



Canadian Security
Intelligence Service

Service canadien du
renseignement de sécurité



CSIS Public Report

20
21



Canada

ISSN : 1495-0138

Catalogue number : PS71E-PDF

Aussi disponible en français sous le titre : Rapport public du SCRS 2021

www.canada.ca

Published in March 2022

© Her Majesty the Queen in Right of Canada, as represented by the Minister of Public Safety, 2022



CSIS Public Report

20 21

The Canadian Security Intelligence Service acknowledges that its 2021 Public Report was written and published on the traditional unceded territory of the Algonquin Anishinaabeg People.

1.	MESSAGE FROM THE DIRECTOR OF CSIS	6
2.	CSIS AT A GLANCE	11
3.	THREATS TO CANADA'S NATIONAL SECURITY	15
	The COVID-19 Pandemic	16
	Foreign Interference and Espionage	16
	Election Security	20
	Economic Security	21
	Cyber Threats	22
	Counter Proliferation	23
	Ideologically Motivated Violent Extremism (IMVE)	24
	Politically Motivated Violent Extremism (PMVE)	24
	Religiously Motivated Violent Extremism (RMVE)	25
	Canadian Extremist Travellers	25
	International Terrorism	26
	Security Screening	27

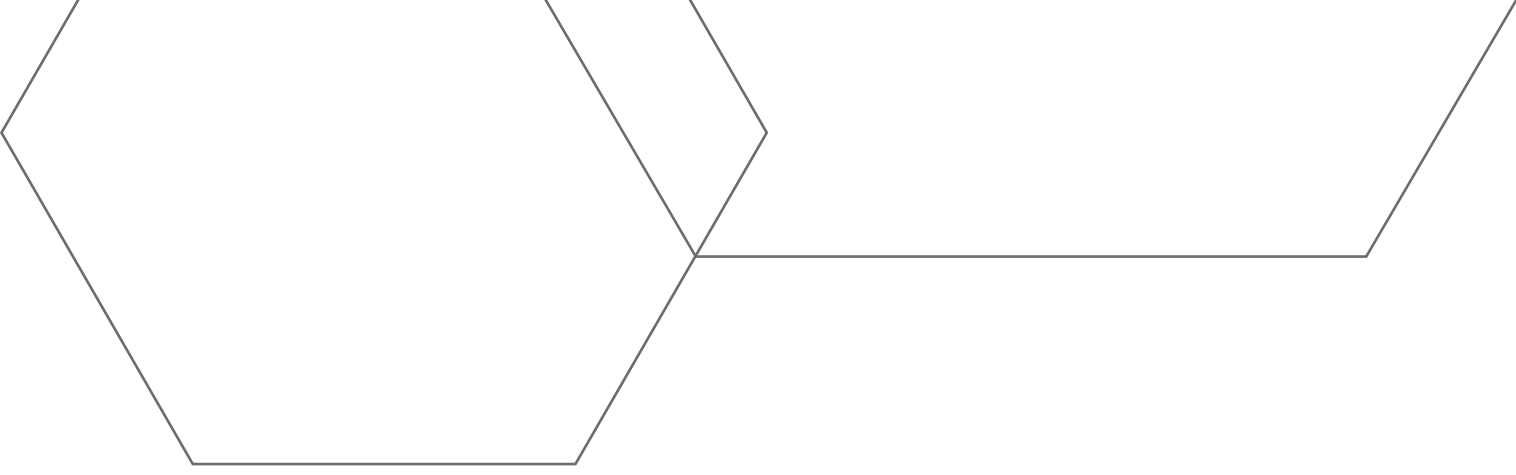
4.	WORKING WITH CANADIANS	29
	Connecting with Communities	30
	Communicating with Canadians	31
	Protecting Canadian Research and Interests	32
	Listening to Experts	33
	Transparency	34
	Review and Compliance	35
5.	THE PEOPLE OF CSIS	37
	Employee Demographics	38
	Communities within CSIS	40
	Diversity and Inclusion Initiatives	40
	Health and Safety	42
	The Future of Work	42
6.	INTELLIGENCE IN A DIGITAL ERA	43
	CSIS's Role in Cyber Security	44
	Modernizing Authorities	45
7.	CSIS'S 2021	47



“

I am pleased to present CSIS's 2021 Public Report. The period of review covered by this report was one of constant evolution and change. Many of the challenges we faced in 2021 continue today.

”



The continued impact of the COVID-19 pandemic has reinforced the unpredictability of the current environment. Geopolitical, societal, environmental and technological changes are reshaping the world around us at a dizzying pace. People everywhere are contending with the human, social and global implications of these transformations.

We continue to see uncertainty regarding the global balance of influence, with shifting power structures posing new and complex challenges to the international rules based order. While it does not fall under the period of review covered by this report, the Russian Federation's invasion of Ukraine in February of this year is one telling example.

In 2021 and today, we continue to see the spread of misinformation and disinformation propagated by both state and non-state actors. This type of information manipulation can have serious consequences – eroding trust in our democratic institutions, polarizing public opinion, and amplifying conflicting narratives and messaging. Unfortunately, we have seen firsthand the impacts this phenomenon can have in our own society with the demonstrations that took place across our country earlier this year, including in Ottawa.

The exponential rate of technological change and our hyper-connected society only exacerbates these challenges. Technology may be the most disruptive force shaping our world today. States, corporations and societies are grappling with how to handle these changes, which are deepening existing global inequities and becoming the focus of global competition.

So how does all this relate to our national security?

Together, these trends demonstrate two important truths. First, to be successful in this dynamic world, a robust and ongoing discussion of national security is essential. Second, our domestic and international security is interconnected; security threats do not stop at the border.

In 2021, the key national security threats facing Canada –foreign interference, espionage, malicious cyber activity, and violent extremism – all accelerated and evolved.

While the threats of espionage and foreign interference are not new, CSIS has observed these threats increase in scale, scope and complexity. In 2021, multiple foreign states continued covert attempts to gather political, economic, and military information in Canada through targeted threat activities in support of their own strategic goals.



CSIS has also seen persistent targeting of specific communities in Canada by multiple foreign state actors, both in person and online. These activities, when undertaken in a clandestine or deceptive manner, or when they threaten our citizens, residents and institutions constitute a threat to Canada's security as well as the safety of Canadians. CSIS will continue to use the full extent of its mandated authorities to counter them and uphold Canada's security, interests and values.

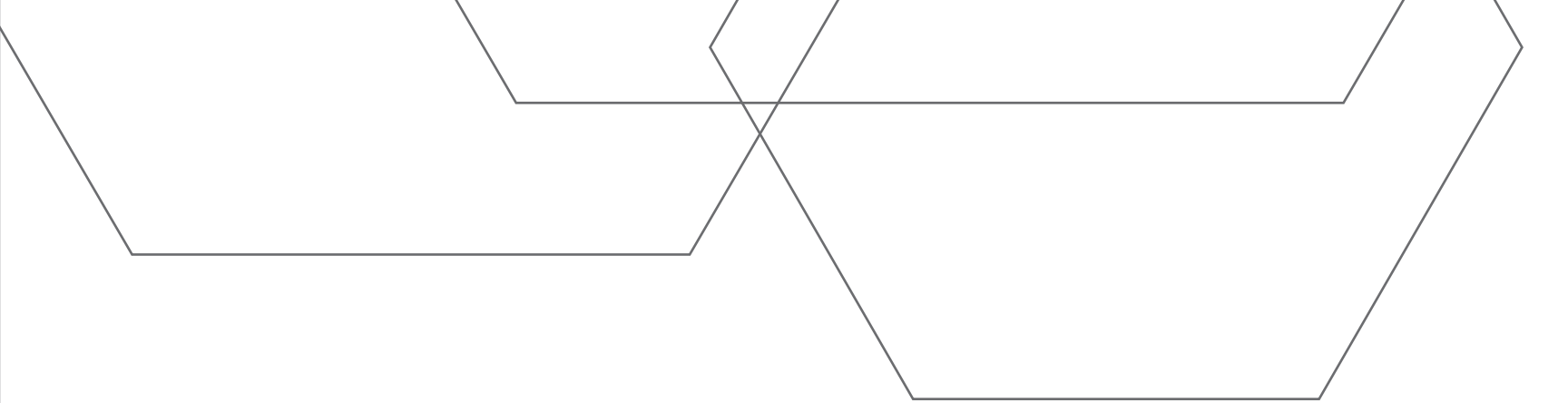
In addition, our country held its 44th Federal Election in 2021. CSIS provided operational support to the Security and Intelligence Threats to Elections (SITE) Task Force, a government wide team of security and intelligence experts leveraging their diverse mandates to mitigate threats to Canada's electoral process. As part of the SITE Task Force CSIS regularly briefed the Panel of non-partisan senior civil servants who administer the Critical Election Incident Public Protocol.

2021 also marked the most significant increase in CSIS's engagement through external stakeholder outreach, public speeches and Parliamentary committee appearances. It included outreach to the public and private sector, academia, human rights advocacy groups and a number of community groups and organizations with a concerted focus on the threat of violent extremism.

The Ideologically Motivated Violent Extremism (IMVE) landscape in Canada remains complex and constantly evolving. In 2021, the Government of Canada added four IMVE groups to its terrorist listings regime and we continue to see an increase in IMVE attacks in Canada and around the world.

