



Canadian Security  
Intelligence Service

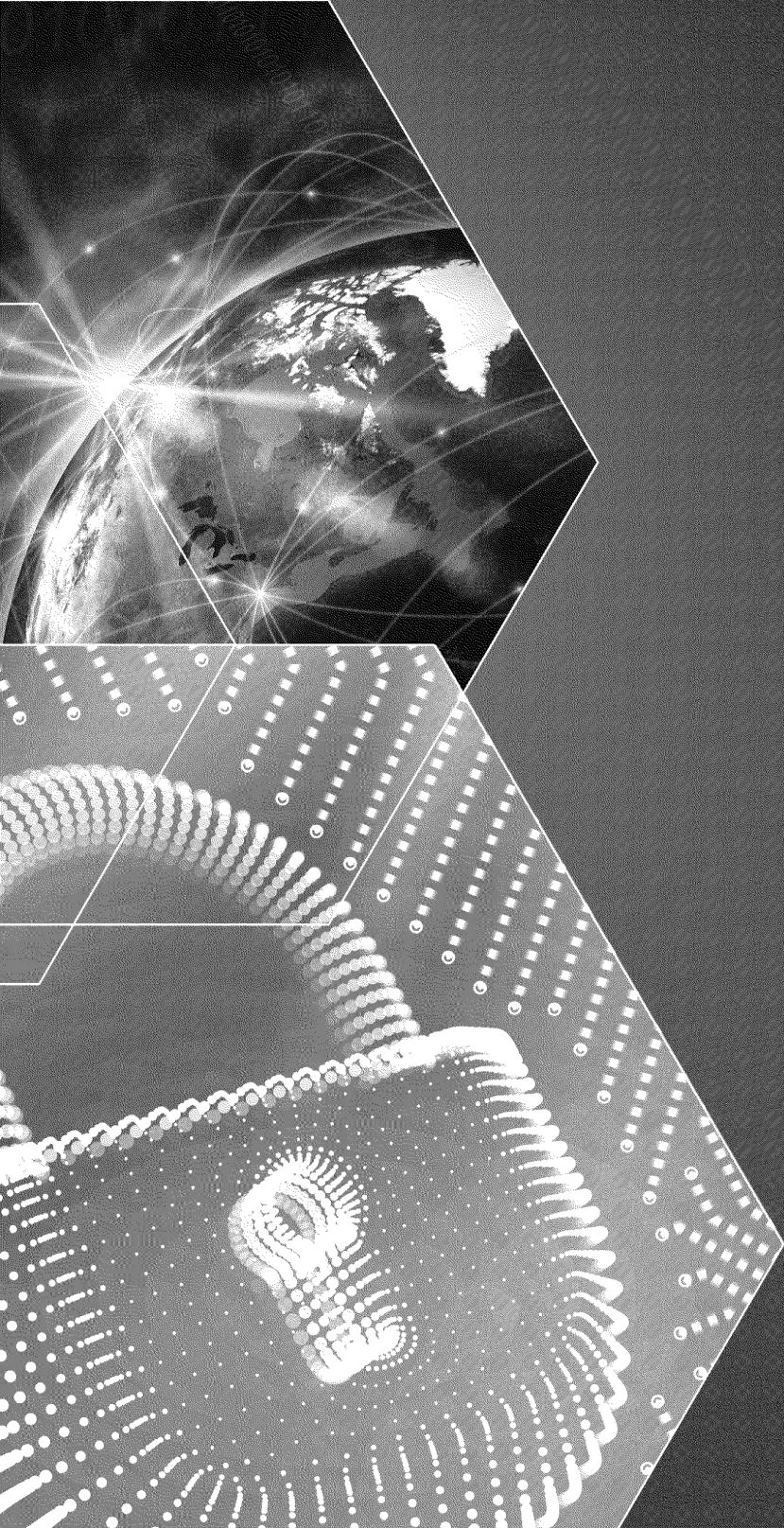
Service canadien du  
renseignement de sécurité



# 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](http://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.*

# Table of Contents

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

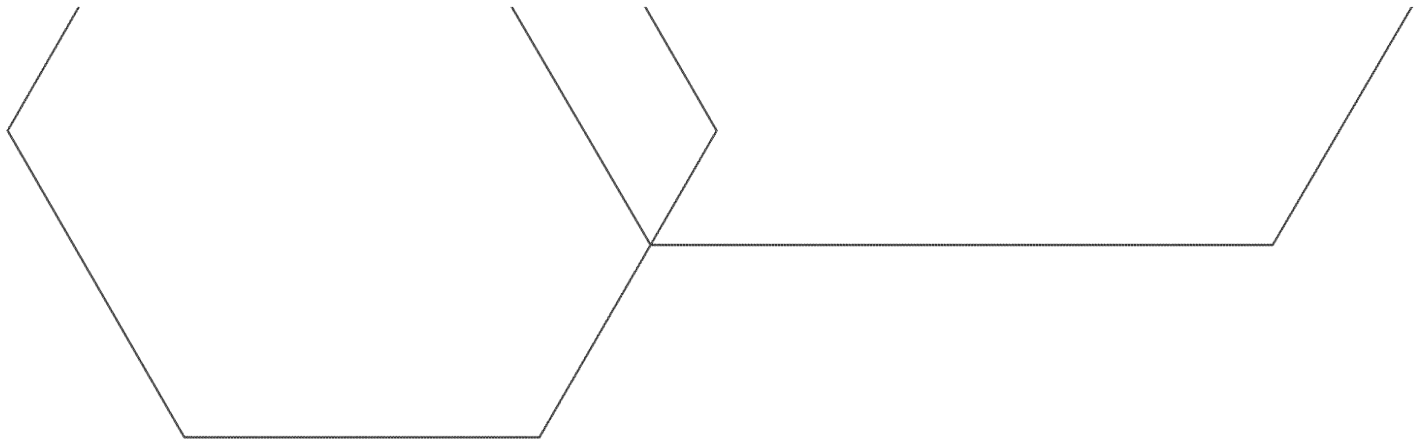
## Message from the Director of CSIS



“

*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.

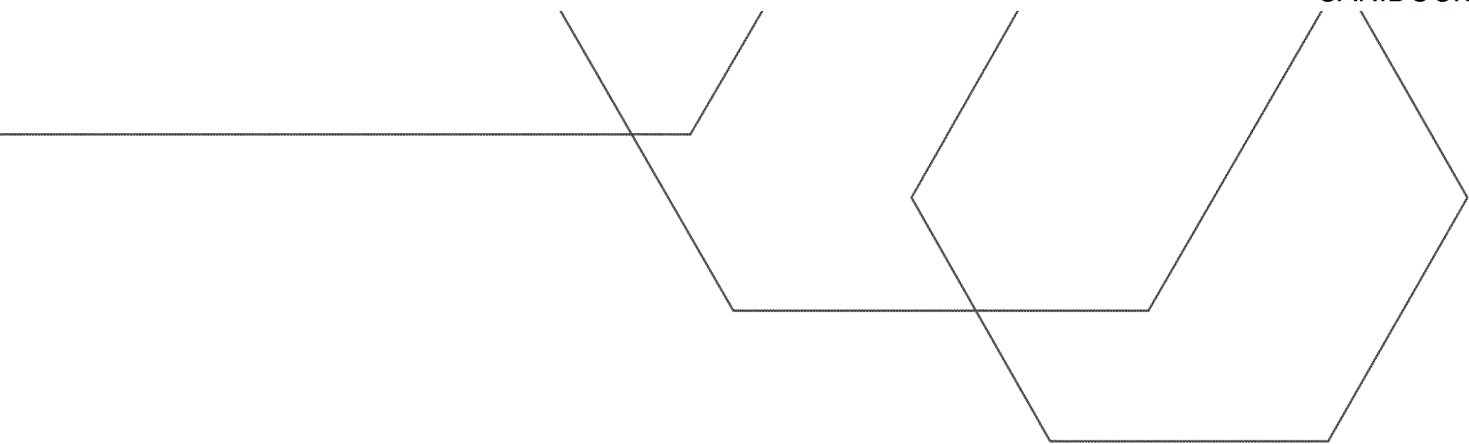
The exponential rate of technological change and our hyper-connected society only exacerbates these challenges. Technology may be the most disruptive force shaping our world today. States, corporations and societies are grappling with how to handle these changes, which are deepening existing global inequities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

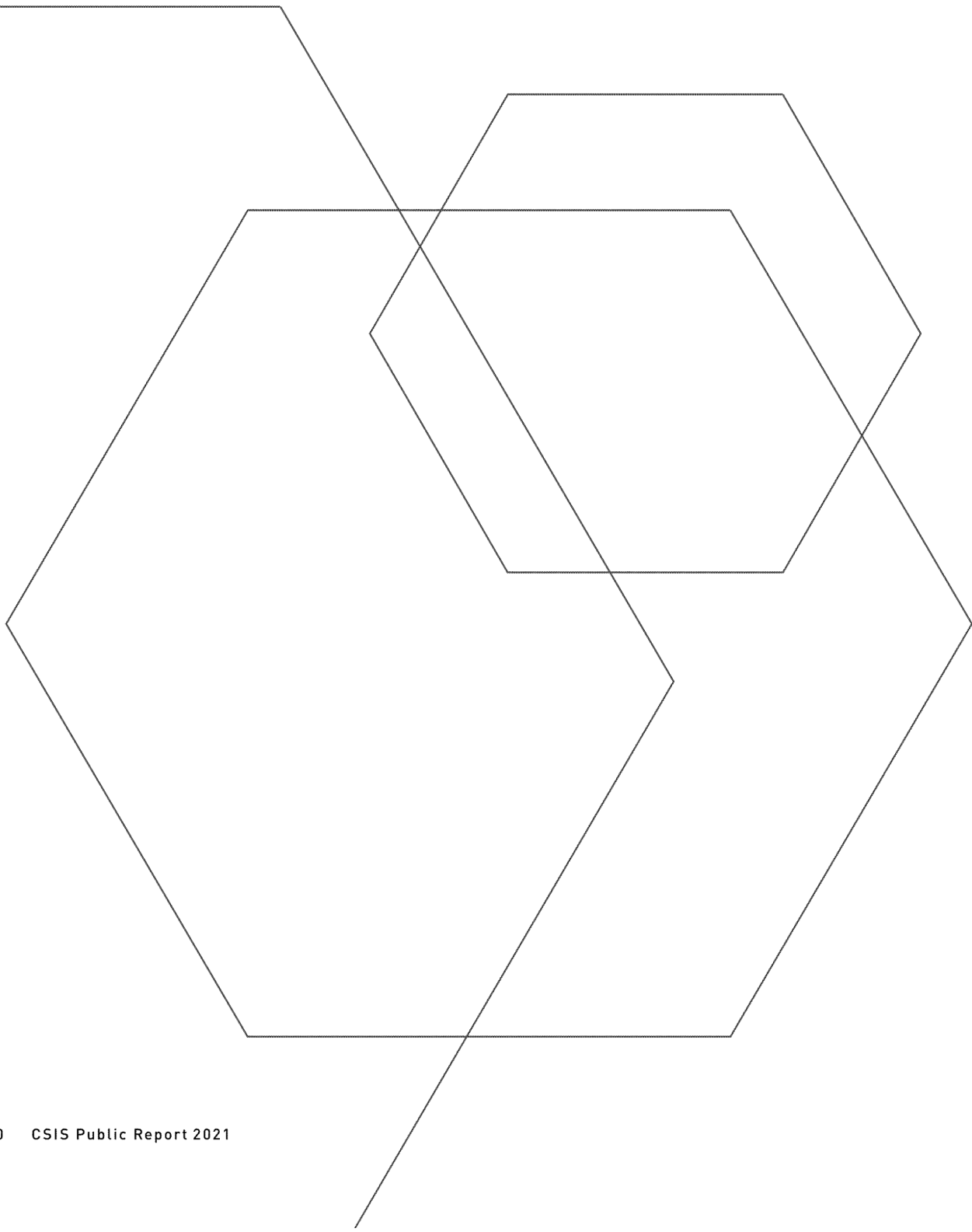
Like all organizations, CSIS has been impacted by a confluence of factors that challenge our conceptions of the nature of work and the workforce. Given CSIS's unique mission and high security requirements, our national headquarters, domestic regional offices and foreign stations remained operational 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.

