Canadian Security Intelligence Service
Service canadien du renseignement de sécurité

CSIS PUBLIC REPORT 2019

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

Canada

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

Published in April 2020

CSIS PUBLIC REPORT 2019

TABLE OF CONTENTS

CONFIDENCE

OUR VISION

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

MESSAGE FROM

THE DIRECTOR

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

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 This legislation modernized the original *CSIS Act* by addressing outdated legal authorities, introducing new safeguards and accountability measures as well as clarifying CSIS' responsibilities.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

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

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

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

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

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

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

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

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

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

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

David Vigneault, Director


RELEVANCE

CSIS AT A GLANCE

CORE MANDATE

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

THREATS TO THE SECURITY OF CANADA

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

PARTNERSHIPS

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

ACCOUNTABILITY

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

DUTIES AND FUNCTIONS

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

DEPARTMENTAL RESULTS FRAMEWORK AND FINANCIAL REPORTING

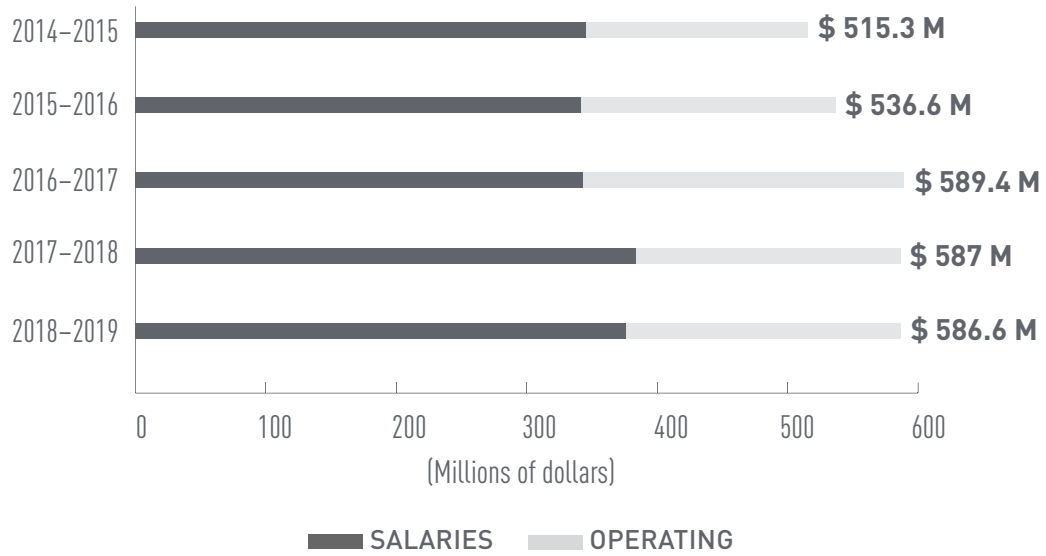
DEPARTMENTAL RESULTS

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

PROGRAM INVENTORY

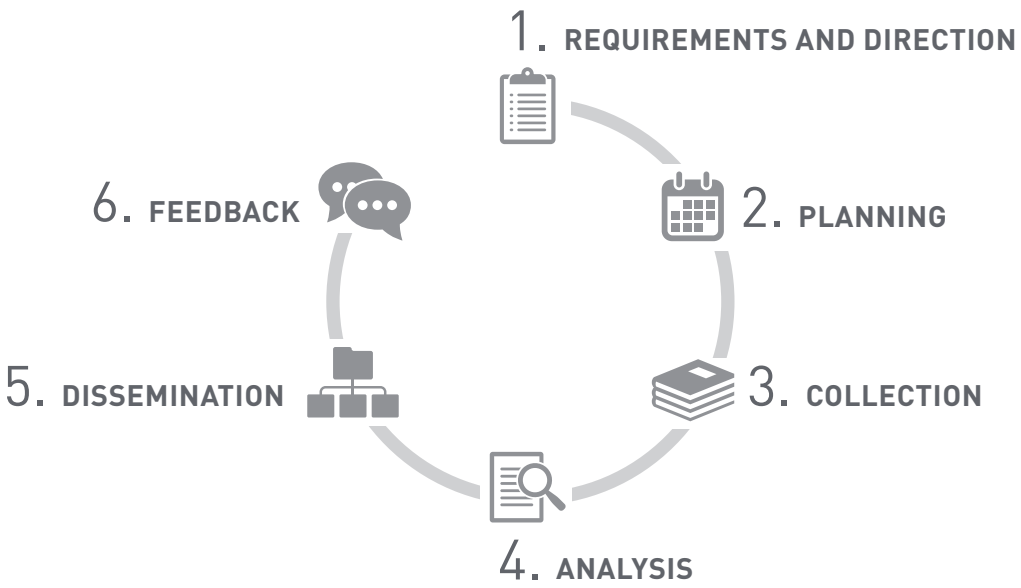
- Operational Program Management
- Regional Collection
- Operations Enablement
- Intelligence Assessment and Dissemination
- Security Screening
- Integrated Terrorism Assessment Centre

ACTUAL EXPENDITURES



THE INTELLIGENCE CYCLE

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



REQUIREMENTS AND DIRECTION

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

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

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

PLANNING

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

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

COLLECTION

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

This information is collected from various sources, including:

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

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

ANALYSIS

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

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

DISSEMINATION AND FEEDBACK

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

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

THREATS TO THE SECURITY OF CANADA AND CANADIAN INTERESTS

TERMINOLOGY – WORDS MATTER

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

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

Religiously Motivated Violent Extremism (RMVE)

Ideologies that underpin RMVE often cast an individual as part of a spiritual struggle with an uncompromising structure of immorality. RMVE ideologies assure their adherents that success or salvation — either in a physical or spiritual realm can only be achieved through violence.