Lone actors remain the primary IMVE threat, as demonstrated by the tragic June 2021 attack in London, Ontario. In this instance, the perpetrator was charged with four counts of first-degree murder, one count of attempted murder, and with terrorism offences under the provisions of the Criminal Code of Canada.

Canada also continues to face the threat of Religiously Motivated Violent Extremism (RMVE). Similar to IMVE, the primary RMVE threat comes from individuals acting alone, often inspired online by groups such as Daesh or Al Qaeda. The fall of Afghanistan to the Taliban in August 2021 has also served as inspiration for some RMVE actors while simultaneously creating a humanitarian crisis in that country. CSIS played an important role in providing security-screening assessments to the Government of Canada regarding the immigration of at-risk and vulnerable Afghan nationals with a link to Canada.



2021 also marked the 20th anniversary of the terrorist attacks of September 11, 2001 which killed nearly 3000 people, including 24 Canadians. At CSIS, we noted this occasion with solemn remembrance and renewed resolve.

The people of CSIS work hard everyday to understand and counter these threats to deliver on our mission of advancing Canada's prosperity, the safety of Canadians, and other national interests. To that end, CSIS provides trusted intelligence, advice, and action. In 2021, CSIS continued to investigate threats to our national security, advise the Government of Canada and reduce threat activities through our lawful mandate to ensure we remain safe.

Our unique mandate required many of our employees to work in the office throughout the pandemic while following strict public health guidelines. I am grateful to each one of them for their personal and professional dedication.

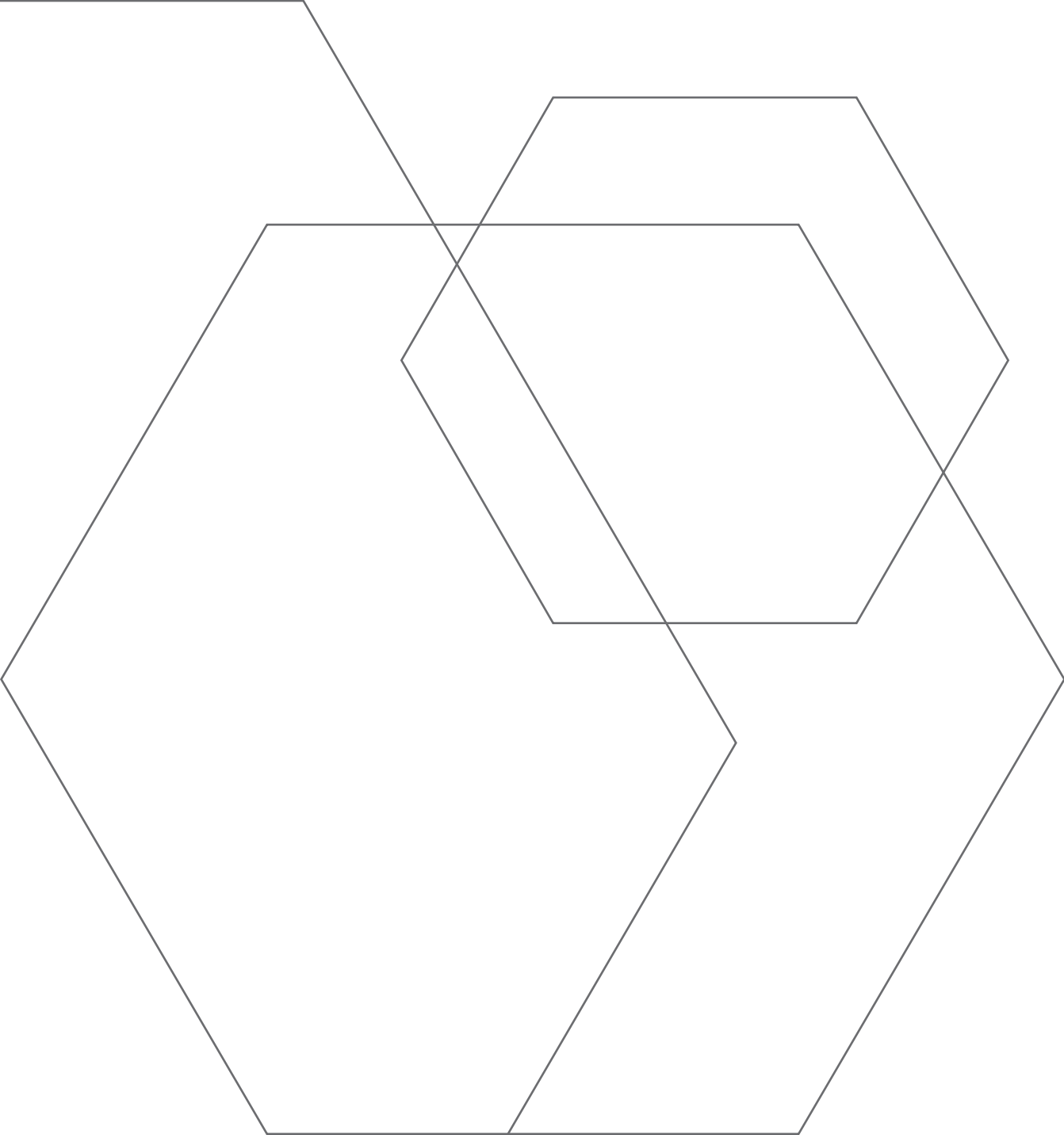
Like all organizations, CSIS has been impacted by a confluence of factors that challenge our conceptions of the nature of work and the workforce. Given CSIS's unique mission and high security requirements, our national headquarters, domestic regional offices and foreign stations remained operational throughout 2021. While this allowed CSIS to deliver on its critical mission it also raised new complexities. The pandemic has also accelerated emergent trends of digitization, remote work, and automation. These changes will have downstream impacts on the nature of education, training, recruitment, retention, and career progression and compensation. I have directed my Executive to launch an employee-driven initiative aimed at transforming our workforce to meet these new realities.

As Director, I am also personally committed to ensuring that CSIS's workplace is free of discrimination, bias, harassment and aggression. All CSIS employees deserve to come to work every day in a safe, healthy and respectful environment where diversity and inclusion are highly valued. CSIS continues to develop and implement new strategies and approaches to reverse and eliminate systemic barriers and broaden the organization's understanding and appreciation of all types of diversity. This work requires the commitment and input of every individual to improve our systems and culture.

While 2021 presented significant challenges that required CSIS to adapt, the devoted and effective efforts of our people have instilled me with great pride. All Canadians should be similarly proud of this service.



DAVID VIGNEAULT
DIRECTOR, CANADIAN SECURITY INTELLIGENCE SERVICE





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

Partnerships

Nearly
80
arrangements with domestic partners



Over
300
arrangements with foreign partners in 150 countries and territories

Accountability

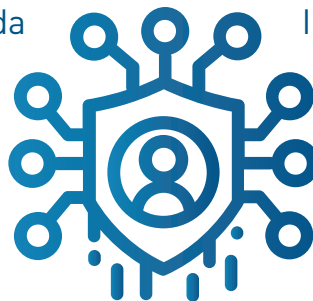
National Security and Intelligence Review Agency

Attorney General of Canada

Federal Court

Minister of Public Safety

Canadian Public



Intelligence Commissioner

Auditor General

Privacy Commissioner

Information Commissioner

National Security and Intelligence Committee of Parliamentarians

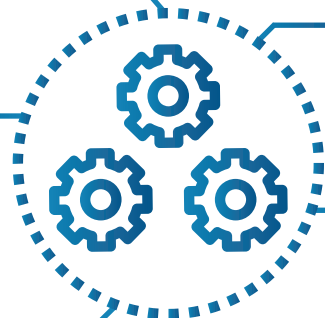
Commissioner of Official Languages

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 of these threats 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

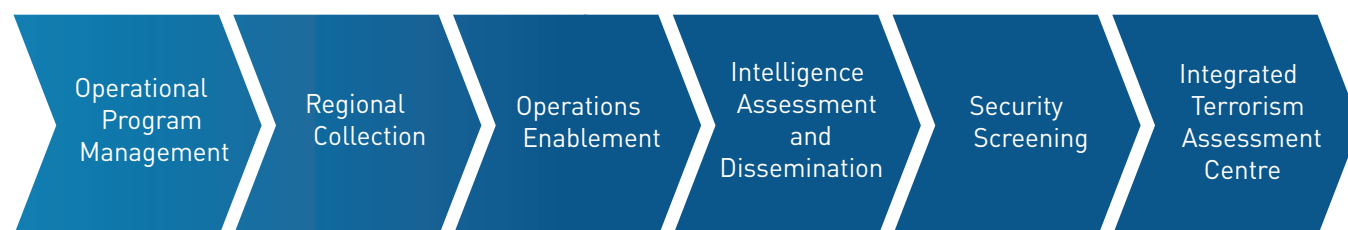
CSIS obtains relevant information and intelligence to carry out its national security activities.

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 inform the Government of Canada's decisions and actions relating to the terrorism threat.

Program Inventory



Actual Expenditures

	2017-2018	2018-2019	2019-2020	2020-2021
Salaries	383,260,577	376,043,621	372,348,794	417,615,370
Operating	203,738,376	210,564,334	238,736,299	259,284,331
Total	586,998,953	586,607,955	611,085,093	676,899,701



Threats to
**CANADA'S
NATIONAL
SECURITY**

The COVID-19 Pandemic

The pandemic reinforced the importance of whole of government responses during periods of emergency. Experts from Canada's security and intelligence community worked closely with the Public Health Agency of Canada (PHAC), Health Canada, Public Services and Procurement Canada (PSPC), the Treasury Board Secretariat (TBS), the Canadian Armed Forces and others to support Government of Canada efforts to respond to the pandemic.

