Winter Olympic and Paralympic Games in Vancouver.

FOREIGN COOPERATION

CSIS's primary focus remains directed on domestic investigations, but under section 12 of the *CSIS Act*, the Service also collects security intelligence information abroad linked to threats to Canada and its interests which originate in a foreign country. With few exceptions, the roots of threats to the security of Canada are located outside of our country's borders. These roots - particularly those feeding terrorist movements - are grounded in regions or states abroad which suffer from endemic security problems, or are actual war zones. This reality poses serious challenges with respect to finding reliable local partners in such areas of conflict, and to giving intelligence services the capacity to collect timely and accurate information.

About 50 CSIS Foreign Officers were located abroad in 2007-08 in approximately

30 countries, including Washington, London and Paris, among others. These officers are declared to the host countries as being CSIS employees. Their primary functions are to provide screening support to CIC posts abroad, liaise and maintain relations with our international partners, and collect security intelligence information linked to Canada and its interests. Occasionally, CSIS also sends Canadian-based officers abroad to engage in intelligence activity to fulfill the requirements of section 12 of the *CSIS Act* relating to threats to Canada and its people.

> *"The (Al Qaeda) terrorist threat is one which does not acknowledge national boundaries. Most of the conspiracies or attacks that it has undertaken in the last decade have involved international networks of individuals and groups. Responding effectively to this kind of multilateralism can only be achieved through international collaboration" .*
>
> — CSIS Director Jim Judd, speaking at the Raoul Wallenberg International Human Rights Symposium.

The Service has information-sharing arrangements with many foreign organizations. These agreements give CSIS access to intelligence that might not otherwise be available to it. In 2007-08, CSIS implemented five new foreign arrangements, and currently has 276 foreign arrangements in 147 countries. The Service has one of the most stringent processes of all intelligence services 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 & 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 regards to those foreign arrangements.

Additionally, the Security Intelligence Review Committee (SIRC) and the Inspector General (IG) carefully examine the Service's foreign arrangements and monitor the exchange of information to ensure the terms of the arrangements are upheld.

In 2007-08, CSIS continued to monitor the human rights situation in all partner countries on an ongoing basis. It also reviewed various government and non-government human rights reports and assessments of all countries with which the Service has implemented ministerially approved foreign arrangements, an

ongoing practice which is part of the Service's management and assessment of its foreign relationships. CSIS also continued to implement the recommendations made by the O'Connor Commission of Inquiry regarding the Service's management of its exchanges with foreign agencies.

Inside CSIS

OUR PEOPLE

In 2007-08, CSIS had 2,529 full-time equivalent (FTE) employees. Many people perceive all CSIS employees as being "spies". In actuality, what one sees in James Bond and similar movies and novels pertaining to the intelligence business - while quite entertaining - is far removed from reality. In fact, 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, among others.

The CSIS workforce is diverse. In 2007-08, it was split evenly along gender lines, while visible minorities were represented in higher proportions than the average for the federal public service. Sixty-five percent of our employees speak both of Canada's official languages. In addition, 42 percent of our IOs can speak a language other than English or French. Collectively, our employees speak about 100 languages.

In 2007, several CSIS employees were awarded a Public Service Award of Excellence for their work in the evacuation of Canadian citizens from Lebanon during the Israel-Lebanon conflict in the summer of 2006. That award recognizes employees who have demonstrated excellence in achieving results for Canadians that reflect the current values, ethics and priorities of the public service of Canada.

Also, in November 2007, CSIS was awarded the Chair's Cup at the 2007 Government of Canada Workplace Charitable Campaign (GCWCC) Achievement Celebration, in recognition of its campaign. The Chair's Cup recognizes overall campaign excellence in a department or agency, and CSIS was chosen by the GCWCC as the award's recipient for 2007. CSIS employees contributed more than $164,000 to the 2007 GCWCC.

EMPLOYEE RECRUITMENT

CSIS has made it a priority to recruit a new generation of professionals reflecting the current demographic realities of Canada. The Service continues to attract many bright young Canadians to its ranks, people who have the knowledge, aptitude, skills and passion for modern intelligence work and the desire to protect Canada's national security.
In 2007-08, CSIS participated in 62 career fairs, provided 111 information briefings on IO positions and participated in eight employee recruitment sessions held at various receptions and cultural events.