Politically Motivated Violent Extremism (PMVE)

PMVE narratives call for the use of violence to establish new political systems – or new structures and norms within existing systems. Adherents focus on elements of self-determination or representations rather than concepts of racial or ethnic supremacy.

Ideologically Motivated Violent Extremism (IMVE)

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

TERRORISM AND VIOLENT EXTREMISM

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

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

GLOBAL

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

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

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

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

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

DOMESTIC

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

IDEOLOGICALLY MOTIVATED VIOLENT EXTREMISM (IMVE)

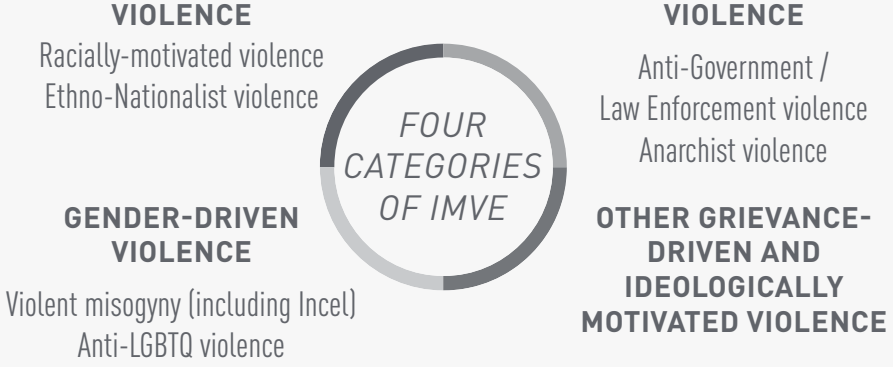
Ideologically motivated violent extremism (IMVE) is often driven by a range of grievances and ideas from across the traditional ideological spectrum. The resulting worldview consists of a personalized narrative which centres on an extremist's willingness to incite, enable and or mobilize to violence.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