Throughout the pandemic CSIS observed persistent and sophisticated state-sponsored threat activity, including harm to individual Canadian companies, as well as the mounting toll on Canada's vital assets and knowledge-based economy.

As a result, CSIS is working closely with government partners to ensure that as many Canadian businesses and different levels of government as possible are aware of the threat environment and that they have the information they need to implement pre-emptive security measures. CSIS's outreach to organisations including supply chain associations and other related industry groups on the risks associated with logistics supply networks is a good example of how CSIS is reaching out to non-traditional stakeholders to ensure Canadians remain safe and Canadian interests are protected from threats.

CSIS will continue to work closely with other members of Canada's security and intelligence community, as well as allied partners to help protect Canada's pandemic response and targeted sectors from potential national security threats.

Foreign Interference and Espionage

As a core part of its mandate, CSIS investigates and advises the Government of Canada on threats posed by espionage and foreign influenced activities. The CSIS Act defines foreign influenced activities as activities that are "detrimental to the interests of Canada and are clandestine or deceptive, or involve a threat to any person." These activities are also commonly referred to as foreign interference, and are almost always conducted to further the interests of a foreign state, to Canada's detriment. Foreign interference is directed at Canadians, both inside and outside Canada and may be undertaken with the use of state or non-state entities, and can include the use of proxies and co-optees.

Foreign interference activities in Canada continue to be sophisticated, persistent, and pervasive. Active targets of these activities include institutions at all levels of government as well as private sector organizations, civil society groups, and Canadian communities. Foreign interference undermines Canada's democratic institutions and the intimidation or coercion of communities in Canada by hostile state actors constitutes a threat to Canada's social cohesion, sovereignty, and national security. In July 2021, CSIS issued a public report entitled "[Foreign Interference: Threats to Canada's Democratic Process](#)" as part of ongoing efforts to protect democratic institutions and processes and to increase awareness among Canadians on this important threat. Foreign interference directed at Canada's democratic institutions and processes, at all levels of government, can be an effective way for a foreign state to achieve its immediate, medium, and long term strategic objectives. As the world has become smaller and more competitive, foreign states seek to leverage all elements of state power to advance their own national interests and position themselves in a rapidly evolving geopolitical environment.

Foreign Interference Techniques used by Foreign State Actors



Elicitation: manipulating someone into sharing valuable and sensitive information through conversation



Illicit and Corrupt Financing: using someone as a proxy to conduct illicit or corrupt financing on their behalf



Cultivation: building a strong friendship or relationship with someone to manipulate them into providing favours and valuable information



Cyber Attacks: compromising electronic devices through various means including socially-engineered emails like spear-phishing, ransomware, and malware



Coercion: blackmailing or threatening someone to provide valuable and sensitive information or access



Disinformation: spreading false information on social media to amplify a particular message or provoke users to serve their own interests

During 2021, hostile activities by state actors in Canada continued to be affected by the COVID-19 pandemic. With public health restrictions in place, state actors in Canada were forced to curtail some activities, however, many adapted their techniques and methods to fit the new normal. Since March 2020, CSIS has observed increased disinformation and influence activities via social media and online platforms, with exploitation of the COVID-19 pandemic forming part of disinformation campaigns supported by hostile state actors.

Hostile intelligence services continue to target Canadians for intelligence collection and asset recruitment. As an example, in addition to traditional espionage operations, the People’s Republic of China (PRC) relies on non-traditional collectors- individuals without formal intelligence training who have relevant subject matter expertise (i.e. scientists, business people), including those who are recruited via talent programs (i.e. scholarships, sponsored trips, visiting professorships, etc.) and other non-transparent means in Canada. While the PRC’s Thousand Talents Plan (TTP) is one example, academic talent plans are used by multiple states. These state-sponsored technological transfer activities exploit the collaborative, transparent, and open nature of Canada’s government, private sector and society. Other foreign interference activities include cultivating and coopting influential people to sway decision-making and control narratives on issues of interest to certain states.

State-sponsored disinformation campaigns represent one of many vectors of foreign interference and hostile states have been involved in actively spreading disinformation in an effort to discredit our government institutions, negatively impact social cohesion and gain influence for their own strategic objectives.

CSIS has also been aware of several Russian military and intelligence entities that are engaged in information confrontations targeting Ukraine. These activities include the spread of disinformation and propaganda attempting to paint Ukraine and NATO as the aggressors in the current conflict. Such measures are intended to influence Western countries into believing Ukraine has provoked a global conflict.

In addition, hostile states actors also continue to monitor and intimidate Canadian communities, with diaspora communities often disproportionately targeted. The tactics and tools used for such purposes include cyber espionage via social media platforms and threats designed to silence those who speak out publicly against them.

On January 8, 2020, Iran’s Islamic Revolutionary Guard Corps (IRGC) shot down Ukraine International Airlines Flight PS752 near Tehran, killing all 176 passengers and crew onboard, including 55 Canadian citizens and 30 Canadian permanent residents. Since then, CSIS has supported Government of Canada initiatives on this priority file, including the [Canadian forensic team final report](#) issued on June 24, 2021. CSIS continues to investigate credible reports of several Canada-based relatives of Flight PS752 victims having experienced harassment and intimidation from threat actors linked to proxies of the Islamic Republic of Iran. This activity may constitute foreign interference.

CSIS will continue to investigate and identify the threats that espionage and foreign interference pose to Canada’s national interests, and will work closely with domestic and international partners to address them. To report espionage and foreign interference, CSIS encourages individuals to call +1-800-267-7685 or visit Canada.ca/CSIS and click on the “[Reporting National Security Information](#)” section. If the person is in immediate danger, they should phone their local police of jurisdiction.

REPORT FOREIGN INTERFERENCE



1-800-267-7685



Canada.ca/CSIS

To report immediate threats, call your local police.

The Security and Intelligence Threats to Elections Task Force (SITE TF) is a whole-of-government working group that coordinates Government of Canada collection and analysis efforts concerning threats to Canada's federal election processes. It consists of experts from CSIS, the Royal Canadian Mounted Police (RCMP), Global Affairs Canada, and the Communications Security Establishment (CSE).

Formed in 2019 in response to greater awareness of the threat of foreign interference by hostile state actors during democratic processes, the SITE TF is Canada's principal mechanism to monitor the threat from hostile state interference during elections. It also sets conditions for the Government of Canada to inform the public of the threat or mitigate the threat as appropriate.

In 2021, the SITE TF hosted its first ever whole-of-government conference on electoral security at CSIS National Headquarters. This conference served to inform officials engaged in delivering a free and fair election to Canadians on the threats associated with foreign interference, as well as from IMVE actors who viewed the election as an opportunity to discourage Canadians from democratic participation or to plan acts of violence. This conference set the stage for further work among agencies, which included:

- Regular security intelligence briefings to key senior government decision makers and political party representatives;
- Increased reporting and transparency on electoral security matters through interagency personnel exchanges; and
- Reviewing and conducting appropriate measures to reduce the threat from specific hostile state proxies or agents;
- Assessing sources of disinformation (defined as entities that wittingly publish false information to deliberately mislead Canadians).

In a world marked by geostrategic economic competition and confrontation, state-sponsored threat actors seek to advance their strategic political, economic and military objectives by exploiting investment and trade with Canada. Foreign states seek to acquire access or control over sensitive technologies, data, and critical infrastructure to advance their own military and intelligence capabilities, deprive Canada of access to economic gains, employ economic coercion against Canada, and support other intelligence operations against Canadians and Canadian interests. Such activities pose a threat to Canada's national security and long-term economic prosperity.

Investigating and assessing the use of economic activities by hostile state actors is a priority for CSIS. Throughout the COVID-19 pandemic, foreign threat actors continued to exploit the prevailing social and economic conditions to advance their interests. Threat actors continue to attempt to access valuable Canadian information through the Four Gates of Economic Security: imports and exports; investments; knowledge; and licenses. Specific threat activities include human and cyber espionage; malign foreign investment; manipulation of imports and exports; exploitation of licenses and rights; and espionage against public academic institutions and private research and development.

In 2021, CSIS supported the Government of Canada's implementation of Canada's research security enterprise. This effort seeks to ensure Canadian resources designated for academic research are properly used to advance Canada's scientific leadership and economic prosperity and are not co-opted by foreign states to obtain military, intelligence, and economic benefits at the expense of Canadian interests and values.

In the context of COVID-19, CSIS has also provided additional national security scrutiny to investments related to public health and threats to the supply of critical goods and services.

Canada remains a target for malicious cyber-enabled espionage, sabotage, foreign influence, and terrorism related activities, which pose significant threats to Canada's national security, its interests and its economic stability. Cyber actors conduct malicious activities to advance their political, economic, military, security, and ideological interests. They seek to compromise government and private sector computer systems by manipulating their users or exploiting security vulnerabilities.

Advanced cyber tools developed and sold by commercial firms are giving new collection capabilities to countries and foreign state actors that historically have not posed a significant threat in the cyber domain. The services offered by these companies can have both defensive and offensive applications. These tools enable a growing list of actors to conduct espionage, sabotage, endanger civilians, undermine democratic values and exert foreign influence. Open-source reporting suggests that multiple authoritarian regimes have used such tools to target lawyers, journalists, politicians, and human rights defenders.