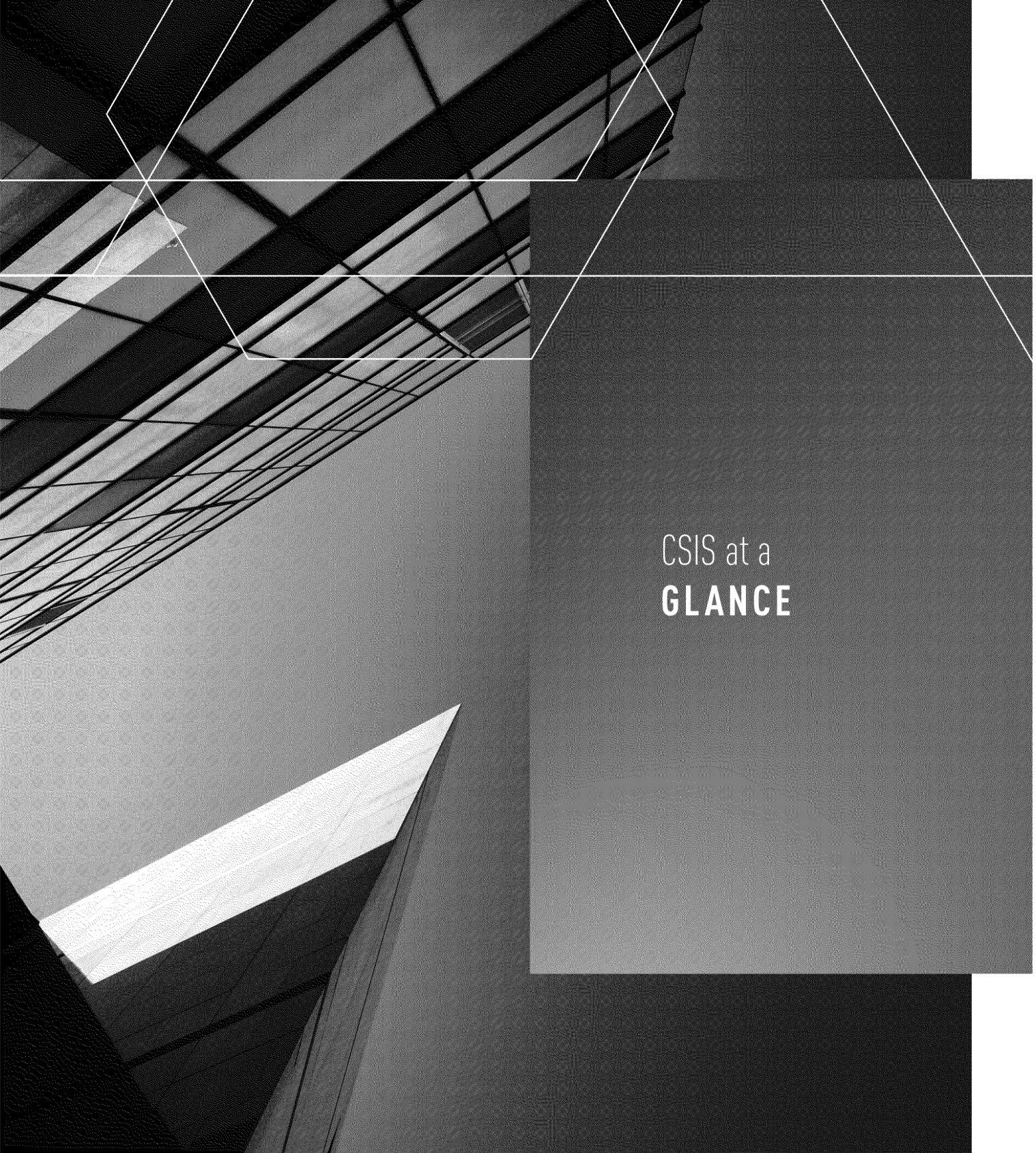
As Director, I am also personally committed to ensuring that CSIS's workplace is free of discrimination, bias, harassment and aggression. All CSIS employees deserve to come to work every day in a safe, healthy and respectful environment where diversity and inclusion are highly valued. CSIS continues 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

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.

# 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 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				
Operating				
<b>Total</b>	<b>586,998,953</b>	<b>586,607,955</b>	<b>611,085,093</b>	<b>676,899,701</b>



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.

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

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

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

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

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

**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.

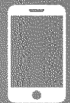
CSIS has also been aware of several Russian military and intelligence entities that are engaged in information confrontations targeting Ukraine. These activities include the spread of disinformation and propaganda attempting to paint Ukraine and NATO as the aggressors in the current conflict. Such measures 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](https://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.

# Election Security

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).

# Economic Security

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.

# Cyber Threats

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 (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 20<sup>th</sup> 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.

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.

# International Terrorism

On August 15<sup>th</sup>, 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

Permanent Resident Inside and Outside Canada	14,800
Refugee (Front-End Screening**)	21,200
Citizenship	240,700
Temporary Resident	9,000
<b>Total</b>	<b>293,700</b>

# Government Screening Programs

## Requests Received\* in 2021

Federal Government Departments	64,600
Free and Secure Trade (FAST)	14,000
Transport Canada (Marine and Airport)	31,000
Parliamentary Precinct	2,100
Nuclear Facilities	12,200
Provinces	140
Others	2,100
Foreign Screening	500
Special Events Accreditation	0
<b>Total</b>	<b>126,640</b>

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.

Twitter

Facebook

YouTube

LinkedIn

**47,000**

Twitter Followers

**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.

# Transparency

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

# of Privacy Act requests received	1161
# of ATIA requests received	795
# of Informal requests received	847

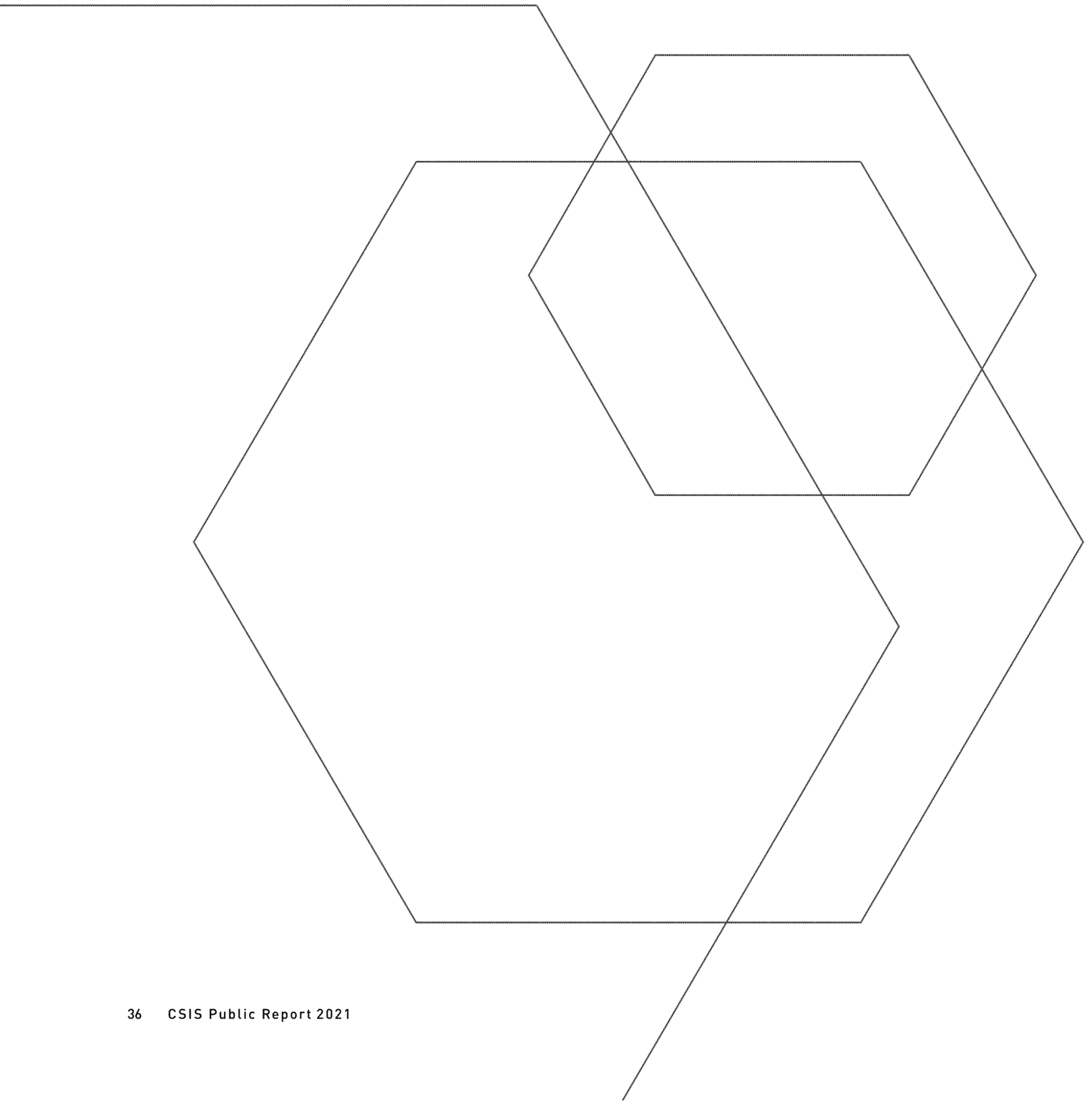
# Review and Compliance

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

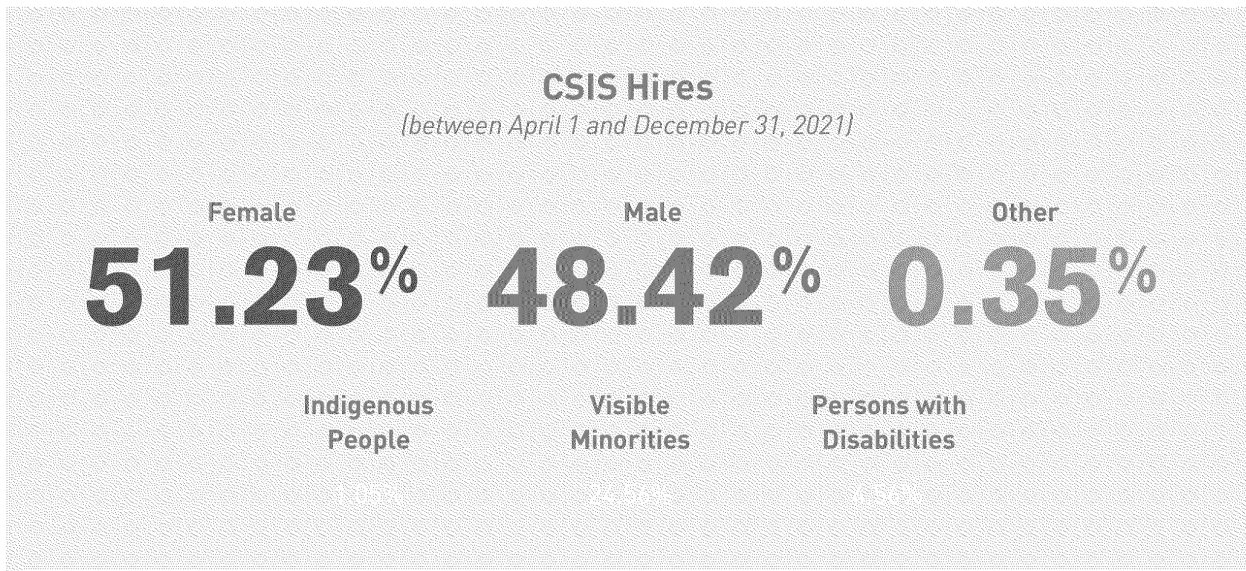
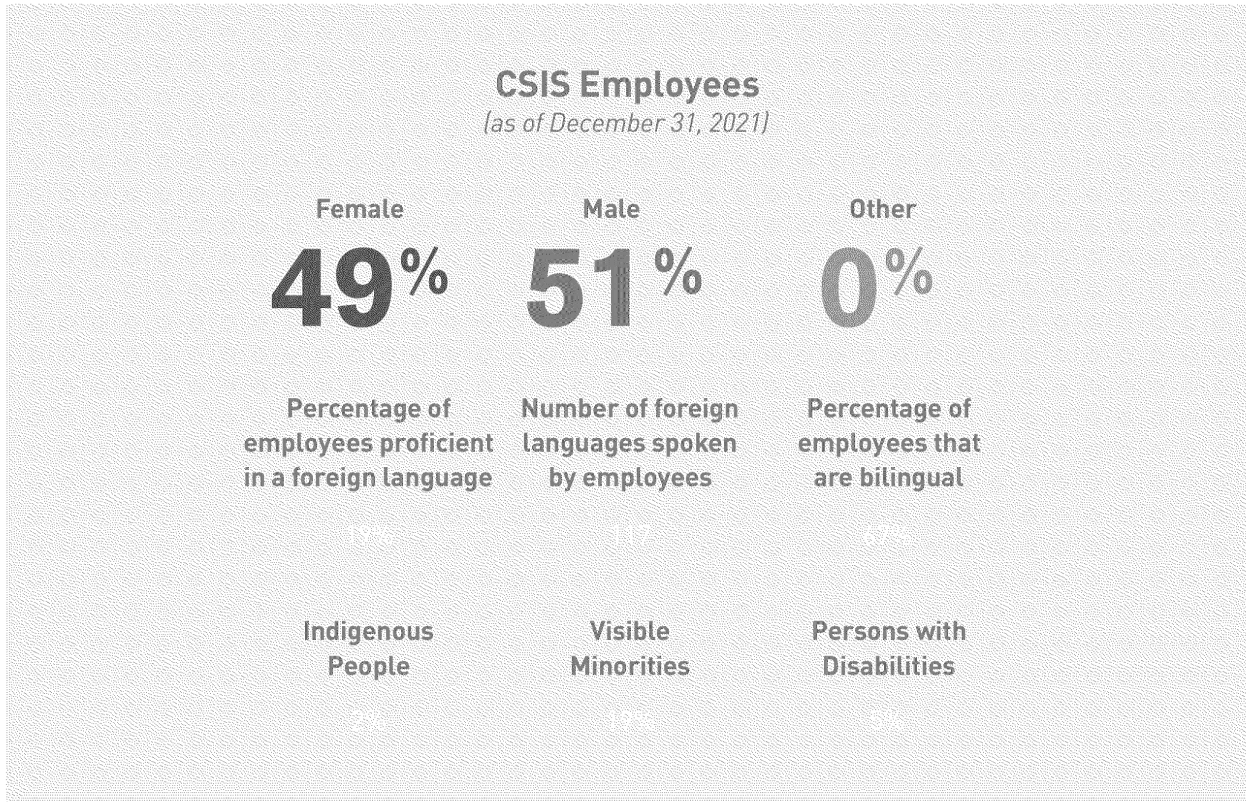
## 85%

of Canadians have  
confidence in CSIS

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

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.



# 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.

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

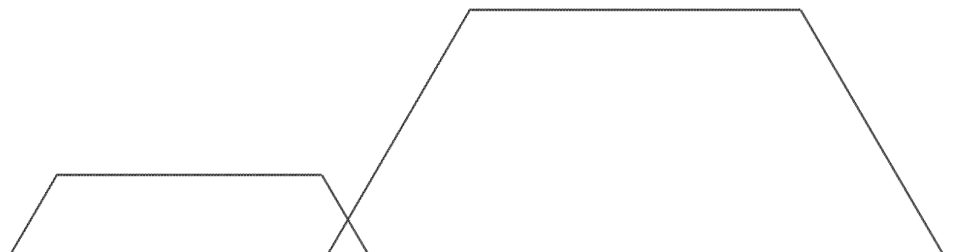
The COVID-19 pandemic continues to bring extra focus to the health and safety of CSIS's employees, which is paramount. The need to ensure the security of operations continues to necessitate a unique response to operating during the pandemic. CSIS continues to take all recommended steps to make its workplaces 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 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**

# CSIS's Role in Cyber

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.