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

EXAMPLE OF IMVE

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

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



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

CANADIAN EXTREMIST TRAVELLERS

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

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

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

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

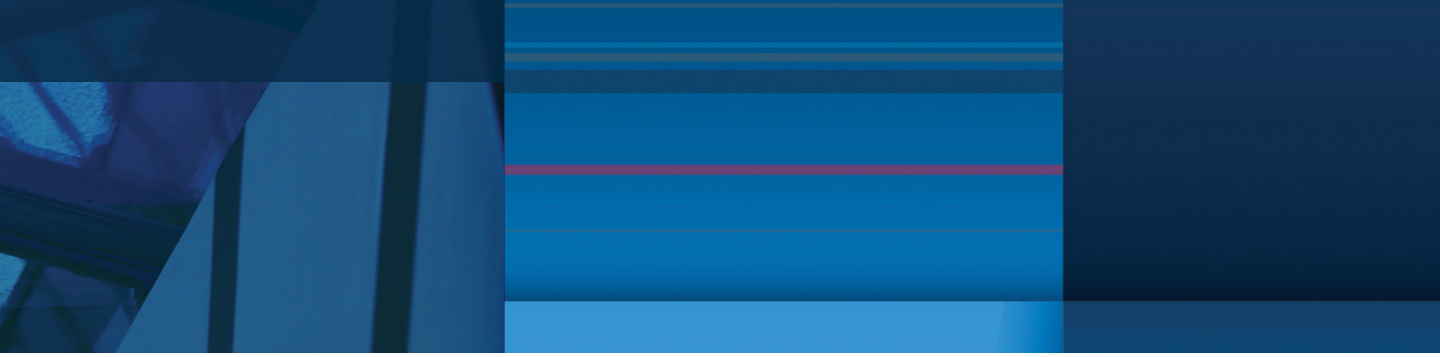
NAVIGATING THE ONLINE SPACE

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

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

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

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



ESPIONAGE AND FOREIGN-INFLUENCED ACTIVITIES

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

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

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

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

ECONOMIC SECURITY

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

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

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

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

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

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

PROTECTING DEMOCRATIC INSTITUTIONS

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

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

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

CYBER THREATS

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

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

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

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

SECURITY SCREENING

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

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

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

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

IMMIGRATION AND CITIZENSHIP SCREENING PROGRAMS

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

GOVERNMENT SCREENING PROGRAMS

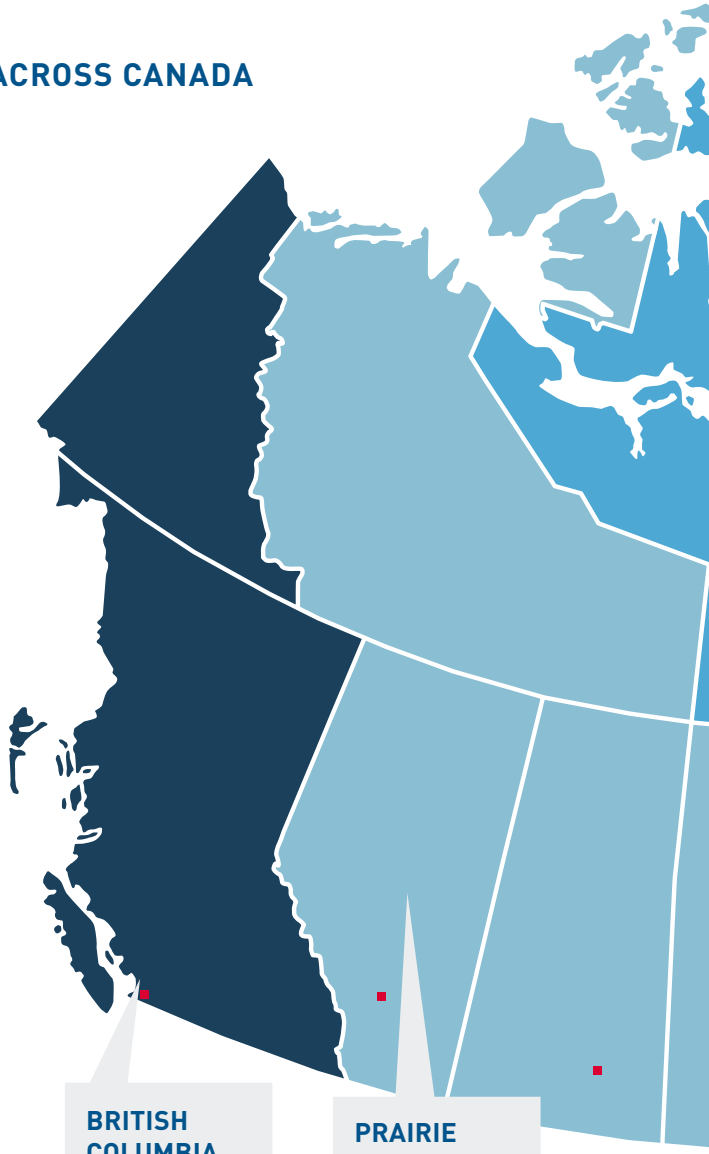
REQUESTS RECEIVED*	2018–2019
Federal Government Departments	74,900
Free and Secure Trade (FAST)	17,900
Transport Canada (Maine and Airport)	46,100
Parliamentary Precinct	2,900
Nuclear Facilities	10,000
Provinces	280
Others	3,300
Foreign Screening	490
Special Events Accreditation	12,500
TOTAL:	**168,370**

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

EXCELLENCE

OUR
PEOPLE

CSIS ACROSS CANADA



BRITISH COLUMBIA REGION

Burnaby, BC

PRAIRIE REGION

Edmonton, AB

▪ District Offices


QUEBEC REGION
Montreal, QC
TORONTO REGION
Toronto, ON
NHQ & OTTAWA REGION
Ottawa, ON
ATLANTIC REGION
Halifax, NS

THE CSIS PEOPLE STRATEGY

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

DEDICATED TO HEALTH AND WELLNESS

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

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

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

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

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

GBA+

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

RECRUITING FOR THE MISSION

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

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

CSIS WOMEN'S NETWORK

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

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

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


CONFIDENCE

ACCOUNTABILITY AND TRANSPARENCY

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

ACCOUNTABILITIES OF THE CSIS DIRECTOR

CSIS DIRECTOR

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

LEGAL

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

REVIEW

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

MANDATORY REPORTING

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

PARLIAMENT

CORE MANDATE

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

OFFICERS AND AGENTS OF PARLIAMENT

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

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

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

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

MINISTERIAL DIRECTION FOR ACCOUNTABILITY

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

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

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

THE *NATIONAL SECURITY ACT, 2017*

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

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

1. THREAT REDUCTION MEASURES

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

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

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

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

2. JUSTIFICATION FRAMEWORK

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

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

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

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

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

WHY DOES CSIS NEED TO ENGAGE IN OTHERWISE ILLEGAL ACTIVITY?

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

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

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

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

3. DATASET FRAMEWORK

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

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

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

NATIONAL SECURITY AND INTELLIGENCE REVIEW AGENCY (NSIRA)

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

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

THE *AVOIDING COMPLICITY IN MISTREATMENT BY FOREIGN ENTITIES ACT*

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

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

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

TRANSPARENCY

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

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

ACADEMIC OUTREACH AND STAKEHOLDER ENGAGEMENT

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

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

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

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

FOREIGN AND DOMESTIC

COOPERATION

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

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

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

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

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

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

2020 AND BEYOND:
MODERNIZING CSIS' AUTHORITIES

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

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

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

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

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