The COVID-19 pandemic has accelerated the digitization of society. This has increased both avenues for cyber espionage and risks from disruption. Work from home arrangements in the private and public sectors have dramatically increased – and so has the amount of sensitive information available for targeting and collection by hostile state actors. Malicious cyber actors can leverage compromised private devices and networks, which often lack advanced cybersecurity protections.

Cyber actors linked to the People's Republic of China (PRC) continue to target multiple critical sectors within Canada. In 2021, PRC state-sponsored actors engaged in the indiscriminate exploitation of Microsoft Exchange servers, putting several thousand Canadian entities at risk. Victims included governments, policy think tanks, academic institutions, infectious disease researchers, law firms, defense contractors, and retailers.

Russian cyber actors also remain a threat to Canada. In April 2021, Canada and its allies publicly attributed a cyber espionage campaign to the Russian Foreign Intelligence Service (SVR). This campaign involved inserting malware into a software update mechanism for a network management tool published by US technology firm SolarWinds. This allowed the cyber actor to install backdoors into the networks of thousands of government and private sector clients. Hundreds of Canadian entities downloaded an infected version of the software, putting personal data and intellectual property at risk.

Ransomware attacks represent yet another national security threat in the cyber domain. These attacks involve a type of malware that threatens to publish the victim's data or block access to it unless a ransom is paid. State actors increasingly use these cybercriminal tactics, often through proxies, to advance their objectives and evade attribution. By harvesting large quantities of victim data, ransomware attacks can further benefit foreign state actors keen on amassing data to enhance their intelligence collection efforts. When ransomware attacks cause severe disruption, foreign state actors can also benefit from the resulting chaos as it may bolster their ideological narratives.

Counter Proliferation

The proliferation of chemical, biological, radiological and nuclear (CBRN) weapons, commonly referred to as weapons of mass destruction (WMD), and their associated delivery vehicles constitutes a global challenge and a significant threat to the security of Canada and its allies. The proliferation of CBRN weapons systems undermines the rules-based international order, contributes to increased international tensions and may even precipitate armed conflicts in some parts of the world.

Several foreign states continue clandestine efforts to procure a range of sensitive, restricted, and dual-use goods and technologies in Canada, as well as expertise they may use to further their own WMD programs and delivery vehicles. CSIS continues to work closely with domestic and foreign partners to uphold the Government of Canada's commitment to counter-proliferation. This entails efforts to detect, investigate, prevent, and disrupt activities in or through Canada involving the illicit acquisition, export, or diversion of goods that may enable WMD programs. These efforts also extend to intangible technology transfers.

Ideologically Motivated Violent Extremism

Ideologically motivated violent extremism (IMVE) represents a societal issue requiring a whole-of-government approach. The IMVE threat is complex and constantly evolving and is fuelled by proponents that are driven by a range of influences rather than a singular belief system. Extreme racist, misogynistic and anti-authority views combined with personal grievances can result in an individual's willingness to incite, enable or mobilize to violence. CSIS plays a key role, alongside other intelligence and law enforcement partners, in a broader government response to this threat.

In 2021, CSIS led a government-wide project to improve understanding of the complex and evolving IMVE threat landscape in Canada. This project, which followed work CSIS previously conducted on violent extremism terminology, aimed to develop cross-government understanding of the analytical process used by CSIS in identifying, assessing, and where appropriate, acting on IMVE threat activity.

There have been seven attacks and three disrupted plots in the Canadian IMVE space since 2014. These attacks have killed 26 people and wounded 40 others on Canadian soil —more than any other form of violent extremism. Most recently, in June 2021, an attack in London, Ontario killed four individuals and injured one. In October 2021, a former Canadian Armed Forces reservist was sentenced to nine years in a US prison for plotting serious violence with members of The Base, a neo-Nazi group that is a listed terrorist entity in Canada.

A range of grievances motivates IMVE actors' willingness to incite, enable, and/or mobilize to violence. Not all of these instances meet a national security threshold, but CSIS has observed a marked increase in violent threats to elected officials and government representatives during the past two years.

Since the beginning of the COVID-19 pandemic, IMVE activity has been fueled by an increase in extreme anti-authority and anti-government rhetoric often rooted in the weaponization of conspiracy theories. A number of Canadian influencers and proselytizers have emerged within IMVE movements. These IMVE influencers promote misinformation and action, including violence.

Politically Motivated Violent Extremism

Politically motivated violent extremism (PMVE) encourages the use of violence to establish new political systems, or new structures and norms within existing systems. There were no PMVE-related attacks in Canada in 2021.

Religiously Motivated Violent Extremism

Religiously motivated violent extremism (RMVE) encourages violence as part of a spiritual struggle against perceived immorality. Adherents believe that salvation can only be achieved through violence. RMVE violence attempts to intimidate or compel a desired action, or to restrain a government from taking an action. RMVE actors can target both the public and the government, domestically and abroad. RMVE actors will also target infrastructure as a way of achieving their goals, such as attacking power plants, hospitals, communication networks and electrical grids.

In 2021, two key events occurred in the global RMVE space. The first was the 20th anniversary of the terror attacks of September 11, 2001. The second was the Taliban takeover of Afghanistan in August 2021. The anniversary of 9/11 is a strangely unifying event for RMVE actors. Daesh supporters, who are often anti-Al Qaeda in their rhetoric, viewed the anniversary of 9/11 as a moment to celebrate. Conversely, the fall of Afghanistan was a divisive occasion, with Daesh leaders and supporters regularly encouraging and promoting attacks against the Taliban.

No RMVE inspired attacks occurred in Canada during 2021. Nonetheless, RMVE propaganda and certain threat-related activities continued. The ongoing threat of RMVE in Canada comes primarily from Daesh-inspired lone actors, who have the potential to mobilize to violence quickly, using low-tech means to take action against soft targets. For these lone actors, there is no known or identifiable form of direction or logistical support from Daesh. The Daesh supporters therefore rely predominantly on personal savings in their threat-related activities and their financial contributions to Daesh-affiliated individuals abroad are personal and small. These contributions are often one of the first triggers of an investigation.

Canadian Extremist Travellers

The Government of Canada has continued to monitor and respond to the threat of Canadian extremist travellers (CETs). CETs are individuals with a nexus to Canada through citizenship, permanent residency, or a valid visa, who are suspected of having travelled abroad to engage in terrorism-related activities. These individuals may leave Canada to support, facilitate, or participate in violent extremist activities. CETs pose a wide range of security concerns, both while abroad and if they return to Canada. Broadly speaking, CETs have affiliations with multiple violent extremist groups and movements, and may represent IMVE, politically motivated violent extremism (PMVE), and/or RMVE perspectives.

Since 2011, conflict in Syria and Iraq has attracted unprecedented numbers of extremists to fight overseas. However, since the collapse of Daesh's territorial Caliphate in Iraq/Syria in 2016-2017, many of these individuals have been killed or are detained in internally displaced persons (IDP) camps or prisons in Syria. The global return of foreign terrorist fighters to countries where they may face varying degrees of justice represents a challenge to counterterrorism efforts.

On August 15th, 2021, the Taliban captured Afghanistan's capital of Kabul and thus became the *de facto* governing body of the country. The takeover was swift and chaotic, leaving the international community limited time to evacuate personnel. The Taliban face significant challenges governing Afghanistan, including an economic and humanitarian crisis that will likely continue throughout 2022.

The Taliban have continued to allow transnational terrorist groups, such as Al Qaeda and Al Qaeda in the Indian Subcontinent (AQIS), to remain in country. While their current activities are limited, there is a possibility that Al Qaeda will once again view Afghanistan as a safe training ground. Meanwhile, the Daesh-affiliated Islamic State Khorasan Province (ISKP) has sought to delegitimize the Taliban's governance by conducting attacks targeting urban areas. CSIS assesses that ISKP will have the capacity to conduct external attacks within the near future and are highly motivated to do so.

In 2021, Daesh remained focused on insurgency in Iraq and Syria. Daesh insurgencies tend to target local security forces and local leaders able to counter its influence. In Iraq, Daesh has also begun to attack economic targets such as electrical infrastructure to undermine public confidence in the government. Daesh shows no indications of being in a position to capture and hold the territory it lost in 2019. However, it retains this aim as a long-term goal, raising the possibility of a future reincorporation of foreign extremists including CETs. Daesh also aims to assault prisons and incite prison riots in Iraq and Syria as part of its jihadi operational strategy based on force regeneration, freeing high-value individuals, and propaganda. CSIS assesses that Daesh will continue to attempt to inspire and enable attacks in Western countries while it gradually rebuilds its direct attack capabilities.

RMVE continues to threaten Canadians and Canadian interests in Africa. Canadians who work or travel near regions where terrorist groups operate continue to face significant threat from both attacks and opportunistic kidnap-for-ransom operations. Al Qaeda-aligned Al-Shabaab and Jamaat Nusrat al-Islam Wal Muslimin (JNIM) are the main terrorist groups in the Horn of Africa and West Africa, respectively. These Al Qaeda affiliates will likely seek to use the Taliban's victory in Afghanistan to motivate current fighters and drive recruitment; however, neither Al-Shabaab nor JNIM has the intent to replace African state governments. Daesh affiliates have also demonstrated increased activities and operational reach, particularly in Sub-Saharan Africa.