# Modernizing Authorities

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.

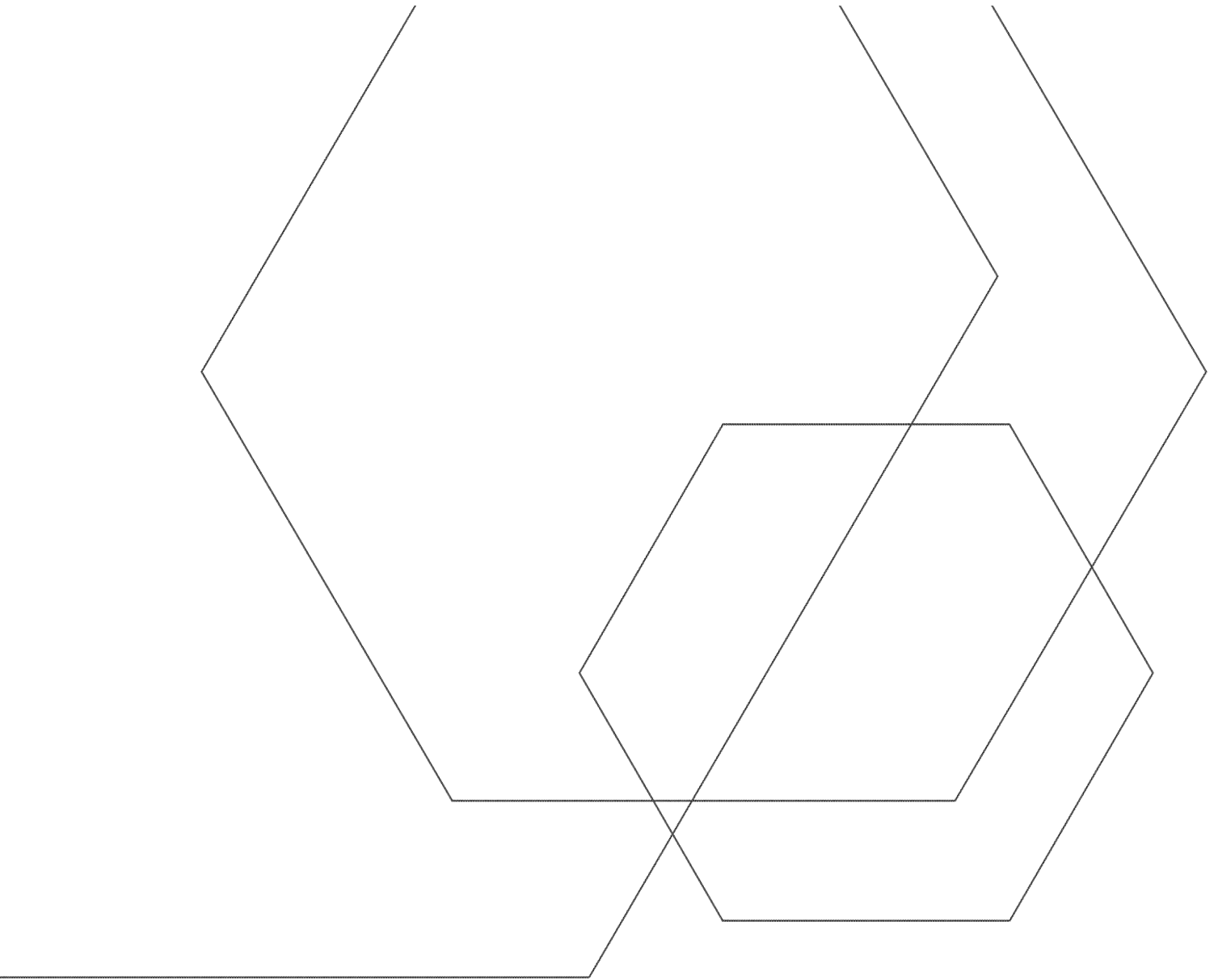
The *CSIS Act* has never been comprehensively reviewed, and has not adequately evolved to meet the challenges of today's complex global threat environment. Even with the significant amendments of the *National Security Act, 2017*, technological evolution, the relevance of bulk data, growing diversity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

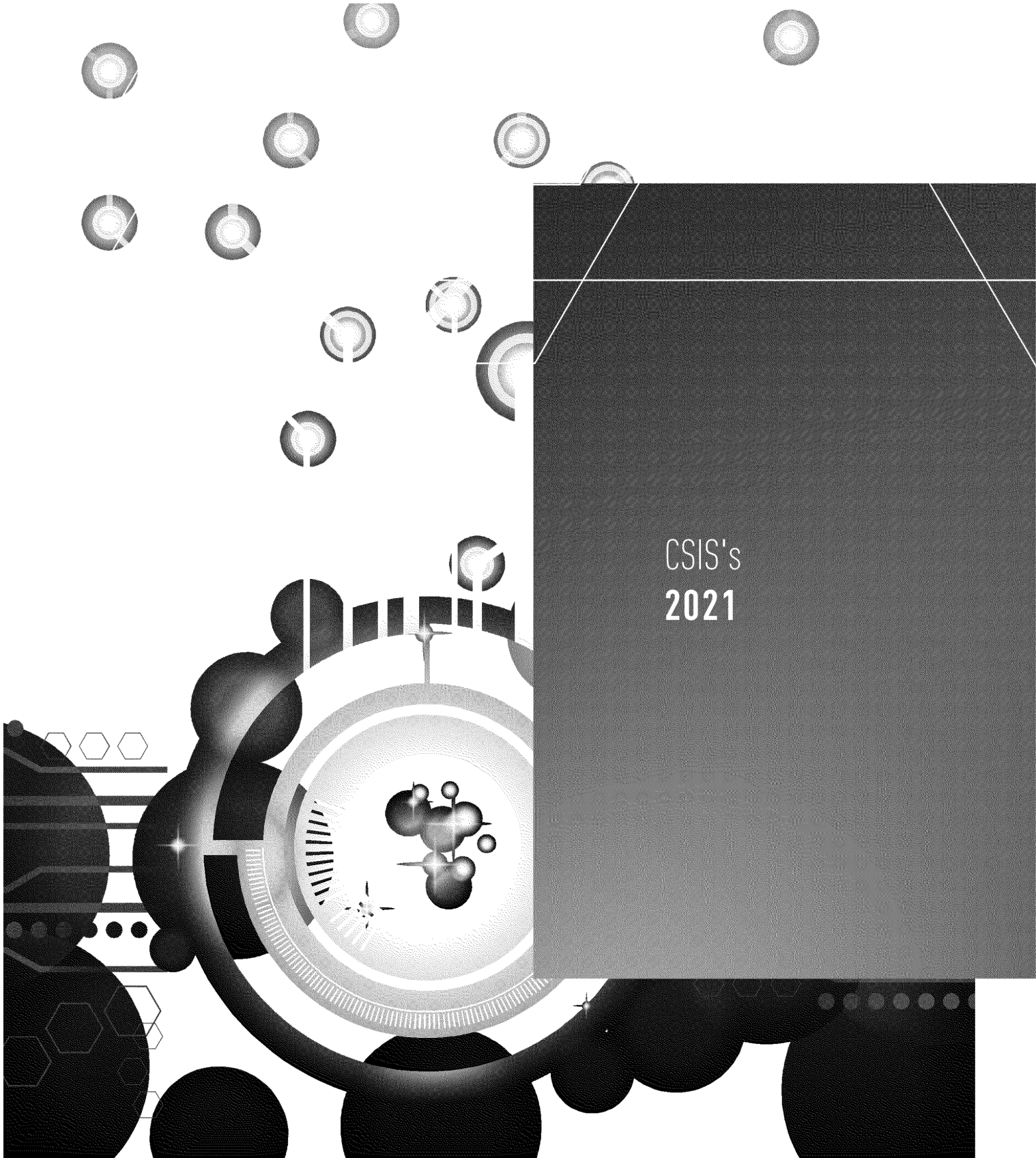
Technological advances have radically changed individual Canadians' expectations of privacy, which require appropriate protection. While judicial authorization is one way to mitigate the privacy impact of certain activities, CSIS has a one-size-fits-all warrant authority. Originally designed to intercept 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

# CSIS's 2021

	Continuation of CSIS's COVID-19 vaccine rollout assistance and outreach
Director Vigneault delivers <u>speech</u> on the threat environment to the Centre for International Governance Innovation	
Publishing of CSIS's annual <u>report</u> to the Minister on <i>Avoiding Complicity in Mistreatment by Foreign Entities Act</i>	
	CSIS launches informative <u>videos</u> to explain violent extremism terminology as well as foreign interference and espionage
Publishing of CSIS's <u>2020 Public Report</u>	
	Publishing of CSIS <u>Public Opinion Research</u>
	Publishing CSIS <u>report</u> on Foreign Interference Threats to Canada's Democratic Process
The Government of Canada's Security and Intelligence Threats to Elections <u>[SITE]</u> Task Force initiated for the 44 <sup>th</sup> Federal Election in Canada	
CSIS hosts its own virtual Technology Career Fair	New Minister of Public Safety is announced and briefed on CSIS
Mandate letter presented to the Minister of Public Safety	
Publishing of the annual CSIS <u>reports</u> on the Administration of the <i>Access to Information Act</i> and Administration of the <i>Privacy Act</i>	





Canadian Security Intelligence Service  
Service canadien du renseignement de sécurité



CSIS  
Public Report  
2020

A SAFE, SECURE AND PROSPEROUS CANADA THROUGH TRUSTED INTELLIGENCE AND ADVICE.  
DES RENSEIGNEMENTS ET DES CONSEILS FIABLES POUR UN CANADA SÛR ET PROSPÈRE.

Canada

ISSN: 1495-0138

Catalogue number: PS71E-PDF

Aussi disponible en français sous le titre : *Rapport public du SCRS 2020*

[www.canada.ca](http://www.canada.ca)

Published in April 2021

© Her Majesty the Queen in Right of Canada, as represented by the Minister of Public Safety and Emergency Preparedness, 2021

© Public Works and Government Services Canada 2021

CSIS  
Public Report  
**2020**



## Table of CONTENTS

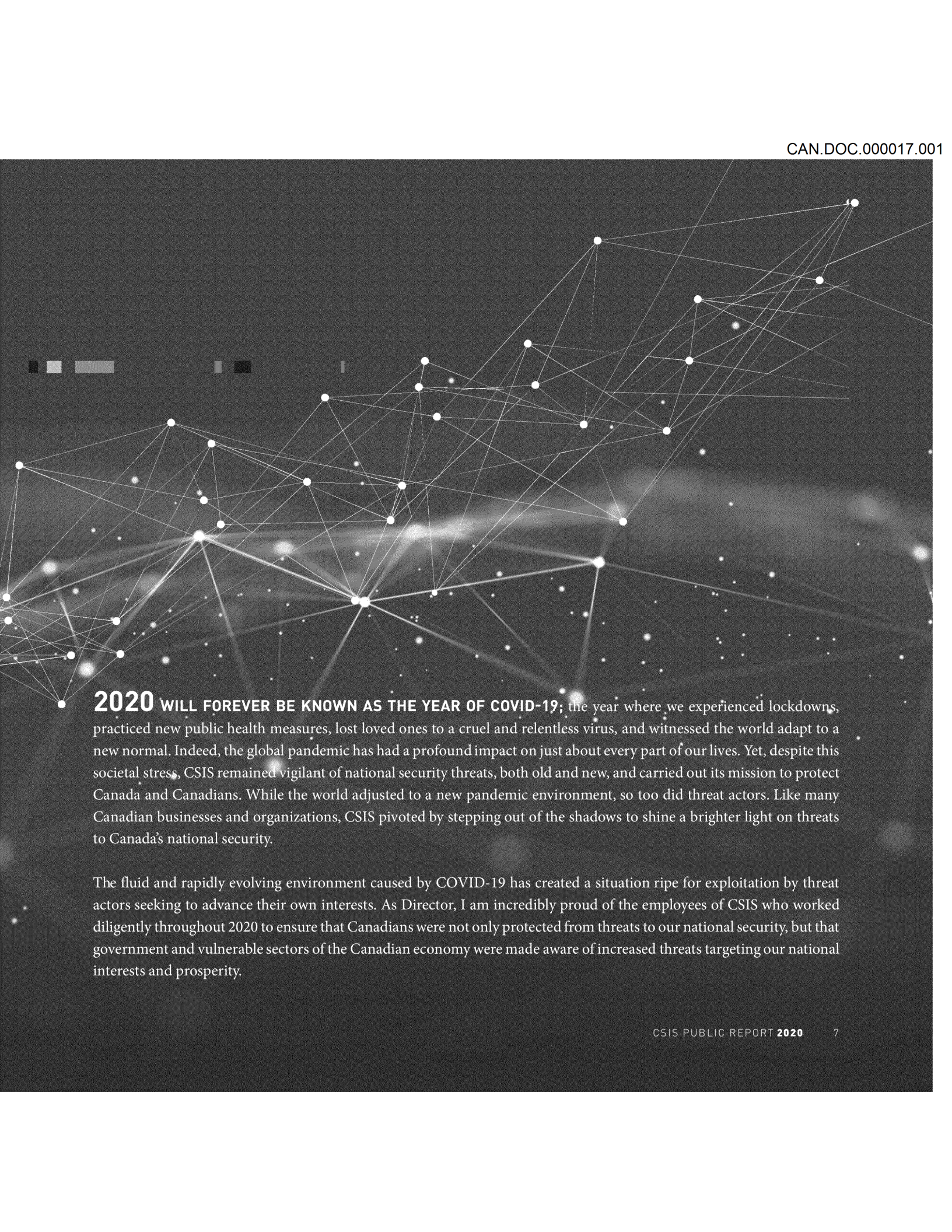
<b>Message from the Director</b>	<b>6</b>
<b>CSIS 101</b>	<b>11</b>
Mandate	12
Accountability	12
Partnerships	13
Duties and Functions	13
Financial Reporting	14
<b>The Pandemic</b>	<b>17</b>
COVID-19 Outreach Initiative	18
The Four Gates of Economic Security	19
CSIS Support to the Government of Canada's Pandemic Response	20
<b>The Threat Environment</b>	<b>21</b>
Espionage and Foreign Interference	22
Cyber Threats	24
Counter Proliferation	25
Ideologically Motivated Violent Extremism	26
Politically Motivated Violent Extremism	27
Religiously Motivated Violent Extremism	27
Canadian Extremist Travellers	27
International Terrorism	28
Security Screening	30

<b>Engagement with Canadians</b>	<b>33</b>
Transparency	34
Outreach	34
<b>The People of CSIS</b>	<b>37</b>
Diversity and Inclusion	38
Code of Conduct	38
CSIS Across Canada	40
CSIS Around the World	41
<b>Foreign and Domestic Cooperation</b>	<b>43</b>
<b>Review and Compliance</b>	<b>45</b>
Compliance	46
External Review	46
<b>Modernizing Authorities</b>	<b>47</b>



Message from  
**THE DIRECTOR**





**2020 WILL FOREVER BE KNOWN AS THE YEAR OF COVID-19;** the year where we experienced lockdowns, practiced new public health measures, lost loved ones to a cruel and relentless virus, and witnessed the world adapt to a new normal. Indeed, the global pandemic has had a profound impact on just about every part of our lives. Yet, despite this societal stress, CSIS remained vigilant of national security threats, both old and new, and carried out its mission to protect Canada and Canadians. While the world adjusted to a new pandemic environment, so too did threat actors. Like many Canadian businesses and organizations, CSIS pivoted by stepping out of the shadows to shine a brighter light on threats to Canada's national security.