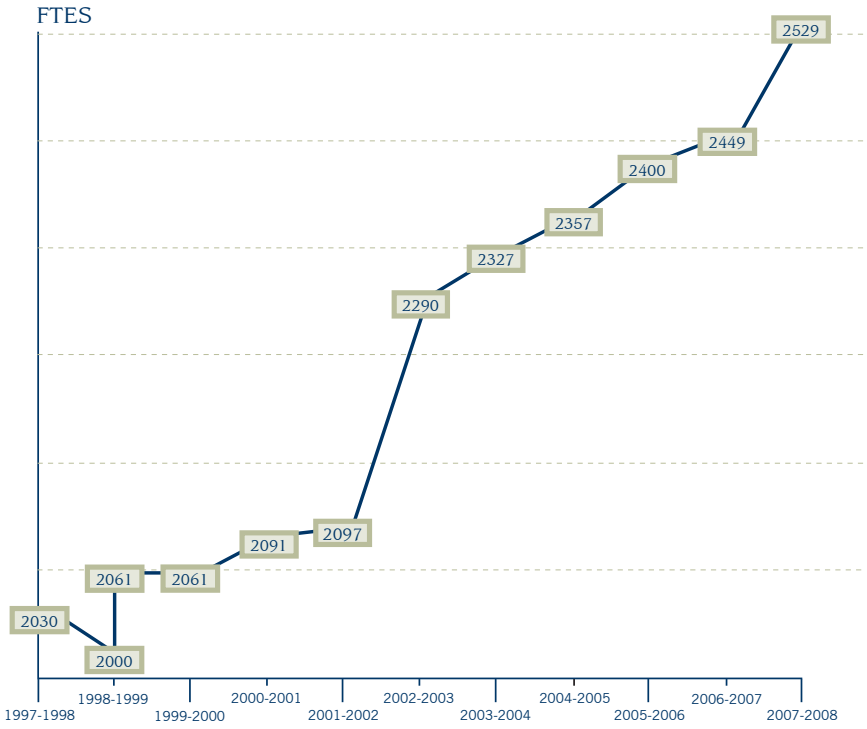
> *"We have very professional and dedicated employees, people who fulfill a core mandate of government, and, increasingly, with a higher level of personal risk. But we also recognize the need to build on those strengths by attracting new types of expertise and talent".*
>
> — CSIS Director Jim Judd, speaking to the Canadian Association for Security and Intelligence Studies (CASIS)

In October 2007, an academic advisory board, which oversees the selection process for the 'Canada's Top 100 Employers' competition as published in Maclean's magazine, named CSIS as one of the 'Top 20 Employers in the National Capital Region'. This special designation recognizes the Ottawa-area employers that lead their industries in offering exceptional places to work.

TABLE 3:
CSIS Workforce 2007-08

No. of FTEs	2,529
Average age of CSIS employees	41
% of bilingual employees (English and French)	65%
% of IOs who speak a language other than English or French	42%
% of women	49%
% of CSIS managers from IO stream	71%

TABLE 4:
CSIS Workforce 2007-08



National Headquarters

In order to meet the Service's evolving needs linked to its increased responsibilities, CSIS was granted approval to proceed with an expansion project to its NHQ in Ottawa. As a result, preliminary site access work began in 2007-08 and the Service is anticipating the beginning of the construction of a five-storey tower next to its NHQ building. The new tower will meet the highest standards in environmental stewardship as well as water and energy efficiency. Environmental and security studies have been carried out to ensure that the new tower will not have a detrimental impact on the surrounding environment or neighbourhood. Estimated completion of the tower is forecast for 2011.

REGIONAL PROFILE: QUEBEC REGION

- In 2007-08, the CSIS Quebec Region office, located in Montreal, continued to strengthen ties with the intelligence community in its geographical area by participating in conferences and meetings with its various partners on security and intelligence issues of mutual interest;
- Quebec Region was also very active in its employee recruitment efforts in 2007-08, particularly in the IO, surveillance, technical and linguistic fields;
- The Region participated in approximately 10 employee recruitment or career fair events in both the private sector and at universities;
- The Region also continued its networking efforts with various university student placement centres to encourage graduating students to apply for employment with CSIS;
- Additionally, Quebec Region offered approximately 30 outreach briefings to various community, cultural, university, private sector and intelligence community groups in an effort to provide a greater understanding of the Service's role and mandate.

CSIS FINANCIAL RESOURCES

CSIS's final expenditures for 2007-08 totalled $389 million.