Security Screening

Through its Government Security Screening (GSS), and Immigration and Citizenship Screening (ICS) programs, CSIS serves as the first line of defence against violent extremism, espionage, and other threats to national security.

The CSIS GSS program conducts investigations and provides security assessments and advice on a wide range of threats to national security in the context of security clearances. Security assessments are part of an overall evaluation to assist federal government departments and agencies deciding to grant, deny, or revoke security clearances. These decisions lie with each department or agency, and not with CSIS.

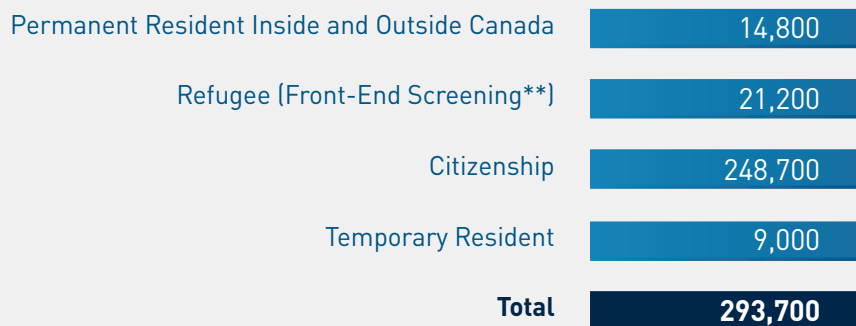
The GSS also conducts screening to protect sensitive sites – including airports, marine, and nuclear facilities – from national security threats. Furthermore, it assists the RCMP in vetting Canadians and foreign nationals who seek to participate in major events in Canada. Finally, the GSS provides security assessments to provincial and 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 do so voluntarily.

The CSIS 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 who are seeking entry to or status in Canada. Through this program, CSIS provides security advice on permanent resident and citizenship applicants; persons applying for temporary resident visas; and persons applying for refugee status in Canada. Decisions related to admissibility to Canada, the granting of visas, or the acceptance of applications for refugee status, permanent residence, and citizenship rest with IRCC.

In response to the withdrawal of allied military personnel from Afghanistan, and the Taliban takeover of Afghanistan in the summer of 2021, CSIS supported Government of Canada efforts to urgently evacuate and resettle at-risk and vulnerable Afghans with links to Canada. With the Government of Canada's decision to resettle 40,000 Afghans to Canada, CSIS's security screening and security advice will remain critical.

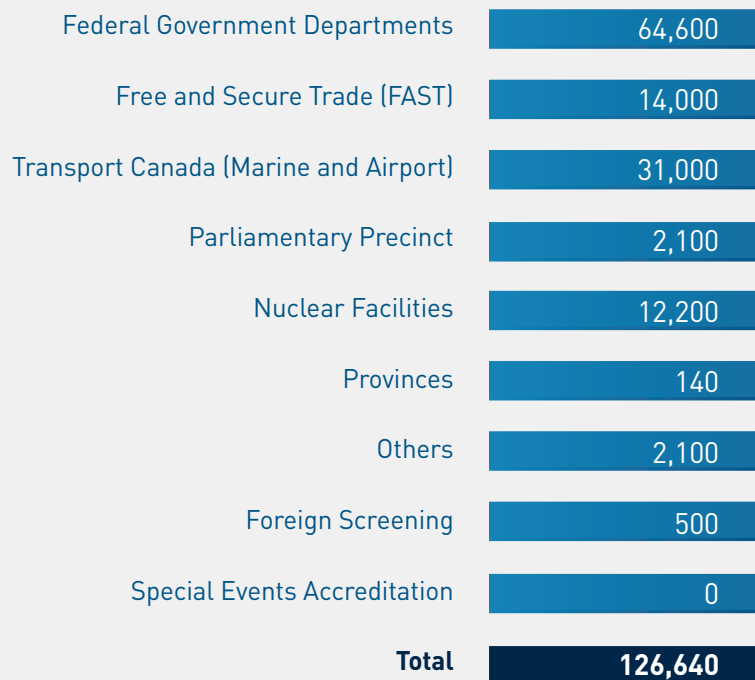
Immigration and Citizenship Screening Programs

Requests Received* in 2021



Government Screening Programs

Requests Received* in 2021



Figures have been rounded.

* The pandemic has caused a reduction of cases received in 2021.

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



Working with
CANADIANS

Connecting with Communities

At its core, national security is about protecting people. National security work requires the trust and help of the Canadian public. CSIS interacts with Canadians to engage with communities who may be targeted by threat actors, to seek different insights and perspectives, to provide important security information, and to inform national security investigations. After all, we all have a role to play in protecting our national security.

CSIS continues to engage with community leaders, members, and advocacy groups to offer support and solidarity and to reinforce the Government of Canada's position that there is no place in Canada for racial prejudice, discrimination and hate. These ongoing discussions also provide an opportunity to affirm CSIS's commitment to ensure the safety and security of all Canadians and to seek input on how CSIS can build trust with marginalized and diverse communities. Further to these efforts, CSIS has sought advice on best practices to ensure its external engagement reflects intersectional considerations and is sensitive to bias, discrimination, and inequity.

In 2021, CSIS engaged with self-identified representatives of Asian Canadian, Muslim Canadian, as well as Black, Indigenous, and People of Colour (BIPOC) communities. In addition, CSIS engaged with anti-racism and counter-radicalization groups as well as those focused on addressing the social impacts of national security laws, policies and discourse on racialized communities. These efforts were aimed at listening, better understanding the communities that CSIS serves, establishing trusted relationships, and conveying threat-related information to increase awareness and resilience.

This foundational trust is imperative and will help CSIS to foster the relationships needed to better protect the communities most affected by threats, including from violent extremism, foreign interference and espionage. CSIS was recognized for its efforts in 2021 to build bridges and conduct meaningful engagement with racialized communities, which were highlighted as a best practice in the 2021 Annual Report of the Operations of the Canadian Multiculturalism Act.

As CSIS continues to grow and deepen partnerships with diverse communities, the knowledge shared by these partners will help inform how CSIS operates and, in turn, will help CSIS continue to earn the confidence and trust of Canadians and invite them to contribute directly to conversations around national security.

Communicating with all Canadians

The current Director of CSIS has often said that “keeping Canada safe requires a national-security literate population.” This imperative, of fostering and supporting informed dialogue about national security and intelligence issues, was reflected in CSIS’s external communications throughout 2021. The importance of open communication with Canadians pushed CSIS further out of the shadows of secrecy and into the public spotlight.

CSIS developed publicly available resources on foreign interference, which were published in a range of foreign languages in order to ensure that vulnerable communities can access threat information in their language of choice. In keeping with the organization’s commitment to transparency and supporting resilience, in advance of the Federal election, CSIS also published a report on [Foreign Threats to Canada’s Democratic Process](#).

Through briefings, public remarks and social media, CSIS continues to communicate that national security concerns about the activities of some foreign states are not to be interpreted as, or conflated with, concerns about the people associated with or whose families have immigrated to Canada from those states.

CSIS continues to seek out new ways of connecting and communicating with Canadians. In 2021, other avenues of communication included a [public speech](#) by the Director of CSIS at the Centre for International Governance Innovation; public briefings and appearances by senior executives at a range of public events, including before the National Security Transparency Advisory Group (NS-TAG); coordinating and publishing [Public Opinion Research](#) on CSIS and national security threats; and extensive social media campaigns to raise awareness on the threat environment.

CSIS on social media - 4 Platforms



Twitter

47,000

Twitter Followers



Facebook



YouTube



LinkedIn

1,950

Tweets to date

[@csiscanada](#)

[@scrsCanada](#)

Protecting Canadian Research and Interests

In 2021, CSIS continued to support Canada's research, health, and supply chain sectors' pandemic related efforts. With the release in July 2021 of the Government of Canada's [National Security Guidelines for Research Partnerships](#), CSIS's outreach and engagement focus shifted from the pandemic to research security. To help protect Canadian innovation, intellectual property, and the valuable data that support them, CSIS provided dozens of briefings in academic forums, to individual universities, and to research institutions, in support of the wider Government of Canada effort, led by Innovation, Science and Economic Development Canada (ISED), to implement the Guidelines. In addition to providing briefings, CSIS also developed supporting guidance materials, checklists, case studies and other materials which were included in the government's [Safeguarding Your Research](#) portal, including [province and territory-specific guidance on research security](#).

Related to these research security efforts, CSIS also engaged a number of associations and companies in the emerging and deep technology sectors. The aim of CSIS's engagement was to increase awareness of state-sponsored espionage threats targeting these sectors, and lay the groundwork for reciprocal partnerships that will help protect Canadian research and development and ensure Canadians and the Government of Canada have access to leading edge and trusted technology. This emerging technology sector is vibrant and growing, with research in areas as diverse as agri-tech, artificial intelligence, quantum, smart cities, and clean-tech.

CSIS also reached out to Canada's business and venture capital community as important partners in protecting economic security and advancing Canadian prosperity interests. Some of the industry associations and innovation leaders CSIS engaged with over the past year include: the MaRS Momentum Program, the Canadian Institute of Traffic and Transportation, Supply Chain Canada, the Canadian Association of Importers and Exporters, the Internet Society of Canada, the Canadian Association of Security Intelligence Studies, the Business Development Bank of Canada's Deep Tech Venture Fund, the Best Defence Conference, the Canadian Science Policy Conference, the Canada Foundation for Innovation, Community of Tech Transfer Professionals, and the International Intellectual Property Forum Québec.