The fluid and rapidly evolving environment caused by COVID-19 has created a situation ripe for exploitation by threat actors seeking to advance their own interests. As Director, I am incredibly proud of the employees of CSIS who worked diligently throughout 2020 to ensure that Canadians were not only protected from threats to our national security, but that government and vulnerable sectors of the Canadian economy were made aware of increased threats targeting our national interests and prosperity.

Very early into the pandemic, CSIS adopted a more visible and proactive public role than ever before by implementing a Canada-wide outreach and engagement initiative focused on academia, research institutions, and private businesses in the biopharmaceutical, life sciences, and data science sectors who were working on COVID-19 vaccine research. Later on, as the pandemic evolved, CSIS gave similar briefings to supply chain associations and other related industry groups on the risks associated with logistics supply networks. Both these outreach activities were conducted to complement other efforts in support of the Government of Canada's overall pandemic response.

In 2020 our world became increasingly interconnected with many Canadians working from home, presenting more opportunities than ever for cyber-actors to conduct malicious online threat activity. Moreover, we observed how online platforms were used by violent extremists to continue the spread of harmful beliefs, including xenophobic, anti-authority narratives as well as conspiracy theories about the pandemic, in an attempt to rationalize and justify violence.

Similarly, in 2020, CSIS observed espionage and foreign interference activity at levels not seen since the Cold War. In short, the key national security threats facing Canada, namely violent extremism, foreign interference, espionage and malicious cyber activity, accelerated, evolved and in many ways became much more serious for Canadians.

While fulfilling our mission to protect Canada from threats to our national security, a Federal Court decision raised concerns about certain CSIS operational activities as well as with CSIS's duty of candour obligations to the Court. To be clear, CSIS's respect for the rule of law is the foundation from which the organization leads our activities. While the *National Security Act 2017* addressed the Court's concerns about operational activities, CSIS has taken a number of concrete actions to address concerns related to its duty of candour. Those concrete actions include: a commissioned review of CSIS's duty of candour obligations, the creation of a dedicated affiant unit to ensure disclosure obligations to the Court are understood and met, new and extensive training for employees, and a Public Safety-CSIS Cooperation Framework with the goal of ensuring greater transparency and accountability to implement an updated Ministerial Direction for Accountability.

When the *CSIS Act* was drafted in 1984, telephone books and alligator clips on phone lines were among the tools used to identify threat actors and collect information. Information was stored in silos. The private sector was not a partner in national security. Clearly the world today is much different. The mechanisms that were appropriate 37 years ago are no longer suitable in a world that is now digital by default and where information volume and transit of that information is accelerating exponentially every day.



CSIS will always champion a sophisticated and mature discussion on national security issues, especially those grounded in a Canadian context. In today's dynamic threat environment, government, civil society and the private sector must work together to protect our national interests. As a matter of course, CSIS will continue to review and assess its authorities to address the national security threats and privacy expectations of Canadians both today and in the future.

CSIS relies on the trust and confidence of Canadians to perform its duties. Part of that trust stems from reassurance that CSIS understands and reflects all communities within Canada. While our work to end systemic racism and make our workplace more inclusive and diverse must continue and grow, I am proud of the significant strides CSIS has made and the organization's collective resolve to do better. CSIS must represent all the communities it protects.

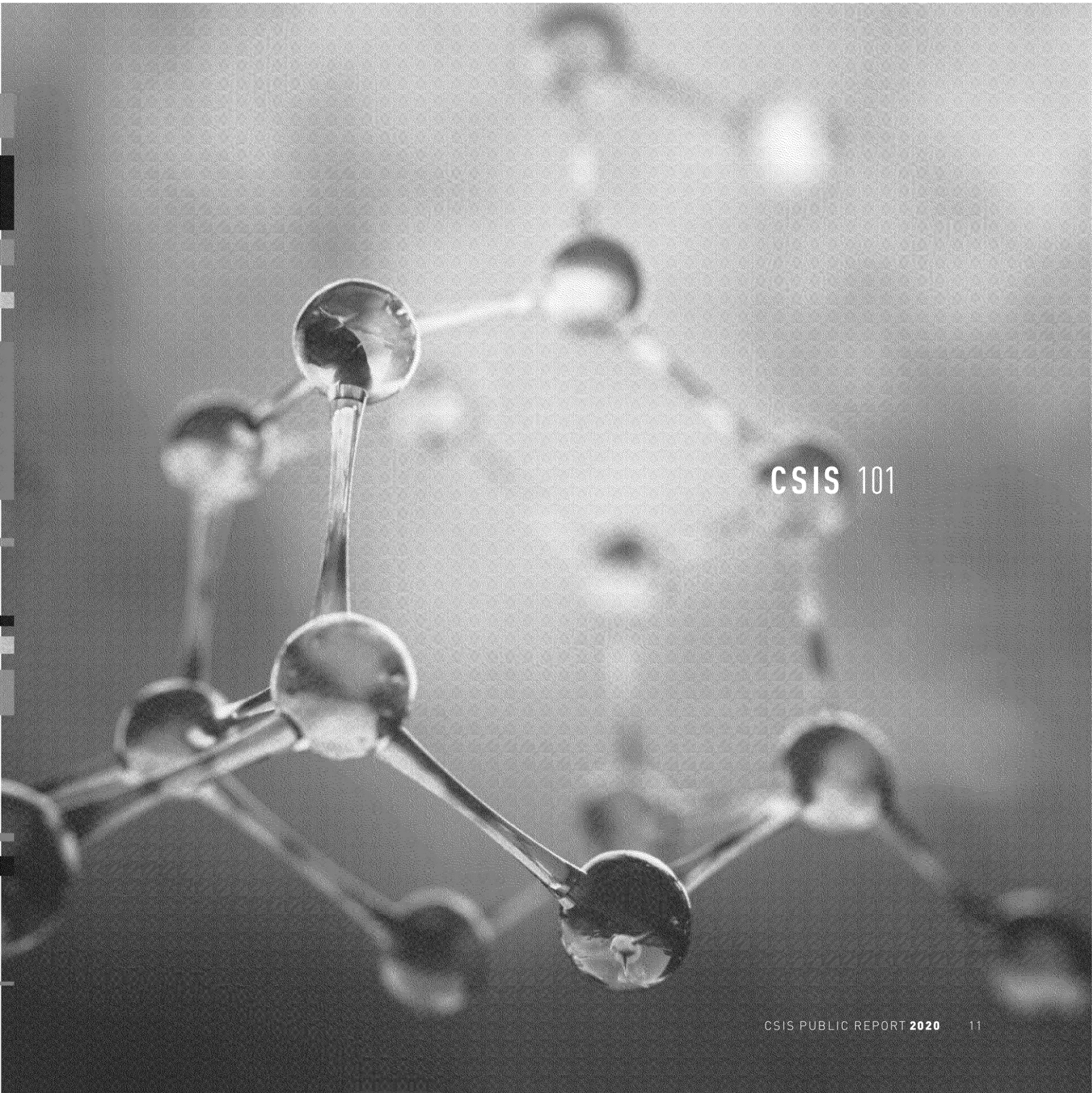
My focus as Director, especially during this pandemic, has been to ensure that all of our employees work in a healthy, safe, and respectful environment. Given our unique mandate, this meant that when much of the world moved to working from home, CSIS employees continued their critical mission in a way that respected the need to protect the most closely-guarded information in the country. While COVID-19 presented new challenges which required the organization to adapt, I am grateful to every single employee for the personal and professional dedication that they continue to bring to our mission. The people of CSIS are what make the organization a world-leading and respected security intelligence service. Their devoted efforts throughout 2020 have instilled me with great pride. Canadians can and should be proud.

While 2020 changed many things, CSIS's mandate remained the same. We will never stop in our pursuit to keep Canada and Canadians safe — and do so in a way that upholds the trust Canadians place in us.



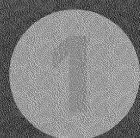
**DAVID VIGNEAULT**  
DIRECTOR, CANADIAN SECURITY INTELLIGENCE SERVICE



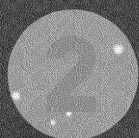


CSIS 101

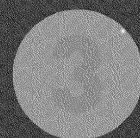
## CORE MANDATE



Investigate activities suspected of constituting threats to the security of Canada

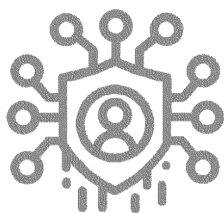


Advise the Government of these threats



Take lawful measures to reduce threats to the security of Canada

## ACCOUNTABILITY



- Canadian Public
- Minister of Public Safety and Emergency Preparedness
- Federal Court
- Attorney General of Canada
- 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

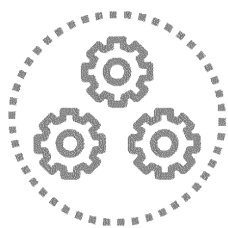
## PARTNERSHIPS

Nearly **80** arrangements  
with domestic partners.



Over **300** arrangements  
with foreign partners in  
150 countries and territories

## 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.

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

## PROGRAM INVENTORY

Operational  
Program  
Management

Regional  
Collection

Operations  
Enablement

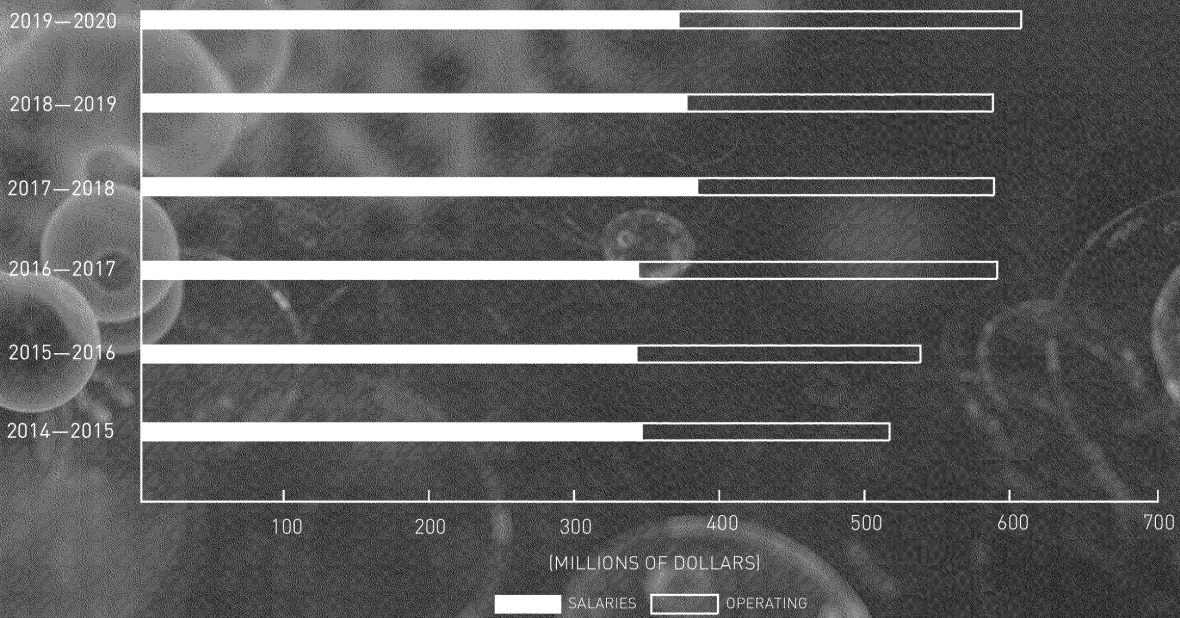
Intelligence  
Assessment and  
Dissemination

Security  
Screening

Integrated  
Terrorism  
Assessment  
Centre



### ACTUAL EXPENDITURES









The  
**PANDEMIC**

## COVID-19 OUTREACH INITIATIVE

As Canadian researchers and businesses adapted and innovated to respond to the COVID-19 pandemic, so too did various threat actors — particularly those from abroad. Canada's research, biopharmaceutical and life sciences sectors, while already of interest to foreign threat actors, became even more valuable targets as the world raced to develop a vaccine, therapeutics, and other measures to combat COVID-19. The vulnerabilities of these organizations to espionage and foreign interference were exacerbated by remote work and increased public visibility of their efforts. CSIS and its allies noted a sharp increase in both the scope and scale of hostile threat actors' activities targeting these sectors.