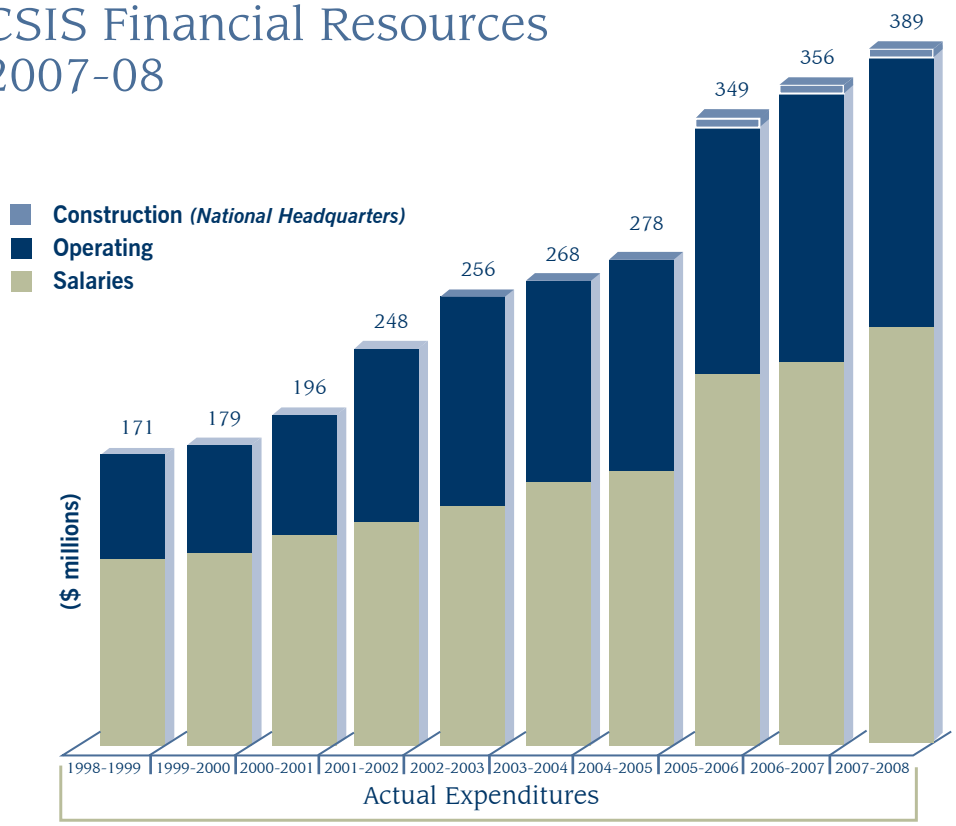
The Service's financial resources have increased since 2001–02 partly as a result of new funding for public security and anti-terrorism initiatives allocated in the December 2001 Federal Budget. In addition, CSIS received resources for its part in the Government of Canada's Marine Security Initiatives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

In 2007-08, additional funding was allocated through the Federal Budget in order to help CSIS maintain its operational capacity and expand its National Headquarters.

Finally, the 2008 Federal Budget committed $10 million over two years to Canada Revenue Agency's Charities Directorate and to CSIS in order to bolster existing capacities to combat terrorist financing.

TABLE 5 :

CSIS Financial Resources 2007-08



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, costs incurred were mainly attributable to site preparation. Preliminary site preparation began in the spring of 2008.

REVIEW AND ACCOUNTABILITY

The CSIS Director is accountable to the Minister of Public Safety. The Minister of Public Safety is responsible for providing Ministerial Direction to the Director of CSIS on matters concerning the policies, operations and management of the Service.

CSIS is bound by the legislation spelled out in the *CSIS Act*. The operational activities of the Service are reviewed on an ongoing basis by two review bodies established by Parliament in the *CSIS Act*. In fact, CSIS is one of the most reviewed intelligence organizations in the world, with more than half of the sections in the

CSIS Act addressing review and accountability issues.

The Service must also respect a variety of other federal statutes, such as the *Access to Information* and *Privacy Acts*, the *Official Languages Act* and others. In 2007-08, the CSIS Access to Information and Privacy (ATIP) Unit received 150 access to information requests, and 745 privacy requests. Like other federal institutions, certain CSIS activities are also reviewed by the Office of the Auditor General and the Canadian Human Rights Commission.

> *"Democracies have taken a long period to develop, and their values, laws and institutions continue to provide inspiration to those without the luxury of living in one. It is thus essential that, in responding to threats such as terrorism, we do so in a fashion that best reflects what democracies stand for".*
>
> — CSIS Director Jim Judd, speaking at the Raoul Wallenberg International Human Rights Symposium.

As a result of the combined efforts of SIRC and the IG, which conducted reviews of various CSIS cases in 2007-08 as part of their respective mandates, CSIS has become a more effective and professional organization. CSIS remains committed to working with these review bodies and maintaining a productive and professional relationship with them.