Listening to Experts

As part of its core mandate of supporting and advising the Government of Canada, CSIS continued to draw upon external expertise, by curating and presenting timely insights on a wide range of topics to help inform and support broader government efforts to serve Canadians. To this end, in 2021, CSIS hosted 16 virtual expert briefings and produced 34 Commissioned Reports, which were shared across the Government of Canada and with other key partners. These briefings and reports covered a range of relevant topics, including ethical artificial intelligence, state-sponsored disinformation, ideologically motivated violent extremism and others. Working with non-governmental experts on prescient issues helped the Government, as a whole, to be both better equipped to respond to the concerns of Canadians, and to integrate Canadian expertise into government-wide operational and policy decision-making.

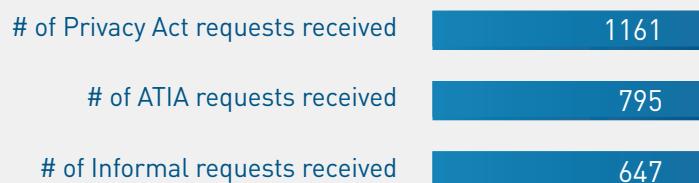
In addition to listening to academic experts, CSIS also worked to mentor students. For the second consecutive year, officials from CSIS mentored a cohort of graduate-level students at the School of Public Policy and Global Affairs at the University of British Columbia, conducting a year-long research project into subjects of relevance to national security. CSIS officials also participated in class and seminar discussions at universities across Canada to engage with students on national security-related issues.

The confidence of Canadians in national security efforts is fundamental to CSIS’s legitimacy, operational effectiveness, and institutional credibility. CSIS recognizes the importance of transparency within the national security community which includes open and clear communication with Canadians. Public communication, transparency and review together enable Canadians to trust their security intelligence service.

In 2021, CSIS continued its work with the National Security Transparency Advisory Group (NS-TAG). The advisory group, established in 2019, 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 information. In 2021, CSIS’s Director General for Academic Outreach and Stakeholder Engagement participated in one of NS-TAG’s meetings to discuss diversity and inclusion at CSIS and in the national security and intelligence community. The meeting highlighted the objectives of CSIS’s stakeholder engagement program, the progress made, and guiding principles for engagement, which include transparency, reciprocity, respect, listening, and learning. The meeting also included frank discussions about challenges encountered, and CSIS’s commitment to continue building foundational trust with various diverse communities.

CSIS’s Access to Information and Privacy (ATIP) branch also contributes to CSIS’s transparency efforts by balancing the public’s right of access to information with the legitimate need to protect sensitive national security information and maintain the effective functioning of government. The *Access to Information Act* (ATIA) and *Privacy Act* provide Canadians, as well as individuals and corporations present in Canada, the right to access federal government records. The CSIS ATIP branch regularly publishes information as part of proactive publication requirements in accordance with the ATIA, as well as summaries of recent ATIA releases to afford the public an opportunity to access previously released records. CSIS prides itself on providing excellent service and a proactive approach to promote transparency.

ATIP Stats for 2021



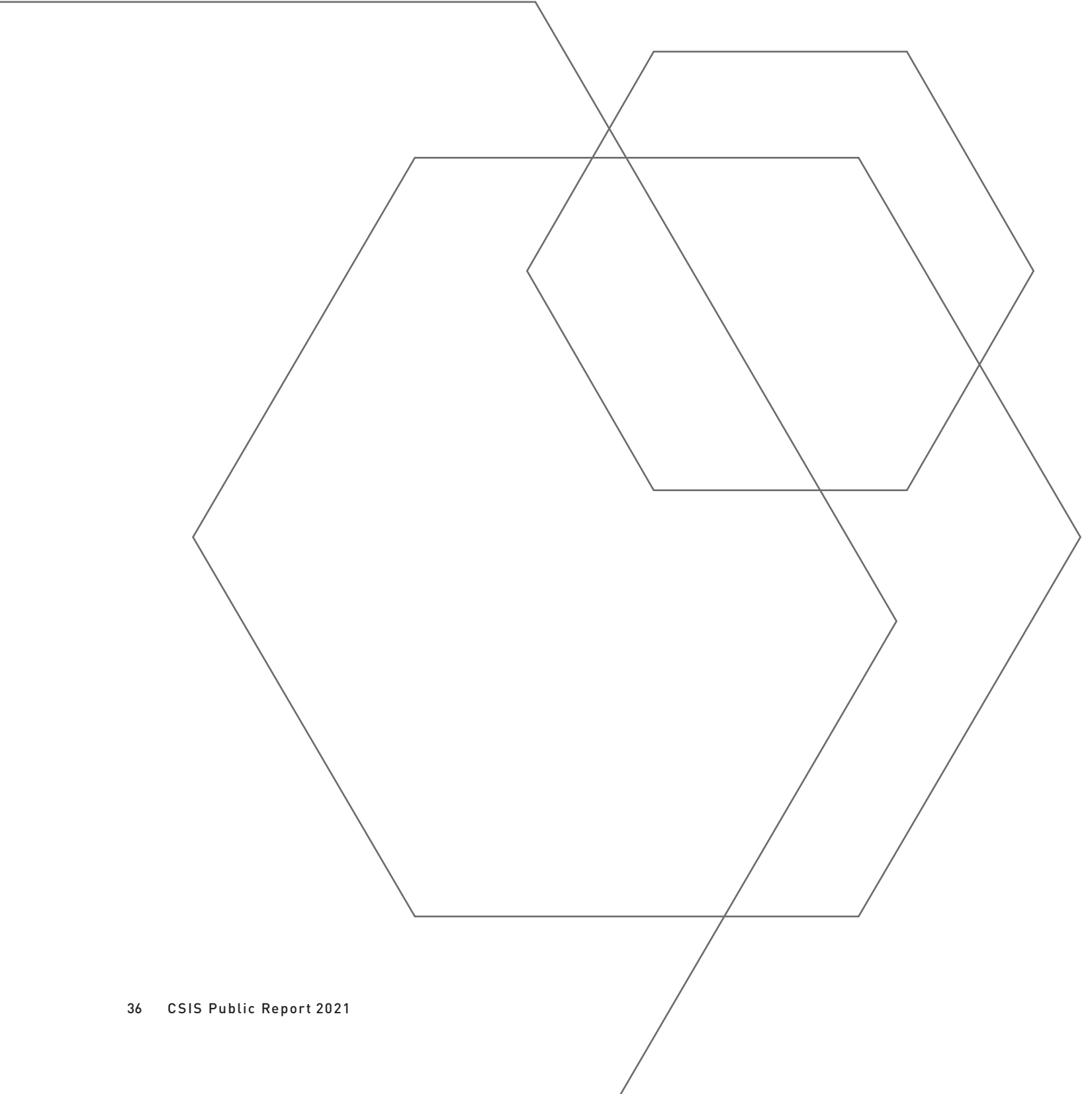
Review and Compliance

In 2021, CSIS continued to address compliance in line with its operational compliance program which was founded on a recognition that compliance is essential to maintaining the trust and confidence of the public, Parliament, the Federal Court, and review bodies. Compliance also supports CSIS's accountability and transparency requirements, as well as operational effectiveness.

Recent government commitments to enhance CSIS's compliance program were used in 2021 to make critical investments in CSIS's information technology infrastructure to support the process around warrants, designing an approach for reporting and assessing potential operational compliance incidents, embedding experts in operational branches to provide timely advice and guidance, and developing clear internal policies and procedures for employees.

In May 2020, the Federal Court issued a decision in which it found that institutional failings, by both CSIS and the department of Justice, led to a breach of CSIS's duty of candour to the Court in failing to proactively identify and disclose all relevant facts in support of warrant applications. The Court recommended a comprehensive external review of the policies and practices of the Department of Justice and CSIS in this area. In response, the Ministers of Public Safety and Justice referred the matter to the National Security and Intelligence Review Agency (NSIRA). Throughout 2021, CSIS actively supported the review process and welcomes the findings and recommendations of NSIRA. Internal efforts to improve processes, assisted by recommendations of a former Deputy Attorney General, were underway before NSIRA's review began. CSIS continues to demonstrate its commitment to the duty of candour through regular technical briefings to the Court, the proactive sharing of information on compliance matters, and careful implementation of the Joint Policy on Duty of Candour with the Department of Justice. CSIS looks forward to demonstrating the progress that has been made to date in addressing the Court's concerns, and identifying opportunities for further improvement.

The National Security and Intelligence Committee of Parliamentarians (NSICOP) and NSIRA play a critical role in conducting independent reviews of CSIS's activities, and offering recommendations for continuous improvement. Their annual public reports provide insight into CSIS's activities and challenges, and help foster positive and informed discussion with Canadians on what their security intelligence agency is and should be doing in today's threat environment. In addition to actively supporting a number of reviews through the provision of materials and briefings, CSIS has also facilitated access to its regional offices throughout 2021 to enable NSICOP and NSIRA members to complete their studies and prepare their reports. Both NSICOP and NSIRA publish redacted reviews, which include CSIS responses to recommendations. This practice increases transparency for Canadians and emphasizes CSIS's commitment to continual improvement.





The People of
CSIS

The People of CSIS

CSIS employees take the mission of protecting Canada's national security very seriously, and they take it to heart. CSIS employees recognize that whether they are an Intelligence Officer, Policy Analyst, HR specialist, IT developer, or Surveillance Officer they all play a significant part in protecting their family, friends, neighbours, and way of life.