While CSIS has long engaged with academia and has been advising the Canadian public about threats to our national security for many years, the high stakes involved in protecting Canada's biopharmaceutical and life sciences sectors during the pandemic led CSIS to take a more visible and proactive engagement role than ever before. At the onset of the pandemic, CSIS initiated a Canada-wide outreach and engagement initiative focused on academia, research institutions, and private sector companies in the biopharmaceutical, life sciences, and data science sectors. A public statement about this outreach was issued jointly with the Communications Security Establishment (CSE) on May 14, 2020 warning Canadians about the increased risk of foreign interference and espionage. Similarly, on September 14, 2020, the Minister of Public Safety and Emergency Preparedness, Minister of Innovation, Science and Industry and the Minister of Health released a joint-statement advising Canadian health organizations, government partners and industry stakeholders to

remain vigilant of cyber threats as well as foreign interference and espionage targeting their institutions and important work.

In order to reach a large number of organizations — and with the necessary speed — during the pandemic, CSIS leveraged all available tools to brief stakeholders. Large virtual briefings were offered to the academic and research community, with complementary threat briefings provided in several instances by CSIS and the Canadian Centre for Cyber Security. In order to reach even wider audiences, CSIS provided briefings to large organizations, including the Canadian Chamber of Commerce, and amplified these efforts online and through the media. These briefings provided stakeholders with clear information about the threat and possible impact of espionage and foreign interference on their work as well as the steps they should take to protect themselves. To convey this information, CSIS publicly introduced the Four Gates of Economic Security framework to explain how foreign interference and espionage present economic security risks including what could be targeted and how threat activity may occur.

Threat actors may try to access valuable information through the four gates: 1) imports and exports; 2) investments; 3) knowledge; and 4) licences. For example, Canadian imports and exports of medical supplies and protective equipment are crucial to keep Canadians safe, and presents one gate threat actors may try to access. Investing in a business can be another way to obtain access to an organization's intellectual property or specialized research and development regarding vaccines and new technologies. Canadian innovation, research and intellectual property could be the target of foreign intelligence operations to gain access to knowledge and sensitive data,

including by cyber-attacks, spies, and insider threats. Threat actors may even exploit patents, rights, and other licenses to illicitly gain access to medicines, technologies, or intellectual property. Threat actors may try to access all four gates, but they only need to exploit one to cause serious harm.

As the focus moved from the development of vaccines and therapeutics to the delivery and distribution of vaccines, CSIS pivoted to reach Canada's supply chain sector and other relevant stakeholders involved in the manufacturing, distribution, and supply of COVID-19 vaccines and other critical supplies.

## THE FOUR GATES OF ECONOMIC SECURITY

Threat actors may try to access valuable information through the four gates:

**1** Threat actors may simply try to purchase sensitive technology from Canadian companies or researchers, either for immediate deployment or in order to try to reverse engineer it themselves. Harm to Canada's national security and economic prosperity (future sales/research) may then occur as a result of the unauthorized onward sharing of the technology.

**3** Threat actors have previously used both technical and human intelligence operations in order to acquire intellectual property or gain the access required to achieve their objectives. Examples include: cyberespionage, insider threat activity within Canadian companies, collaboration agreements, and co-opted individuals (e.g., talent programs).



**2** Threat actors use a range of financial arrangements (e.g., foreign direct investment, joint ventures) through which they can gain access to Canadian technologies and know-how. Through these investments, threat actors gain new capabilities and Canada loses out on future economic opportunities.

**4** Threat actors may seek privileged access to technology or intellectual property through licenses and rights which can be abused to gain new capabilities and rob Canadian entities of the economic benefits of their work. Examples include: patents; rights to deliver a service; or permission to enter Canada. Often the licenses are not the objective themselves, but rather the means to the threat actor's ultimate goal.

In total, CSIS contacted more than 225 entities across Canada and briefed at least 2000 Canadian stakeholders during the COVID-19 pandemic in 2020. As the pandemic moves into new critical phases through 2021, CSIS will continue to engage vulnerable Canadian sectors to ensure they are aware of the threats of espionage and foreign interference targeting their innovation and intellectual property. This will allow them to take proactive steps to mitigate these threats, protecting their work as well as Canada's economic security and future prosperity.

## CSIS SUPPORT TO THE GOVERNMENT OF CANADA'S PANDEMIC RESPONSE

From the outset of the pandemic, CSIS monitored and advised the Government of Canada on threat actors' exploitation of the spread of COVID-19 for geo-strategic purposes, including activities that constituted potential threats to Canada's national response to the pandemic. CSIS's support to the government's pandemic response efforts included the distribution of unclassified and classified intelligence reports to provide senior decision-makers with up-to-date situational awareness and to alert partners to specific national security threats.

As the pandemic progresses, CSIS will continue to be a trusted source of advice for government partners, including Public Services and Procurement Canada, the Public Health Agency of Canada, Health Canada, and the Canadian Armed Forces on vaccine procurement, logistics, and other efforts by the Government of Canada. CSIS will continue to work closely with the other members of Canada's security and intelligence community, as well as allied partners, to help protect Canada's pandemic response from potential national security threats.



The Threat  
**ENVIRONMENT**

## ESPIONAGE AND FOREIGN INTERFERENCE

As a core part of its mandate, CSIS investigates and advises the Government of Canada on threats posed by espionage and foreign influence activities. The *CSIS Act* defines foreign influence 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 country using both state and non-state entities, including state proxies and co-optees. These activities are directed at Canadian entities both inside and outside of Canada, and directly threaten national security.

In the midst of the COVID-19 pandemic, espionage and foreign interference threats continue to persist and, in some areas, are increasing. Canada’s advanced and competitive economy, and its close economic and strategic partnership with the United States, makes it an ongoing target of hostile foreign state activities. Similarly, Canada’s efforts to protect and enhance the international rules-based system and to work with key partners on significant foreign policy issues of concern, as well as its status as a founding member of the North Atlantic Treaty Organization (NATO) and its participation in a number of bilateral and multilateral defence and trade agreements, makes it an attractive target for espionage and foreign interference.

Canadian interests can be damaged by espionage activities through the loss of sensitive and proprietary information or leading-edge technologies, and through the unauthorized disclosure of classified and sensitive government information. While federal, provincial, and municipal levels of Canadian government are of interest, foreign states such as

the People’s Republic of China and Russia also target non-governmental organizations in Canada — including academic institutions, the private sector, and civil society. In 2020, the People’s Republic of China, Russia, and other foreign states continued to covertly gather political, economic, and military information in Canada through targeted threat activities in support of their own state development goals. To accomplish this, these states take advantage of the collaborative, transparent, and open nature of Canada’s government, economy and society, often using “non-traditional collectors” including those with little to no formal intelligence training — such as researchers, private entities, and other third parties — to collect information and expertise of value on behalf of the state.

Foreign governments also continue to use their state resources and their relationships with private entities to conduct clandestine, deceptive, or threatening foreign interference activities in Canada. In many cases, these clandestine influence operations are meant to support foreign political agendas or to deceptively influence Government of Canada policies, officials, or democratic processes. An example of significant concern are activities by threat actors affiliated with the People’s Republic of China that seek to leverage and exploit critical freedoms that are otherwise protected by Canadian society and the Government in order to further the political interests of the Communist Party of China.

Foreign powers have attempted to covertly monitor and intimidate various Canadian communities in order to fulfil their strategic and economic objectives. When engaging in such activities, foreign states target members of vulnerable communities and groups who often lack the means to protect themselves. These communities often fear state-backed or

state-linked retribution targeting both themselves and possibly their loved ones in Canada and abroad. When community groups in Canada are subjected to such harassment, manipulation, or intimidation by foreign states that are either seeking to gather support or mute criticism of their policies, these activities constitute a threat to Canada's sovereignty and to the safety of Canadians. Furthermore, by aggressively conducting such activities, foreign actors have shown disregard for Canadian government institutions and their mandates to keep Canada and Canadians safe.

On 8 January, 2020, the Ukraine International Airlines Flight PS752 was shot down 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. There are 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.

While foreign interference conducted by hostile state actors and their proxies most often occurs in the form of human interaction, the manipulative activities of foreign entities on a range of online social media platforms are increasingly of concern. Most recently, such state-sponsored manipulation, including through disinformation, has sought to reshape or undermine certain narratives to sow doubt about the origins of the coronavirus and pandemic as well as the means required to counter it; discredit democratic responses to COVID-19 while casting their own responses as superior; and erode confidence in Canada's values of democracy and human rights. Russia and Russian Intelligence Services have, for example, been actively engaged in disinformation campaigns since

March 2020 in an effort to blame the West for the COVID-19 pandemic. This is part of a broader campaign to discredit and create divisions in the West, promote Russia's influence abroad, and push for an end to Western sanctions.

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.

### Protecting Democratic Institutions

Democratic institutions and processes around the world, including elections, have increasingly become the targets of foreign threat actors. Canada's role as a middle power with the ability to influence like-minded allies and liberal multilateral institutions makes its democratic institutions and processes an especially attractive target. Although Canada's electoral system is strong, threat actors have sought to target its politicians, political parties, elections, and media outlets in order to manipulate the Canadian public and interfere with Canada's democracy. Certain states may seek to manipulate and misuse Canada's electoral system to further their own national interests; 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 elections was the creation of the Security and Intelligence Threats to Election (SITE) Task Force. As an active partner in SITE, CSIS works 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.

## Economic Security

Prior to 2020, the use of economic activities by hostile state actors to harm Canada's national security interests was already a priority for CSIS. The COVID-19 pandemic has accelerated these efforts. Throughout 2020, and especially since March, foreign threat actors — including hostile intelligence services and those working on their behalf — have sought to exploit the social and economic conditions created by the pandemic to gather valuable political, economic, commercial, academic, scientific, and military information. Moreover, these threat actors engaged in covert, deceptive foreign interference activities to advance their own pre-pandemic strategic interests. These threats often involve traditional and non-traditional methods of intelligence collection, including human or cyber-espionage, foreign investment, manipulation of imports and exports, exploitation of licences and rights, and attacks on knowledge such as academic espionage.

CSIS continues to collect intelligence and advise government partners on threats to Canada's national security and prosperity interests. For example, in April 2020 the Government of Canada issued its *Policy Statement on Foreign Investment Review and COVID-19*, which committed to ensuring that inbound investment during the pandemic would not introduce new risks to Canada's economy, national security, or the health and safety of Canadians. CSIS played a key role in providing additional national security scrutiny to investments related to public health or the supply of critical goods and services, as well as enhanced scrutiny of any investments by, or under the influence of, foreign governments. These enhanced efforts are expected to continue until the economy recovers from the effects of the COVID-19 pandemic.

## CYBER THREATS

Cyber-espionage, cyber-sabotage, cyber-foreign influence and cyber-terrorism pose significant threats to Canada's national security, its interests and its economic stability. Canada remains a target for malicious cyber activities and a platform from which hostile actors attempt computer network operations (CNOs) against entities in other countries. The increasing interconnectedness of the world presents cyber actors with more opportunities than ever to conduct malicious activity. The dramatic rise of individuals working from less secure home office environments due to the pandemic significantly increases the risk of sensitive information and networks being exposed to malicious cyber activity.

Cyber actors conduct malicious activities to advance their political, economic, military, security, and ideological interests. They seek to compromise both government and private sector computer systems by manipulating their users or exploiting security vulnerabilities. New and emerging technologies such as artificial intelligence offer threat actors potential new ways to compromise computer systems. State-sponsored cyber threat actors use CNOs to steal intellectual property or trade secrets, or to achieve geopolitical objectives through the disruption of critical infrastructure and vital services, interference with elections, or to conduct disinformation campaigns. In 2020, a cyber espionage group linked to Russian intelligence services conducted CNOs directed towards Canadian, British, and American-based organizations that were involved in COVID-19 response and recovery efforts. These malicious cyber activities were believed to be an attempt to steal information and intellectual property related to the development and testing of COVID-19 vaccines. Of similar concern, non-state actors, including terrorist groups, have



also attempted to conduct CNOs to further their ideological objectives, such as recruiting supporters, spreading propaganda, or encouraging violence against specific individuals or groups.