The Inspector General (IG)

The mandate of the IG of 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)

SIRC 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, all of which are given careful consideration for implementation by the Service; in fact many of SIRC's recommendations are implemented. SIRC also investigates public complaints against CSIS, and has access to all information under CSIS's control (except for Cabinet confidences). SIRC informs the Minister of Public Safety of its investigative findings on an ongoing basis.

Management Accountability

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 with a list of management expectations and suggests ways for departments and agencies to move forward and to measure progress.

The MAF observations of CSIS in 2007-08 were generally positive. TBS acknowledged the Service's status as an excellent employer with innovative human resource practices that attract and retain quality staff. Also, the Service was recognized as having improved since the 2006-07 MAF assessment in areas such as: 'Effectiveness of Financial Management Controls'; 'Effectiveness of the Corporate Management Structure'; and 'Managing Organizational Change'.

In its 2007-08 assessment, TBS recommended that in 2008-09, the Service focus on the CSIS 'Corporate Performance Framework'. The development of a 'Management, Resources, and Results Structure' will also more clearly explain what results CSIS strives to achieve in carrying out its mandate. It will also provide a comprehensive list of programs managed by the Service in support of its objectives in order to assess results of its performance on an annual basis.

"In the realm of traditional public communications, it is increasingly important for us to be able to explain both what we do - and what we do not - and how. While there will always be limits on what we can and cannot discuss publicly, there is a clear imperative for a better understanding of an organization such as ours, given the mandate we have and the misconceptions that often surround our work".

— CSIS Director Jim Judd, speaking to the Canadian Association for Security and Intelligence Studies (CASIS).

PUBLIC COMMUNICATIONS

In a poll[2] conducted in December 2007, 65% of Canadians queried indicated some level of awareness of CSIS, and 81% of those cited either 'moderate' or 'high' confidence in the Service. These numbers have remained virtually unchanged over the past five years.

CSIS is often labelled as a secretive agency. However, CSIS is not a secretive organization, but rather one which, due to the nature of its work, must deal in secrets and classified information and activities. Although the Service takes a number of initiatives to keep Canadians informed about what it is and what it does, the nature of security intelligence work prevents CSIS from discussing the details of its operational activities and information. Where it can, however, CSIS does reach out to Canadians in order to better explain the Service's role, mandate and organization in general.

For example, in 2007-08, CSIS:

- responded to over 330 media queries;
- responded to more than 990 public queries;
- 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 maintain its public website.

Aside from its public and media communications program, the Service also participates in many outreach initiatives so as to better explain to various communities who we are and what we do. In 2007-08, CSIS continued its efforts in this regard by providing briefings and presentations to:

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

In 2007-08, CSIS participated in regional events of the federal Cross-Cultural Roundtable on Security, in career fairs, employee recruiting events at universities, and community festivals.

[2] *Source: EKOS Research Associates 2008.*

The CSIS Director and Deputy Director also participated in the Canadian Association for Security and Intelligence Studies (CASIS) Conference in November 2007, which was held in Calgary. Additionally, the CSIS Director delivered a keynote speech at the Carleton University Alumni Association Luncheon in May 2007.

In November 2007, CSIS hosted its 12th Annual 'Youth Day' at its National Headquarters, where 57 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 challenging learning and career opportunities for young people and to showing them how important skills, training and education are critical to their success.