CSIS's most valuable resource is truly its people; they are what make CSIS a leading intelligence service. CSIS also recognizes that it must reflect the society it works so hard to protect because diversity within the organization allows for greater understanding of communities across the country and helps build and maintain the confidence and trust that needs to exist between civil society and intelligence agencies.

84%

of CSIS employees are proud of
the work they do

85%

of Canadians have
confidence in CSIS

sources: Public Service Employee Survey 2020 and CSIS Public Opinion Research 2021, respectively.

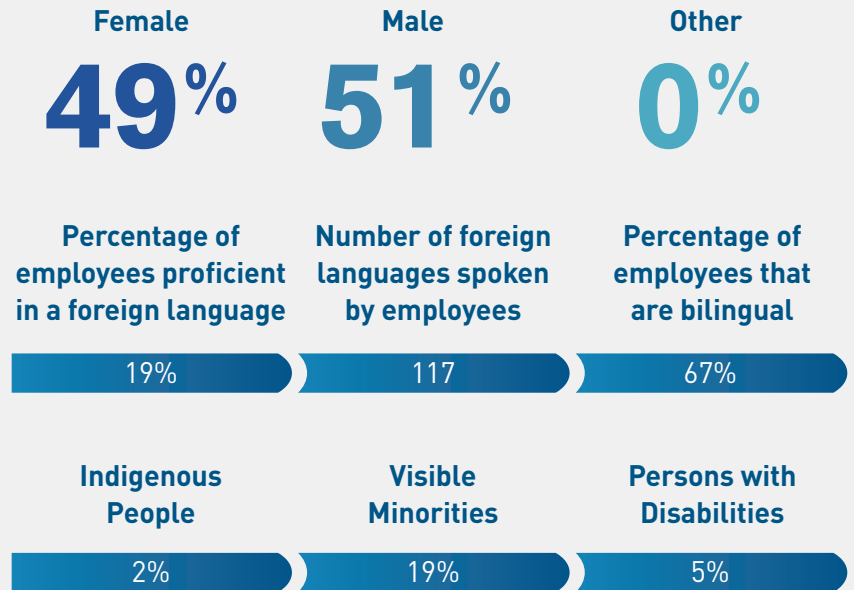
Employee Demographics

CSIS is dedicated to increasing diversity and inclusion in its workforce. These are core values, fundamental to the success of CSIS's mission. CSIS needs Canadians from all backgrounds, experiences, and abilities. From its headquarters in Ottawa, to offices across Canada and the world, CSIS is working to reflect the population it serves.

Collectively, CSIS employees speak more than 117 languages and dialects, with 67% of employees speaking both official languages. CSIS's workforce in 2021 was 49% female and 51% male. CSIS has also started collecting data for individuals who identify as non-binary or another gender and 0.35% of new hires for 2021 are represented in that category. CSIS's employment equity data is provided by employees who choose to self-identify. In 2021, 19% of CSIS employees identified themselves as visible minorities, 2% as Indigenous, and 5% as persons with disabilities. As outlined in the Diversity and Inclusion Initiatives section of this Report, CSIS is improving its recruitment efforts to reduce barriers and increase diversity and inclusion in its workforce.

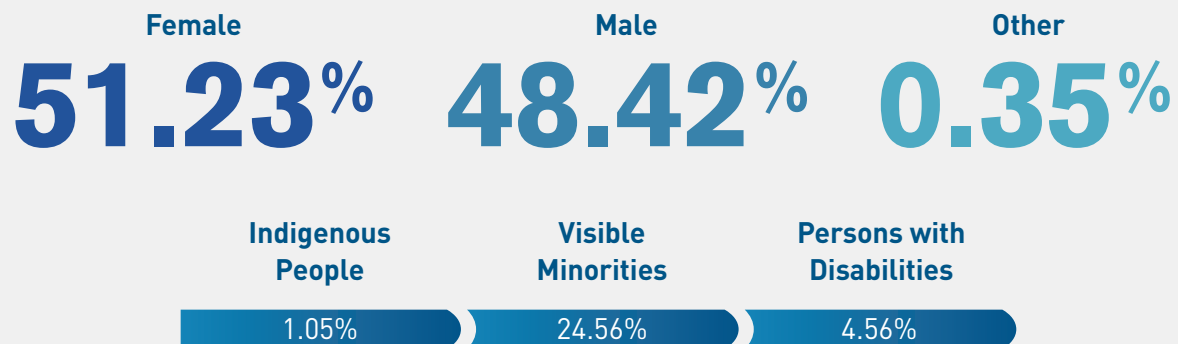
CSIS Employees

(as of December 31, 2021)



CSIS Hires

(between April 1 and December 31, 2021)



Communities within CSIS

Throughout 2021, CSIS leadership actively engaged employees to deepen the organization's understanding of racism, diversity, and inclusion, to foster a safe, positive environment where voices from diverse backgrounds are heard and included to ensure new approaches have meaningful impacts.

CSIS collaborates with and supports the advancement of grassroots networks and communities within the organization. CSIS leadership works with committees and employee-initiated networks such as the Advisory Committee on Diversity and Inclusion; Accessibility Committee; Women's Network; Young Professional's Network; Pride Network; Black, Indigenous, People of Colour (BIPOC) Network; and Gender Based Analysis plus (GBA+) Network to discuss issues and solutions, and to foster awareness and communication with senior management. These groups' contributions and perspectives have informed leadership and program area decisions on a variety of matters such as the delivery of training courses, recruitment initiatives, the development of a diversity and inclusion communication and awareness plan, and a new Diversity and Inclusion Strategy.

Diversity and Inclusion Initiatives

Throughout 2021, CSIS worked to develop a new Strategy on Diversity and Inclusion. This comprehensive strategy will prioritize inclusive leadership, recruitment, retention, career and development opportunities, addressing bias, and open communication on difficult issues such as systemic racism. The Strategy will include an action plan highlighting recommendations submitted by internal Diversity and Inclusion working groups, acting as direction for CSIS initiatives for the next three fiscal years. This strategy is employee-driven and will be shared widely within CSIS to continue the promotion of an inclusive and respectful workplace.

CSIS managers and employees need to have the right skills, knowledge and abilities to fulfill the organizational mandate and deliver on strategic priorities. This includes building cultural competence with respect to complex and intersectional elements of employees and the Canadians CSIS serves. In addition to promoting numerous courses and professional development opportunities on unconscious bias, cultural competency and anti-racism initiatives through the Canada School of Public Service, CSIS has created new training opportunities, some of which are mandatory, to encourage employees to expand their knowledge of diversity and inclusion.

Throughout 2021, CSIS also implemented new initiatives to increase diversity and inclusion through its recruitment efforts. This year CSIS's recruitment branch:

- Conducted a dedicated job competition for Intelligence Officers who are Indigenous or identify as a visible minority;
- Prioritized consideration of diverse candidates where employment equity gaps were identified;
- Encouraged hiring managers to consider flexible official language requirements when staffing diverse candidates;

- Reviewed and revised job poster formats, how leadership development opportunities were communicated, and provided workshops on how to prepare for executive selection processes;
- Mandated bias-free selection training for interview board members and placed diverse board members on assessment panels for job appointments and promotions; and,
- Made diversity and inclusion related coaching available to leaders.

CSIS is continuing an employment systems review with a target completion of spring 2022. The review will determine whether any of CSIS's employment systems, policies and practices are barriers for persons in designated groups, and recommend measures for improvement.

This year, the Director of CSIS also issued an invitation to employees who identify as Black, Indigenous or People of Colour (BIPOC) to join him in informal sessions and discuss their lived experiences as employees of CSIS. Over 150 employees accepted the invitation, and the sessions have been an essential part of ensuring that employee perspectives are not only heard, but are also influencing concrete change. Presentations from internal diversity champions to our employees have helped raise awareness, with guest professionals brought in to help lead open and honest conversations on racism, discrimination, leadership, diversity, and inclusion.

All these efforts enabled CSIS to provide a positive response to the Clerk of the Privy Council's Call to Action on Anti-Racism, Equity, and Inclusion, an initiative to which CSIS remains firmly committed. The work does not end here. CSIS must continue to efforts to build a Service that equitably represents all Canadians and the diverse communities we serve.

Health and Safety

The COVID-19 pandemic continues to bring extra focus to the health and safety of CSIS's employees, which is paramount. The need to ensure the security of operations continues to necessitate a unique response to operating during the pandemic. CSIS continues to take all recommended steps to make its workplaces safe for those needing access to classified material. CSIS is also allowing more flexibility for its employees who are juggling professional and personal responsibilities, while ensuring security requirements are not compromised. CSIS's existing programs that support psychological health and safety have continued to support employees with the pressures brought on by the pandemic, and with frequent and timely information related to health.

The pandemic has amplified the need for CSIS to support the health of employees, including their mental health. The CSIS Health and Wellness team is working on a new, comprehensive Organizational Wellness Strategy to improve upon CSIS's current Mental Health Strategy.

The Future of Work

The COVID-19 pandemic forced our world to become increasingly interconnected, with many Canadians working from home. The pandemic changed the expectations of many workers who are seeking to capitalize on work flexibilities that are now the norm rather than the exception; at the same time, employers are still working out how their organizations will operate in the long term.