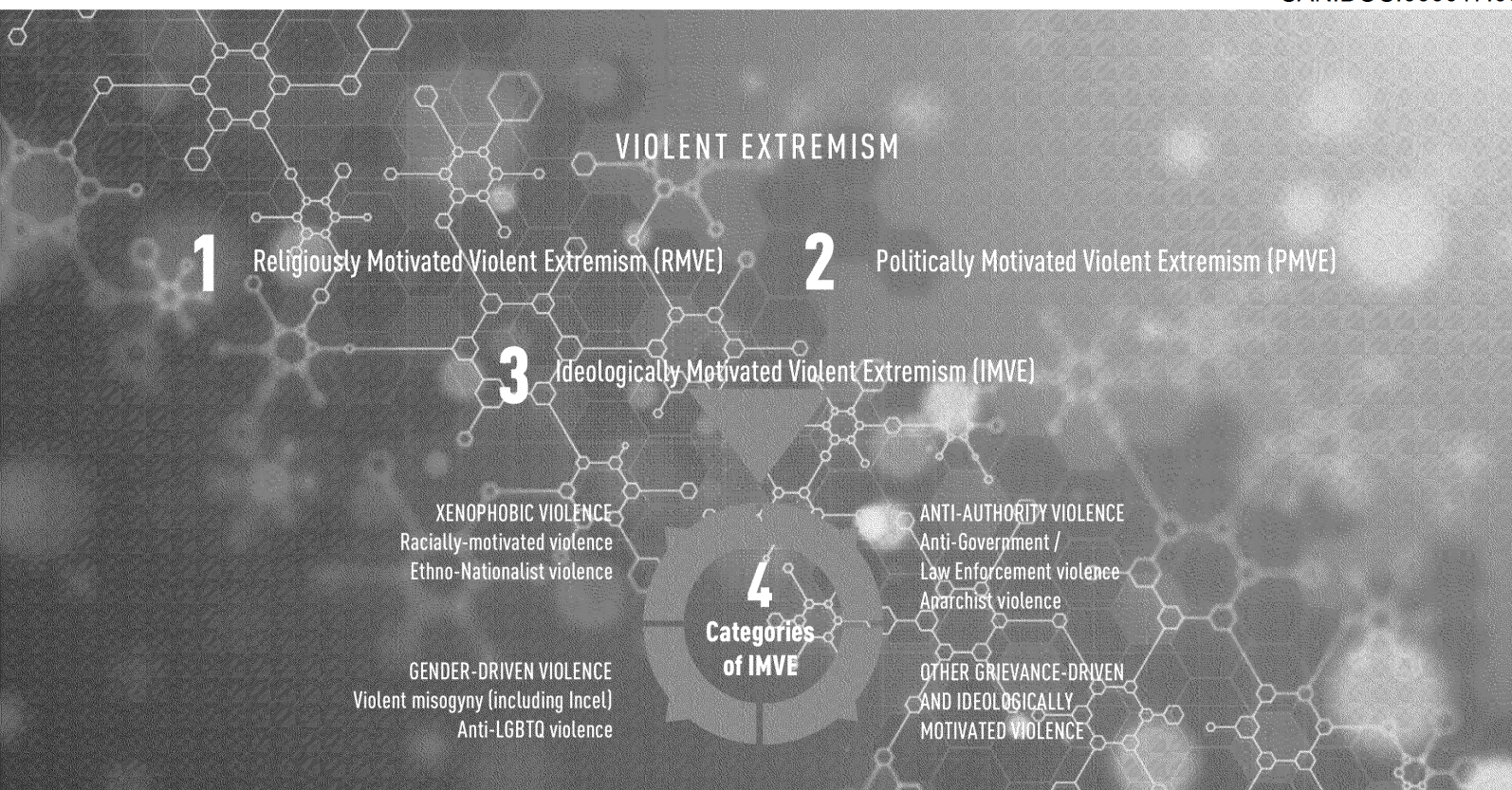
Threat actors have also compromised third-party vendor software or equipment in order to conduct cyber-operations against that vendor's clients. In 2020, a state-sponsored cyber threat actor modified an update mechanism for a popular brand of network management software which allowed the actor to gain covert access to thousands of government and private sector networks around the world. The effect of this kind of attack is profound.

*Canada's National Cyber Security Strategy* views cyber-security as an essential element of Canadian innovation and prosperity. CSIS plays an active role in shaping and sustaining our nation's cyber resilience through collaborative action with partners to respond to evolving threats of malicious cyber activity. While CSIS, the Communications Security Establishment (CSE), the Royal Canadian Mounted Police (RCMP), and other key government partners have distinct and separate mandates, they share a common goal of keeping Canada, Canadians, and Canadian interests safe and secure online. In today's global threat environment, national security — including cyber security — must be a collaborative effort. In responding to cyber threats, CSIS carries out investigations into cyber attacks 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.

## COUNTER PROLIFERATION

Several foreign states continue their clandestine efforts to procure a range of sensitive, restricted, and dual-use technologies and goods in Canada. These technologies and goods can be used to develop weapons of mass destruction (WMD) programs and associated delivery vehicles.

In August 2020, evidence indicates that Russian state threat actors used a nerve agent of the Novichok group to poison leading Russian opposition figure, Alexei Navalny. This attack contravened international norms prohibiting the use of chemical weapons and was strongly condemned by the Government of Canada. The event is also particularly troubling as it represents another instance of Russian state actors using chemical weapons to stifle dissent.



## IDEOLOGICALLY MOTIVATED VIOLENT EXTREMISM

Since 2014, Canadians motivated in whole or in part by their extremist ideological views have killed 21 people and wounded 40 others on Canadian soil — more than religiously motivated violent extremism (RMVE) or politically motivated violent extremism (PMVE). In early 2020, for example, a Canadian minor motivated by the involuntary celibate (Incel) ideology was charged under the terrorism provisions of the *Criminal Code*.

Proponents of ideologically motivated violent extremism (IMVE) are driven by a range of influences rather than a singular belief system. IMVE radicalization is more often caused by a combination of ideas and grievances resulting in a personalized worldview that is inspired by a variety of sources

including books, videos, online discussions, and conversations. The resulting worldview often centres on the willingness to incite, enable or mobilize to violence. These individuals and cells often act without a clear affiliation to a specific organized group or external guidance, but are nevertheless shaped by hateful voices and messages online that normalize and advocate violence.

The COVID-19 pandemic has exacerbated xenophobic and anti-authority narratives, many of which may directly or indirectly impact national security considerations. Violent extremists continue to exploit the pandemic by amplifying false information about government measures and the virus itself on the internet. Some violent extremists view COVID-19 as a real but welcome crisis that could hasten the collapse of

Western society. Other violent extremist entities have adopted conspiracy theories about the pandemic in an attempt to rationalize and justify violence. These narratives have contributed to efforts to undermine trust in the integrity of government and confidence in scientific expertise. While aspects of conspiracy theory rhetoric are a legitimate exercise in free expression, online rhetoric that is increasingly violent and calls for the arrest and execution of specific individuals is of increasing concern.

In 2020, CSIS has assessed that threat narratives within the IMVE space have evolved with unprecedented multiplicity and fluidity. Broadly speaking, IMVE conspiracy theories are often influenced by decentralized online trends and communities of extremist influencers who interpret local, national and international events through a radical lens. These broader narratives are often individualized by extremists and are impacted by perceived concerns regarding economic well-being, safety and security, the COVID-19 pandemic or other special events.

## 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.

## RELIGIOUSLY MOTIVATED VIOLENT EXTREMISM

Religiously motivated violent extremism (RMVE) encourages the use of violence as part of a spiritual struggle against a perceived immoral system. Followers believe that salvation can only be achieved through violence.

While there were no RMVE inspired attacks that occurred in Canada during 2020, the threat remains as these attacks can be planned and executed swiftly with little warning. RMVE-inspired attacks tend to be low in sophistication, and can involve firearms or another device, weapon, or tool that can cause maximum damage in a crowded public venue. CSIS assesses that the COVID-19 pandemic has not disrupted online RMVE narratives. In fact, as a result of individuals spending more time online and therefore potentially becoming more exposed to online messaging, CSIS assesses that COVID-19 has potentially increased the threat of RMVE radicalization among certain threat actors.

## CANADIAN EXTREMIST TRAVELLERS

The Government of Canada continues to monitor and respond to the threat of Canadian extremist travellers (CETs). CETs are individuals who have a nexus to Canada through citizenship, permanent residency, or valid visa and 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.

Due to the effects of the COVID-19 pandemic, the number of CETs has remained relatively stable over 2020. CSIS is aware of CETs who have travelled to Turkey, Syria, and Iraq, as well as Afghanistan, Pakistan, and parts of North and East Africa. These individuals have left Canada to support and facilitate extremist activities and, in some cases, directly participate in violence. Similarly, the number of individuals with a nexus to Canada who engaged in extremist activities abroad and have returned to Canada has also remained stable.

Since 2011, the conflict in Syria and Iraq has attracted unprecedented numbers of extremists to fight overseas. However, since the decline of the so-called Caliphate in 2017, many of these individuals have been killed or are currently being detained in internally displaced persons (IDP) camps or prisons. Roughly half of the detainees are women with children. Since the onset of the global COVID-19 pandemic, the movement of CETs in Turkey, Syria, and Iraq has been curtailed due to enhanced border and travel restrictions.

Five Eyes partners, including the Australian Security Intelligence Organisation, have recently noted that, for the first time, an Ideologically Motivated Violent Extremist was prevented from travelling offshore to fight on a foreign battlefield due to passport cancellation based on an adverse security assessment. This example further demonstrates the complexity of extremist travellers as these threat actors can transcend multiple violent extremist groups and movements.

CSIS is aware of the serious threat posed by CETs who return from conflict zones. The range of training and operational experience they acquire while abroad and the unique environment to which they have been exposed make CETs an especially dangerous threat to the security of Canada. While the pandemic degraded the possibility of CETs returning to Canada, CSIS and other Government of Canada departments and agencies remain engaged as a community to collectively manage the possible threat posed by returning Canadian extremists.

## INTERNATIONAL TERRORISM

The al-Qaida network suffered significant leadership losses in 2020 with the assassination of its deputy leader and the elimination of other regional leaders in the Arabian Peninsula (AQAP), Islamic Maghreb (AQIM), and Hurras ad-Din (HAD). The conditions of the February 2020 agreement between the United States and the Taliban also place restrictions on al-Qaida activity in Afghanistan. Despite the death of the AQIM emir in June 2020, al-Qaida remains resilient in West Africa where affiliates maintain influence in central and northern areas of Mali. Frequent international military operations targeting al-Qaida affiliate, Al Shabaab, have not prevented the group from expanding its geographic area of control in Somalia nor limited its capabilities to carry out attacks against both soft and hard targets. While al-Qaida-affiliated and aligned groups in Africa as well as the Middle East have generally had a local or regional focus, RMVE inspired attacks continue to pose a threat to Canada.

Following the loss of its physical territory in 2019, Daesh prioritized its rural-based insurgencies in Syria and Iraq with the intent of expanding into urban centres. This is a conditions-based rather than time-based objective that may be connected to future withdrawals of US-led coalition forces. Daesh has successfully exploited the pandemic to surge attacks regionally and internationally with successive attack campaign messaging.

The online threat environment became increasingly decentralized and fragmented since Daesh's loss of physical territory in 2019 and remained so in 2020. Certain social media platforms remained popular for propaganda dissemination however, other niche platforms have since emerged where CSIS has observed activity driven by the

creativity and persistence of Daesh supporters rather than by Daesh media officials. There is an apparent increase in propaganda that has been developed by media personnel with no formal affiliation to Daesh. This propaganda ranges from calls for attacks against domestic targets to videos celebrating and promoting Daesh, and serves to fill gaps left by a decrease in official Daesh media, thereby augmenting and amplifying official Daesh messaging as part of a robust online RMVE narrative.

CSIS assesses that the primary threat posed by Daesh to Western countries, including Canada, continues to be violent extremist attacks, inspired by online propaganda in parallel to Daesh's insurgencies.

## Africa

Both al-Qaida and Daesh affiliates continued to conduct attacks on Western interests throughout West and East Africa. The loss of physical territory in Iraq and Syria has not impacted the spread of Daesh affiliates in Africa. The porous nature of African borders, coupled with the ineffectiveness of many regional counterterrorism (CT) forces, allows affiliates to establish bases of operations in ungoverned spaces outside capital cities. There remains a significant threat to Canadians who work or travel in these regions as they may fall victim to an attack or an opportunistic kidnap for ransom operation. Al-Qaida affiliate Jamaat Nusrat al-Islam Wal Muslimin (JNIM) continues to destabilize Mali, Niger and Burkina Faso with frequent and complex attacks. Al-Qaida-aligned al-Shabaab remains the dominant terrorist group in the Horn of Africa and has not been hampered by military activities by the United States and other foreign partners. Daesh affiliates in the Greater Sahara, West, Central, and East Africa have conducted successful attacks against regional CT

forces. Daesh is focused on expanding and aligning with jihadist groups across East Africa, most notably in Somalia, the Democratic Republic of the Congo, and Mozambique. Due to the global reach of al-Qaida and Daesh, both groups continue to pose an ongoing threat to Canada's national security.

## Afghanistan and Pakistan

In late February 2020, the United States and the Taliban signed an agreement that laid out the conditions for a full withdrawal of Coalition forces from Afghanistan by May 2021. This withdrawal is conditional on the Taliban's participation in the Afghan Peace Negotiations, an end to Taliban attacks on foreign forces, and the Taliban's commitment not to cooperate with al-Qaida and other non-Afghan militant groups — or permit the use of Afghan territory to attack the United States or its allies. The Coalition intervention in Afghanistan that followed the September 11, 2001, terrorist attacks — and involved a Canadian military force from 2002 to 2014 that peaked at over 2,000 personnel — is drawing to a close.

As of late 2020, the Taliban controlled or dominated large parts of Afghanistan and maintained a presence in Pakistan. Since the Afghan government is determined not to become a theocracy or abandon the economic, political, and social progress made since 2002, the conflict will likely continue in 2021, intensifying the situation for the people of Afghanistan, its regional security, and Canadian interests in the region.

Many non-Afghans, including al-Qaida- and Daesh-aligned foreign fighters, remain active in the region. The Islamic State of Khorasan Province (ISKP) has become the most active Daesh affiliate outside of Syria and Iraq. ISKP has successfully launched high-profile lethal attacks in Afghanistan, including against a prison on August 2-3, 2020, to release hundreds of

its imprisoned members. COVID-19, the Taliban, and Coalition Forces have thus far been unsuccessful in disrupting ISKP.

## SECURITY SCREENING

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

The CSIS Government Security Screening (GSS) program conducts investigations and provides security assessments or advice on a wide range of threats to national security. The security assessments are one 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 and not with CSIS.

The GSS also conducts screening to protect sensitive sites from national security threats, including but not limited to airports, marine, and nuclear facilities. It assists the RCMP by vetting Canadians and foreign nationals who seek to participate in major events in Canada. Finally, it provides security assessments to provincial and foreign governments, in addition to 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 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

<b>REQUESTS RECEIVED*</b>	<b>2019–2020</b>
Permanent Resident Inside and Outside Canada	18,000
Refugees (Front-End Screening**)	46,400
Citizenship	216,800
Temporary Resident	43,300
<b>TOTAL:</b>	<b>324,500</b>

## GOVERNMENT SCREENING PROGRAMS

<b>REQUESTS RECEIVED*</b>	<b>2019–2020</b>
Federal Government Departments	75,500
Free and Secure Trade (FAST)	18,100
Transport Canada (Marine and Airport)	52,100
Parliamentary Precinct	2,400
Nuclear Facilities	10,600
Provinces	240
Others	2,700
Foreign Screening	570
Special Events Accreditation	5,000
<b>TOTAL:</b>	<b>167,210</b>

\*Figures have been rounded

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





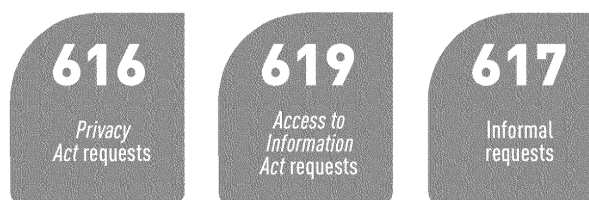


Engagement with  
**CANADIANS**

## TRANSPARENCY

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. It is this communication which enables Canadians to trust their security intelligence service. As part of efforts to be more transparent, CSIS has committed to making information about some of the organization's activities more open, while ensuring there is no risk or compromise to national security. Through public forums, public communications, and social media platforms, CSIS endeavours to communicate transparently about decision making processes and national security activities.