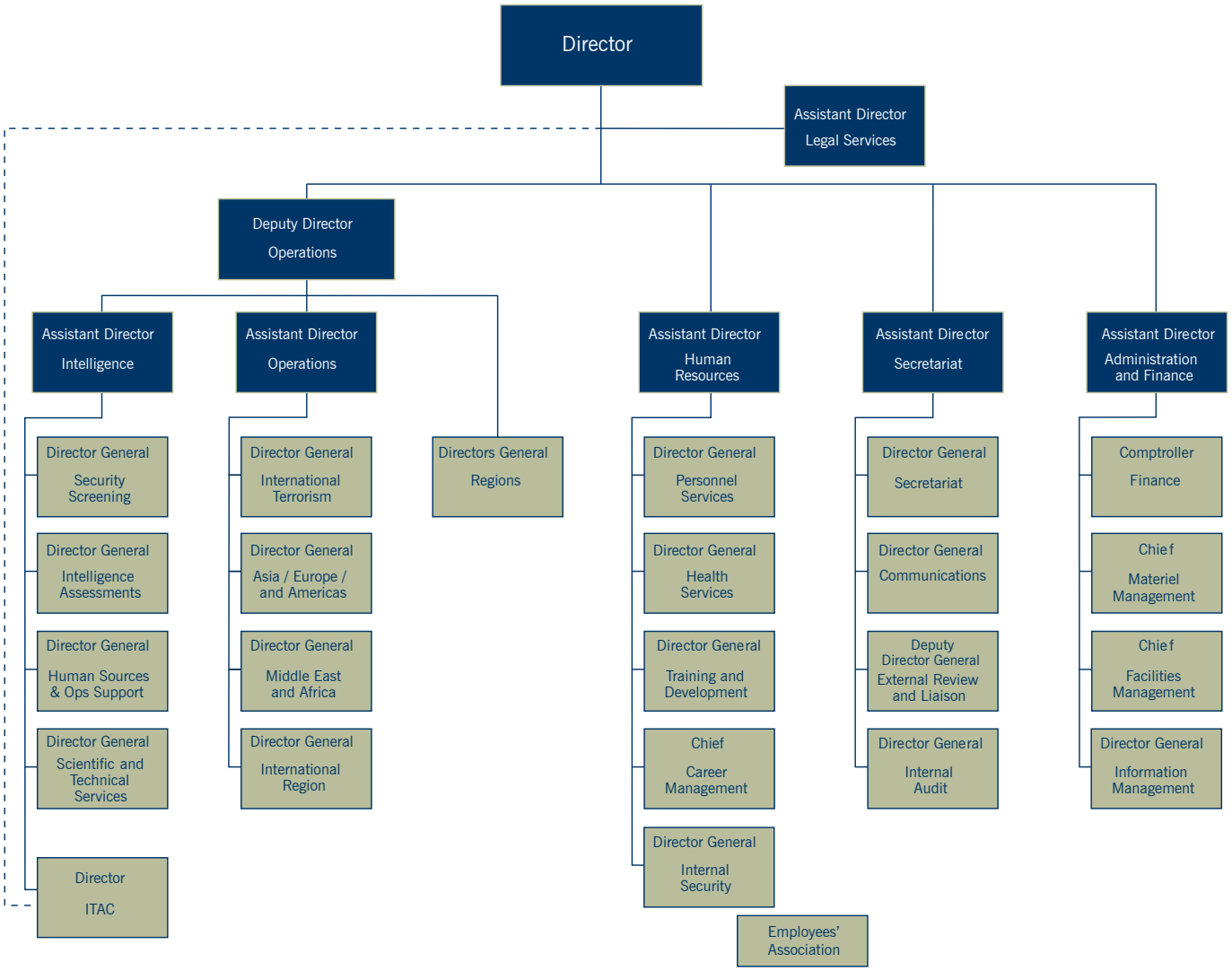
Lastly, the CSIS website (www.csis-scrs.gc.ca) continued to be a popular Internet destination for those looking for information about the Service and on various issues associated with its work. The following chart provides approximate figures on the number of times various pages on the CSIS site were viewed in 2007-08:

CSIS Website – 2007-08*

Item(s) viewed	Number of views
Website (total views of all pages)	6,468,236
Backgrounders	69,723
Integrated Threat Assessment Centre	64,160
Commentary	169,842
Perspectives	49,070
Public Report (all years)	48,061
Recruitment information and job postings	3,554,626

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

Annexes
CSIS Organization 2007-08



CONTACT US

NATIONAL HEADQUARTERS:
Canadian Security Intelligence Service
PO 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
PO Box 9732, Station T
Ottawa ON K1G 4G4
Tel. 613-231-0100

REGIONAL OFFICES:

Atlantic	PO Box 126, Station Central Halifax NS B3J 3K5 Tel. 902-420-5900
Quebec	PO Box 2000, Station A Montreal QC H3C 3A6 Tel. 514-393-5600 or 1-877-223-2265 toll-free (Quebec only)
Ottawa	PO Box 9732, Station T Ottawa ON K1G 4G4 Tel. 613-998-1679 or 1-800-267-7685 toll-free (Ontario only)
Toronto	PO Box 760, Station A Toronto ON M5W 1G3 Tel. 416-865-1480
Prairie (Alberta, Saskatchewan, Manitoba, Thunder Bay)	PO Box 47009 62 City Centre Edmonton AB T5J 4N1 Tel. 780-401-7800 or 1-800-661-5780 toll-free (Prairie only)
British Columbia	PO Box 80629, Station South Burnaby BC V5H 3Y1 Tel. 604-528-7400