While the pandemic has defined a "new normal" for so many, it has not changed CSIS's mandate, nor has it reduced the need to protect the most closely guarded information in the country. With operations and lives at risk, CSIS is not able to jump headfirst into the flexibilities and technologies that define the 'future of work' without considering how it can do so without jeopardizing its mandate to protect information. CSIS is now in the midst of a comprehensive initiative to consider and prioritize the opportunities and challenges that present themselves in the 'future of work'. CSIS also recognizes that it still needs to attract and retain a diversity of top talent in a rapidly changing labour market, and is considering all it can offer as an employer, from workplace flexibilities, to career mobility.

Ultimately, recruitment is the key to CSIS's future. CSIS is actively engaged in attracting and retaining the talent needed for success in the years to come, as well as in giving existing employees the support and opportunities they need to develop, thrive and advance. In addition to focusing certain hiring processes on increasing diversity, CSIS is also taking steps to improve the way jobs are advertised to attract candidates, and to explore how technology can be used to optimize virtual candidate assessments.



Intelligence in a
DIGITAL ERA

In 2021, CSIS continued to collect and analyse cyber intelligence further to its mandate to advise the Government of Canada on espionage, sabotage and foreign influenced activities but with a lens towards digital networks. In particular, CSIS investigates cyber activity which may pose a threat to Canada's national interests, cyber espionage, cyber sabotage, and cyber foreign influenced activity.

To investigate these threats, CSIS utilizes its powers outlined in the CSIS Act, such as warrants and threat reduction measures, in addition to liaising closely with foreign intelligence partners as well as with public and private sector entities. CSIS also works closely with its trusted Government of Canada partners who each have distinct and separate cyber mandates, though share a common goal of keeping Canada, Canadians, and Canadian interests safe and secure online. These partners include the Communication Security Establishment (CSE) – responsible for foreign signals intelligence, the Canadian Centre for Cyber Security (Cyber Centre) – responsible for safeguarding government systems and mitigation and technical guidance for cyber attacks against critical infrastructure and other levels of government, and the Royal Canadian Mounted Police (RCMP) – responsible for the prosecution of cyber criminals.

With all of this information, CSIS helps to identify malicious cyber actors, learn their methods and techniques, find their targets of interest, and define their motivations and goals; it then advises the Government of Canada accordingly.

As more Canadians utilize a growing number of internet-connected devices, such as smart home security systems and medical devices, new vectors of attack are available to state and non-state actors to conduct, as well as disguise, their hostile cyber operations. Future smart city platforms will almost certainly expand the cyber attack surface, and may introduce new vulnerabilities in sectors across the board, including those providing vital services.

In addition, emerging technologies such as artificial intelligence, quantum computing, and big data are radically transforming science and the future of how we will live and function. These technologies offer revolutionary advancements that will have a transformative impact on society. However, they can also have disruptive impacts on Canada's national interests if weaponized or used to facilitate intelligence collection by Canada's adversaries.

CSIS is constantly adapting to investigate new threat actors and activities that emanate from the rapid change in technology.

CSIS has always had to adapt its operations to respond to new technologies, emerging threats, and geo-political developments. Enacted in 1984, the *CSIS Act* was a modern, flexible, and forward-looking statute that enabled CSIS for many years, to adapt to the threats facing Canada and Canadians. But the world is not as it was in 1984; technology is now ubiquitous, and has changed the threats facing Canada, the privacy and legal landscape, and how CSIS conducts its national security investigations. In 2021, the *CSIS Act* is showing its age, and requires modernization to equip CSIS to adapt to future threats and capabilities.

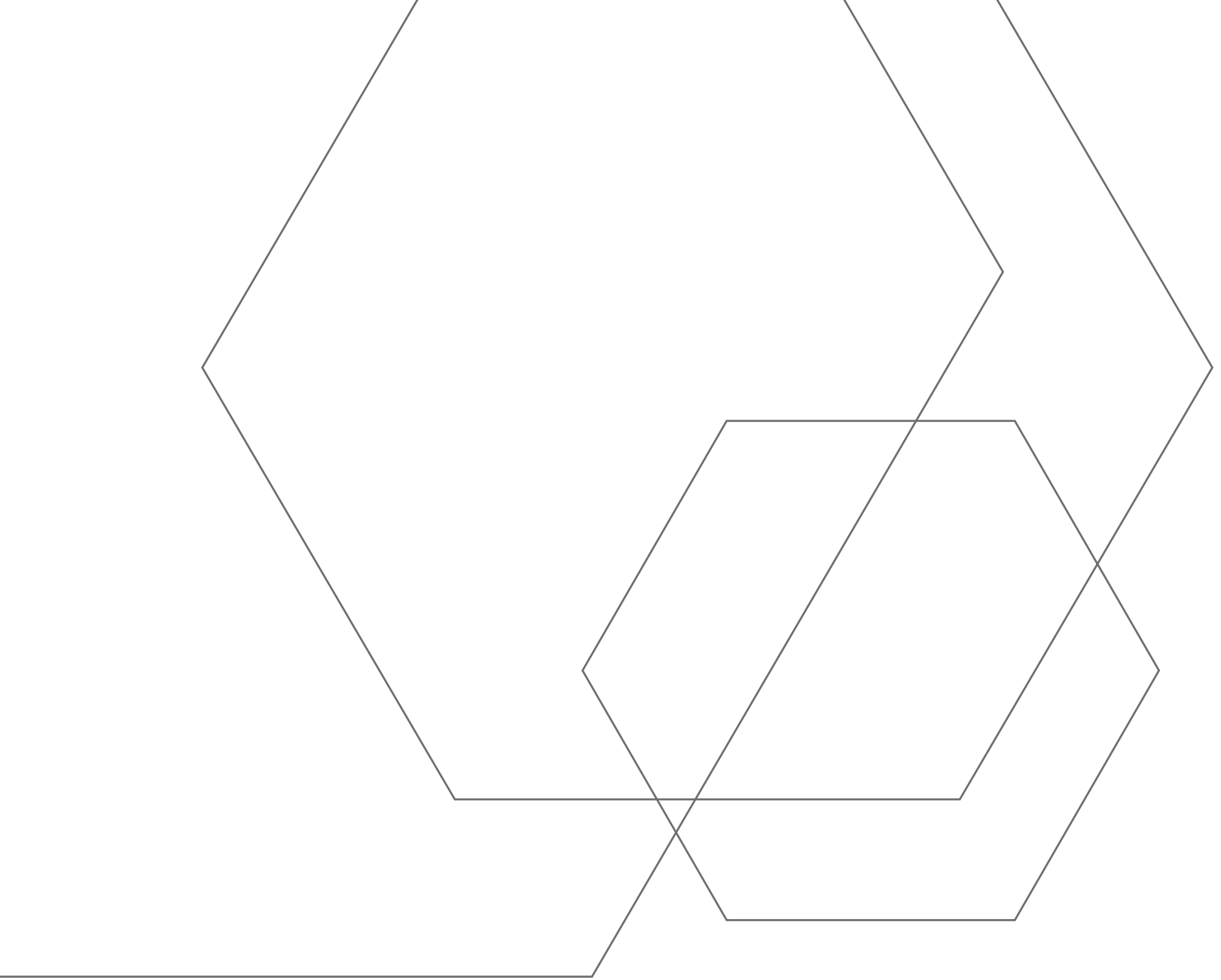
The *CSIS Act* has never been comprehensively reviewed, and has not adequately evolved to meet the challenges of today's complex global threat environment. Even with the significant amendments of the *National Security Act, 2017*, technological evolution, the relevance of bulk data, growing diversity and sophistication of threat activities, and additional legal decisions have further exposed the limitations of the *CSIS Act* in 2021.

Technological advances have radically changed individual Canadians' expectations of privacy, which require appropriate protection. While judicial authorization is one way to mitigate the privacy impact of certain activities, CSIS has a one-size-fits-all warrant authority. Originally designed to intercept phone calls on a landline, this authority does not have the flexibility necessary to meet CSIS's needs in an evolving privacy landscape. A growing range of less-intrusive techniques may require additional privacy protections but not those of traditional warrant powers. For example, information that used to be easily collected from public sources, such as phone books, today presents a privacy intrusion because of the ways our cellphone or online identifying information can reveal insights about our lifestyles and habits. Yet this basic investigative building block requires CSIS to exhaust other means of collecting the information first before applying for the same warrant as the most intrusive investigative techniques.

Much has changed in the nearly 40 years since 1984, but what has remained the same is the need to balance the protection of national security with the protection of individual rights. CSIS has always had robust mechanisms to ensure the privacy of Canadians' is protected as it does its vital work, including with judicial oversight. New legislation in 2017 enhanced review of CSIS by both the National Security and Intelligence Review Agency and the National Security and Intelligence Committee of Parliamentarians. But in a democratic society, protecting individuals' privacy and national security cannot be a zero sum.

Canadians rightly expect that CSIS has the necessary authorities to protect Canada against today's threats, and is equipped to face the threats of tomorrow. The reality is, however, that CSIS faces significant challenges, operating in a data-driven modern world. In order to enable CSIS to continue operating as it always has, its authorities must be suited for current realities and future needs.

As Canada prioritizes rebuilding from the pandemic, there is an opportunity to engage Canadians in a national security dialogue. There is a need for greater awareness of how the threat landscape is evolving, and how modernizing Canada's national security legislative framework will help protect Canadians, innovation and economic investment, democratic values, and indeed, Canada's future.





CSIS's
2021