In 2020 CSIS continued its work 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's own long-established commitment with Canadians.



Access to Information and Privacy Statistics

CSIS's regular engagement with NS-TAG over the course of 2020 culminated in a December appearance by Director Vigneault to discuss a variety of topics including CSIS's proactive engagement with the biopharma and healthcare sectors, ongoing work to increase diversity and inclusivity in national security, CSIS's work with its review bodies and the need to modernize CSIS's authorities.

## OUTREACH

CSIS builds important linkages to Canadians through open and transparent collaboration. Primarily driven through the work of the Academic Outreach and Stakeholder Engagement program, CSIS builds relationships that help develop a better understanding of current and emerging security concerns while informing public understanding of both national security issues and CSIS's mandate and activities. This work contributes to CSIS's transparency and accountability commitments while also ensuring that CSIS is recognized as a sophisticated and responsive security intelligence service, trusted by Canadians to uphold and defend Canadian interests in an increasingly complex geopolitical environment.

## Engagement with academia

As an advanced economy and open and free democracy, Canada has long been targeted by persistent and sophisticated threat activity. This activity, which is conducted to gain information and intelligence as well as influence in order to advance the national interests of a foreign state, targets Canadian entities, including and especially academic institutions. This activity threatens Canada's core values, vital assets and knowledge-based economy.

As a result and throughout 2020, CSIS provided advice on espionage and foreign interference threats to national security to Canadian post-secondary institutions to ensure they are aware of the threat environment and have the information they need to make informed decisions as well as implement pre-emptive security measures.

Despite the challenging conditions of the pandemic, CSIS was able to contribute to informed dialogue on national security issues by drawing on subject matter expertise in academia and hosting 16 virtual events, commissioning 25 reports, and coordinating CSIS expert briefings for numerous external stakeholders. Covering key national security priorities, as well as issues such as mental health and coping during a pandemic, social license, and GBA+ initiatives, CSIS facilitated collaboration and information sharing between CSIS and external sources of expertise to create an environment of continuous learning, challenge assumptions and unconscious bias and to support innovation. During the year, CSIS employees participated in class and seminar discussions in over thirty universities across eight provinces. In addition to broadening the awareness of students about CSIS, the effort also supported the organization's proactive recruitment strategy by organizing virtual 'job fairs' to coincide with the presentation by CSIS's employees.

## Engagement with innovation sectors

Over the year, CSIS established trusted, reciprocal relationships with academia, industry, and other levels of government. The primary focus during the year was coordination of the COVID-19 outreach initiative and the development of relationships with stakeholders in the biopharmaceutical, research, life sciences and data sectors, as well as in the logistics, distribution and supply chain sectors. In 2020, CSIS provided hundreds of threat briefings and offered tailored threat mitigation advice to assist these sectors to take meaningful measures to protect Canadian research and economic interests. CSIS also used additional forms of engagement including the targeted publication of articles in industry magazines.

## Engagement with communities

CSIS has invested significant effort in building relationships with individuals, communities and community leaders to establish and sustain trust. CSIS's ongoing offer of support and commitment to work in partnership with these communities is not only good practice but serves in protecting individuals from intimidation or other hostile activities by foreign state actors.

For example, the tragic downing of flight PS752 prompted important outreach with Iranian-Canadian communities through targeted communication with various groups and community leaders. These discussions opened the door to future engagement opportunities. Similarly, following the tragic Toronto Mosque attack, CSIS engaged with important leaders in the Muslim community and is committed to continuing more proactive engagement.

These examples are an important demonstration of how CSIS continues to encourage all Canadian communities to engage in important discussions in order to help communities and have a more informed society on the national security threats that face Canada.

## CSIS ACADEMIC OUTREACH AND STAKEHOLDER ENGAGEMENT

Engaging with partners and stakeholders in sectors including academia, industry, non-governmental, and community organizations and other levels of government

Supporting operational activities by connecting staff and decision-makers with external sources of information and diverse perspectives

Commissioning and disseminating research and expert analysis to inform operational activities and public dialogue on national security issues

Fostering trust by providing a human face of CSIS, dispelling myths, and building reciprocal relationships



The People of  
**CSIS**

## DIVERSITY AND INCLUSION

CSIS has been working to integrate new strategies and approaches to remove systemic barriers and broaden the organization's understanding, appreciation, and valuing of diversity of all types. CSIS turned to its people, systems, and culture to implement this change. Recognizing the importance and value of including diversity and inclusion elements in CSIS's practices and policies helps CSIS deliver its mandate more effectively.

In 2020, CSIS began developing a comprehensive Diversity and Inclusion Strategy to address bias, inclusive leadership, recruitment, career and development opportunities, and open communication on difficult issues such as systemic racism. This work complements the CSIS Accessibility Strategy with the purpose of ensuring a barrier-free workplace.

## CODE OF CONDUCT

Protecting Canada's national security and that of its citizens is a critical job — and how CSIS employees conduct themselves and interact in the workplace is just as important. 2020 marked an important step in the organization's commitment to providing a healthy and respectful workplace for all of our employees by publishing the CSIS Code of Conduct. CSIS employees are at the heart of this new Code of Conduct which was developed following extensive consultation across the organization to give every employee an opportunity to directly contribute to its development. In addition to adherence as a condition of employment, the CSIS Code of Conduct clearly articulates what is expected of employees and ensures accountability for fostering a respectful workplace. It puts forward the values employees are committed to uphold in their work environment: respect for people, respect for democracy, integrity, stewardship, and excellence. In all decisions, it is expected that CSIS considers, discusses and challenges itself to uphold these values in the workplace and in the work done for Canadians.

## In 2020, CSIS has:

- Implemented and published a new Code of Conduct and related policies designed to integrate a healthy, respectful, and harassment-free workplace, to which all employees must affirm their adherence annually, as a condition of their employment;
- Continued the *Respect Campaign* launched in 2019 as part of a workplace transformation with the goal of promoting a safe, respectful, and inclusive environment through proactive prevention;
- Facilitated GBA+ consultation in development of fair and equitable policies, programs, and practices, and ensured that GBA+ advice was reflected in major initiatives — including input to workforce mobility policies and practices, new operational technology, pandemic business continuity and resumption plans, the Public Safety Bias Sensitivity Diversity and Identity for National Security Framework, a Diversity & Inclusion review, Government of Canada Workplace Charitable Campaign events, and the CSIS People Management Framework;
- Placed substantial focus on diversity and inclusion in discussions with executives across the organization, and held a dedicated session underscoring the accountability and importance of leaders and leadership in this domain — an accountability that is explicit in every executive's performance agreement;
- Implemented new strategies to increase hiring of employees from diverse groups;
- Developed a catalogue of relevant learning opportunities for all employees, including training that addresses issues such as bias, racism, and discrimination; and
- Celebrated cultural events that are important to employees and are reflective of CSIS's diverse workforce, and developed a plan in collaboration with employees to ensure important multicultural events and days are recognized.

**While recognizing there is more work to be done, CSIS is committed to taking meaningful action to ensure the organization reflects and supports the diverse and inclusive Canadian communities it protects.**

# CSIS across CANADA







# INTERNET

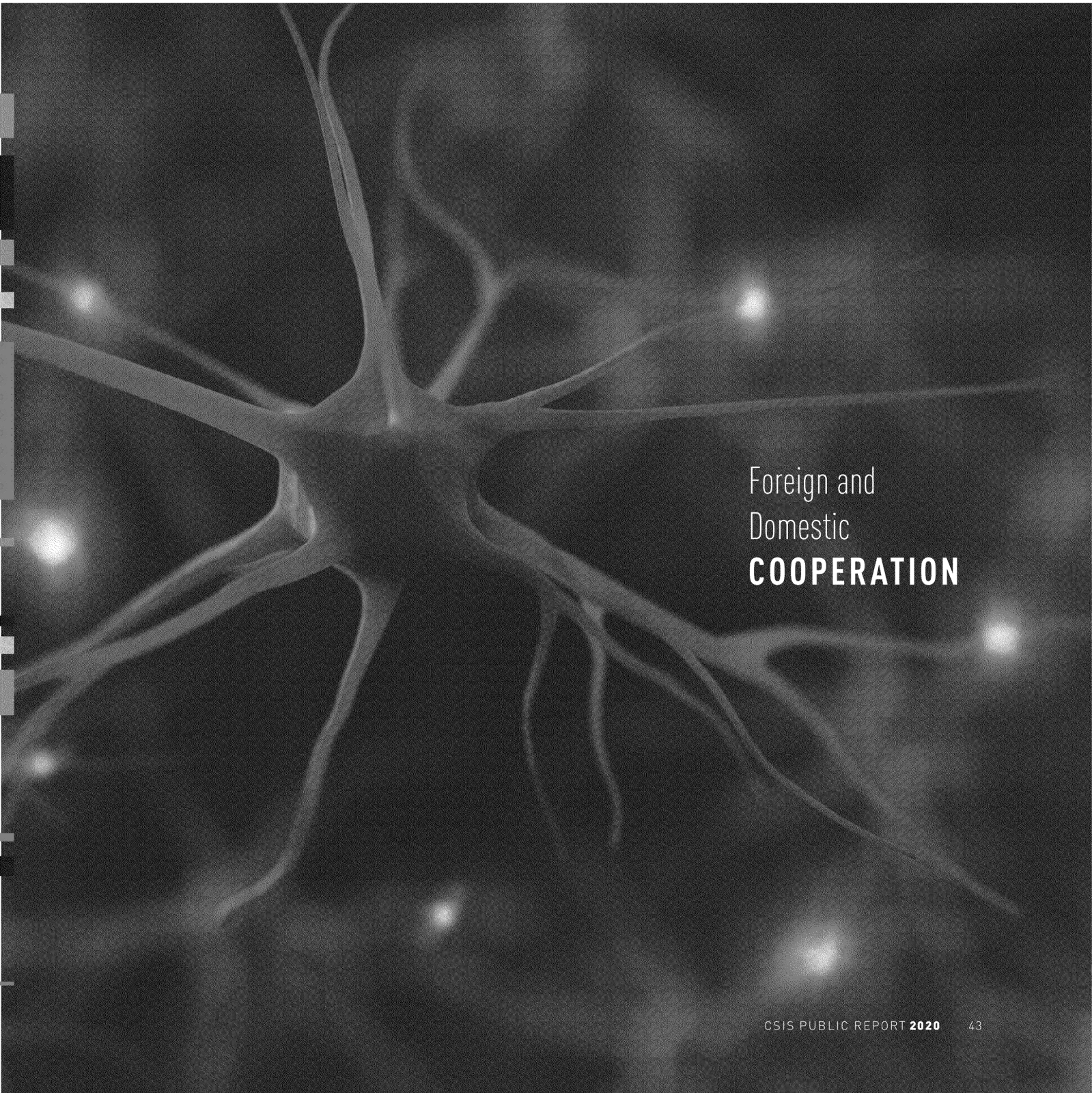
While CSIS has regional and district offices across Canada that are responsible for intelligence collection to fulfill CSIS's mandate, there are also CSIS offices located around the world. These offices, often referred to as "foreign stations," are responsible for CSIS's activities and include, for example, the CSIS office in the Canadian diplomatic mission in Washington.

These offices work to maintain CSIS's international presence. CSIS has forged over many years, and collect information on threats to Canada's national security. The world is more inter-connected than ever before, and not all national security threats to Canada emerge within Canada's borders. Many threats to Canada's national security have a nexus to someone or something located elsewhere in the world — whether that be an

philosophy, a terrorist actor or a criminal organization. CSIS's foreign stations investigate these threats to national security before they reach Canada's borders.

In 2020, CSIS's international work was impacted by the pandemic as many countries instituted severe measures to control the spread of the virus including border closures, travel restrictions and meeting restrictions, lockdowns, and curfews. While these measures presented challenges, CSIS employees displayed great ingenuity and resilience to maintain communication with important international partners despite the difficulties presented by the pandemic. CSIS's intelligence continued to flow, including the timely delivery of information that assisted in CSIS's significant work on outreach with the health and life science sectors.





Foreign and  
Domestic  
**COOPERATION**

## FOREIGN AND DOMESTIC COOPERATION

The increasingly interconnected and global nature of security threats means that CSIS cannot fulfill its mandate in isolation. Foreign information sharing has been and remains fundamental to the Government of Canada's national security requirements. Cooperation with foreign agencies provides CSIS access to timely information linked to a number of potential or specific threats, and allows CSIS to obtain information which might otherwise not be available to Canada.

CSIS has more than 300 foreign relationships in 150 countries and territories, each authorized by the Minister of Public Safety and Emergency Preparedness, 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. Additionally, CSIS officers stationed in various countries around the world collect and share security intelligence information related to threats to Canada, its interests, and its allies.

CSIS opposes in the strongest possible terms the mistreatment of any individual by a foreign agency. As part of its foreign information-sharing framework and policies, CSIS assesses all of its foreign arrangements, including human rights reputations within the security intelligence communities of all countries with which there is an established arrangement.

CSIS engagement with foreign entities must align with Canada's laws and legal obligations. This includes ensuring CSIS remains fully compliant with the requirements outlined in the *Avoiding Complicity in Mistreatment by Foreign Entities* (ACMFE) Act. CSIS provides an annual report to the Minister of Public Safety and Emergency Preparedness outlining CSIS's implementation of those requirements during the previous calendar year. Furthermore, s.7(2) of the *ACMFE Act* also requires CSIS to publish public information on that implementation process.

The COVID-19 pandemic has reinforced the importance of cooperation with international partners. Despite the pandemic, CSIS continues to work closely with such partners on security issues of mutual concern, including and especially regarding hostile activities by state actors and violent extremism. CSIS has continued to engage with key foreign partner agencies during the pandemic to exchange information and obtain security intelligence on threats to Canada and Canadian interests, both domestically and abroad.

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 unique mandate and legal authorities to protect Canada and Canadians from threats at home.



Review and  
**COMPLIANCE**

## COMPLIANCE

Demonstrating compliance is essential to maintaining the trust and confidence of Parliament, the Federal Court, partners and the public, while supporting accountability and transparency requirements, as well as operational effectiveness.

In the past, compliance at CSIS was addressed through managerial oversight, internal audits, as well as Inspector General and Security Intelligence Review Committee (SIRC) reviews; however, in response to internal reviews, CSIS determined there was a need to establish a formal internal compliance program.

The operational compliance program began in 2016 and has grown to be recognized as a leader in strengthening the compliance culture within CSIS. The Government also recognized the importance of investing in compliance activities by providing funding to enhance CSIS's compliance program.

Among the key activities are critical investments in 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 response to a recent Federal Court ruling that criticized CSIS for failing to meet its duty of candour obligations, CSIS has undertaken additional concrete steps to strengthen internal accountability. This includes the creation of a dedicated Affiant Unit to centralize expertise and lead warrant applications, as well as the launch of an independent review, led by a former

Deputy Attorney General, to provide recommendations. CSIS is now implementing recommendations from that review, which are critical to maintaining the confidence of the Federal Court, and Canadians, and fulfilling its mandate to keep Canada safe.

Following the Federal Court ruling, the Ministers of Public Safety and Justice referred the matter to the National Security Intelligence Review Agency (NSIRA), and NSIRA has initiated a review which CSIS is actively supporting. CSIS welcomes the findings and recommendations, including those related to measures already implemented to address the Court's concerns and additional opportunities for improvement.

## EXTERNAL REVIEW

The National Security Intelligence Committee of Parliamentarians (NSICOP) and the National Security Intelligence Review Agency (NSIRA) play a critical role in conducting an independent review of CSIS's activities, and offering recommendations for further 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 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 2020 to enable the Committees to complete their studies and prepare their reports.

# MODERNIZING Authorities

## MODERNIZING AUTHORITIES

The COVID-19 pandemic has created new vulnerabilities to be exploited by highly-capable state actors seeking to further their strategic interests to Canada's detriment. The online environment, more than ever, provides fertile ground for radicalization, recruitment and communication by a host of Ideologically- and Religiously-Motivated Violent Extremists. In the past year, CSIS has been forced to pivot its operational stance to respond to emerging and changing threats, while faced with many of the same restrictions felt by all Canadians.

CSIS's ability to respond nimbly to these dynamic threats, however, is limited by its authorities under the *CSIS Act*. There is ongoing public debate regarding the implications of privacy in the smart phone era. Canada's legal landscape as it relates to privacy and technology continues to evolve. This directly influences CSIS operations, including the way information is collected and when a warrant must be sought.

The world operates in a data-rich environment, which presents both significant opportunities, but also challenges under the current legislative framework. By necessity and according to its mandate, CSIS information is held in silos to manage privacy requirements — limiting data analytics, a potentially powerful tool to advance investigations.

The *CSIS Act* was enacted in 1984 and can present interpretive challenges today, which can have practical implications on daily investigative activities. For example, prohibitions on disclosing classified information limit how CSIS can support entities outside of Government — including municipalities, universities and critical infrastructure — that face significant national security threats. CSIS is considering the implications of the strictly necessary limitation of CSIS's core collection mandate on its activities in the online threat environment.

More work remains to be done to ensure CSIS has the right authorities and tools to be a modern intelligence agency and fulfill its mandate, which will include consideration of the conclusions and recommendations of review bodies, findings of internal reviews and Federal Court decisions. CSIS is learning from allied experiences, as these challenges are not Canada's alone. For example, both Australia and New Zealand have recently concluded major intelligence reviews that provide valuable insights for Canada. CSIS will continue to work closely with Government of Canada partners both within the Public Safety Portfolio and with the Department of Justice to ensure that CSIS can act effectively to protect national security while meeting its legal obligations and respecting the rights of Canadians.









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.

Aussi disponible en français sous le titre : Rapport public du SCRS 2019  
[www.canada.ca](http://www.canada.ca)

Published in April 2020

© Her Majesty the Queen in Right of Canada, as represented by the Minister of Public Safety and Emergency Preparedness, 2020.  
© Public Works and Government Services Canada 2020

# CSIS PUBLIC REPORT 2019



# TABLE OF CONTENTS

## **MESSAGE FROM THE DIRECTOR** 4

### *RELEVANCE*

---

## **CSIS AT A GLANCE** 7

Core Mandate, Partnerships, Duties and Functions 7

Departmental Results and Financials 8

## **THE INTELLIGENCE CYCLE** 9

## **THREATS TO THE SECURITY OF CANADA AND CANADIAN INTERESTS** 11

Terminology 11

Terrorism and Violent Extremism 12

Ideologically Motivated Violent Extremism 13

Canadian Extremist Travellers 14

Espionage and Foreign-Influenced Activities 16

Cyber Threats 18

Security Screening 19

### *EXCELLENCE*

---

## **OUR PEOPLE** 20

The CSIS People Strategy 22

Dedicated to Health and Wellness 22

GBA+ 22

Recruiting for the Mission 23

CSIS Women's Network 23

## CONFIDENCE

---

### **ACCOUNTABILITY AND TRANSPARENCY** 25

Accountabilities of the CSIS Director	25
Ministerial Direction and Accountability	27
<i>The National Security Act, 2017</i>	27
Transparency	29
Academic Outreach and Stakeholder Engagement	30

### **FOREIGN AND DOMESTIC COOPERATION** 31

### **2020 AND BEYOND: MODERNIZING CSIS' AUTHORITIES** 32

## 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 35<sup>th</sup> 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

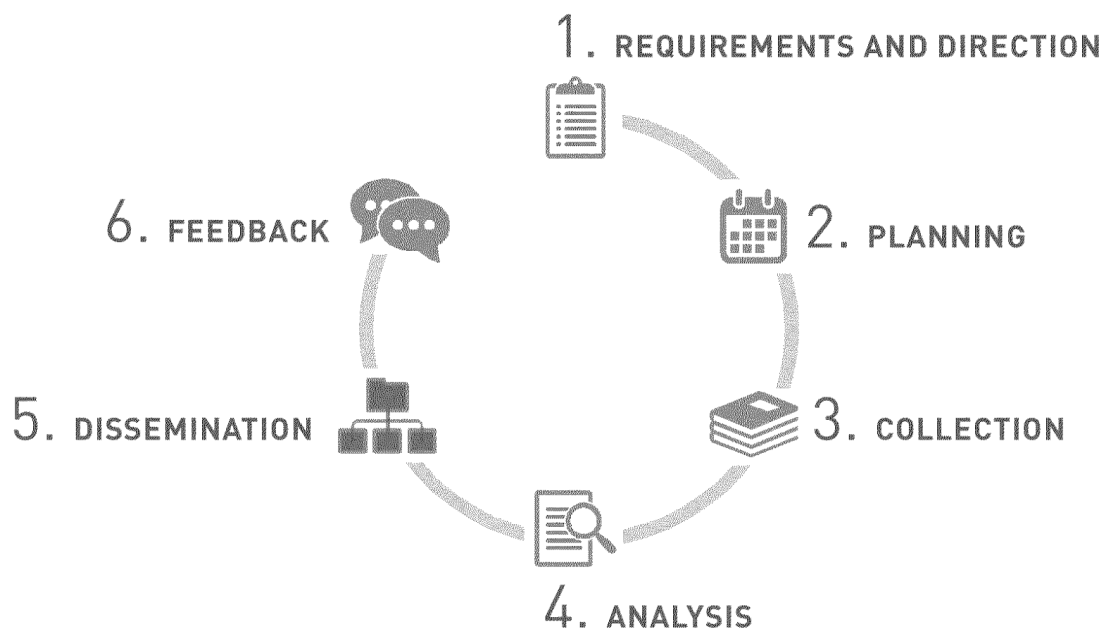
Integrated  
Terrorism  
Assessment Centre

### 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.

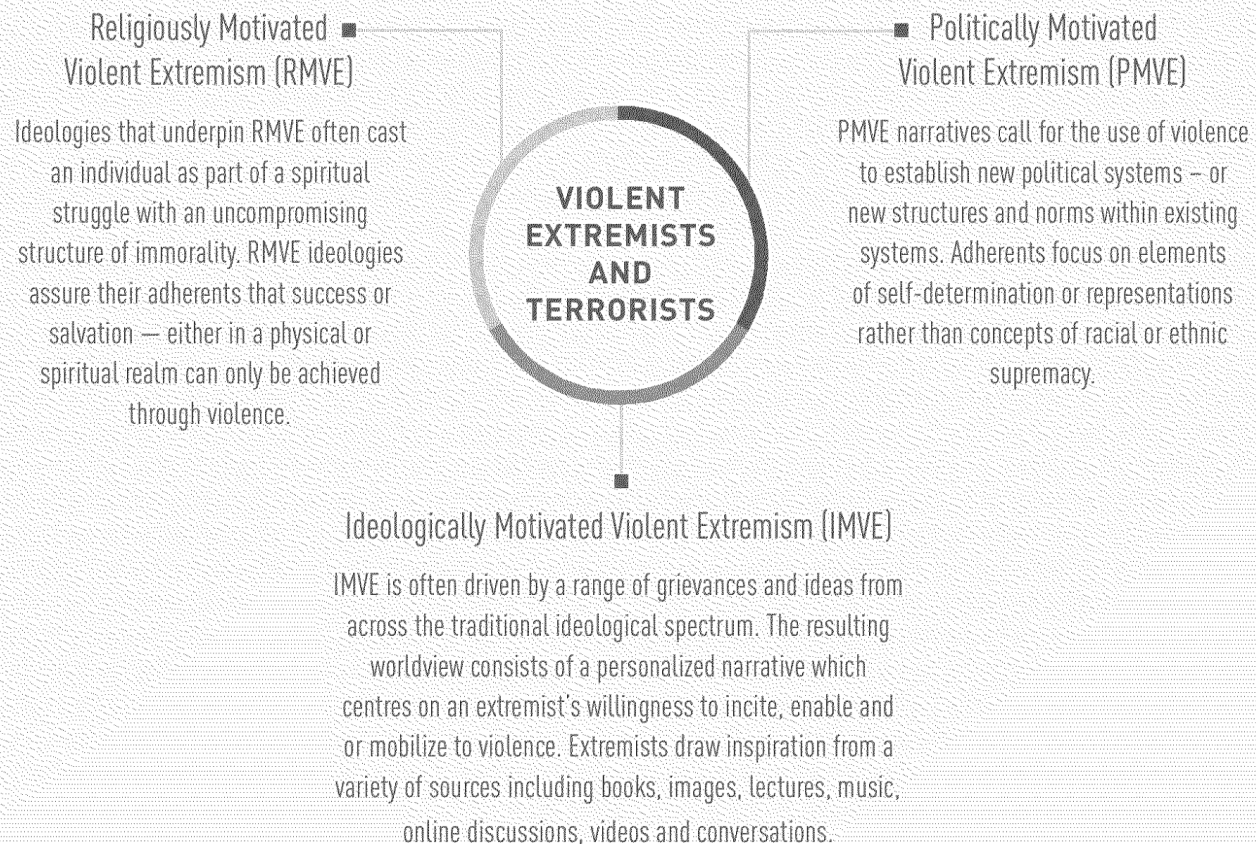
An integral part of the intelligence cycle is collecting feedback on intelligence products from all partners. CSIS gathers product specific feedback from all partners and routinely gathers requirements from the Government of Canada to help shape and drive collection and production efforts.

# 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:



## 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 lethality 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)

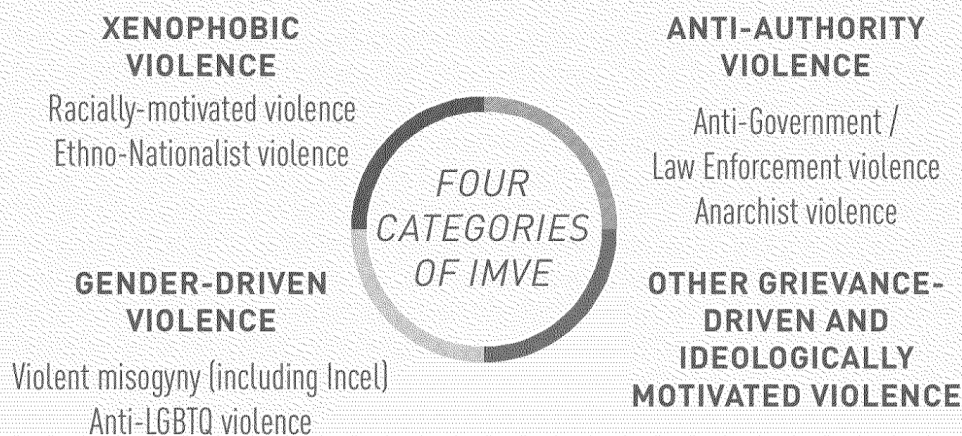
Ideologically motivated violent extremism (IMVE) is often driven by a range of grievances and ideas from across the traditional ideological spectrum. The resulting worldview consists of a personalized narrative which centres on an extremist's willingness to incite, enable and or mobilize to violence. 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
<b>TOTAL:</b>	<b>356,200</b>

## 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
<b>TOTAL:</b>	<b>168,370</b>

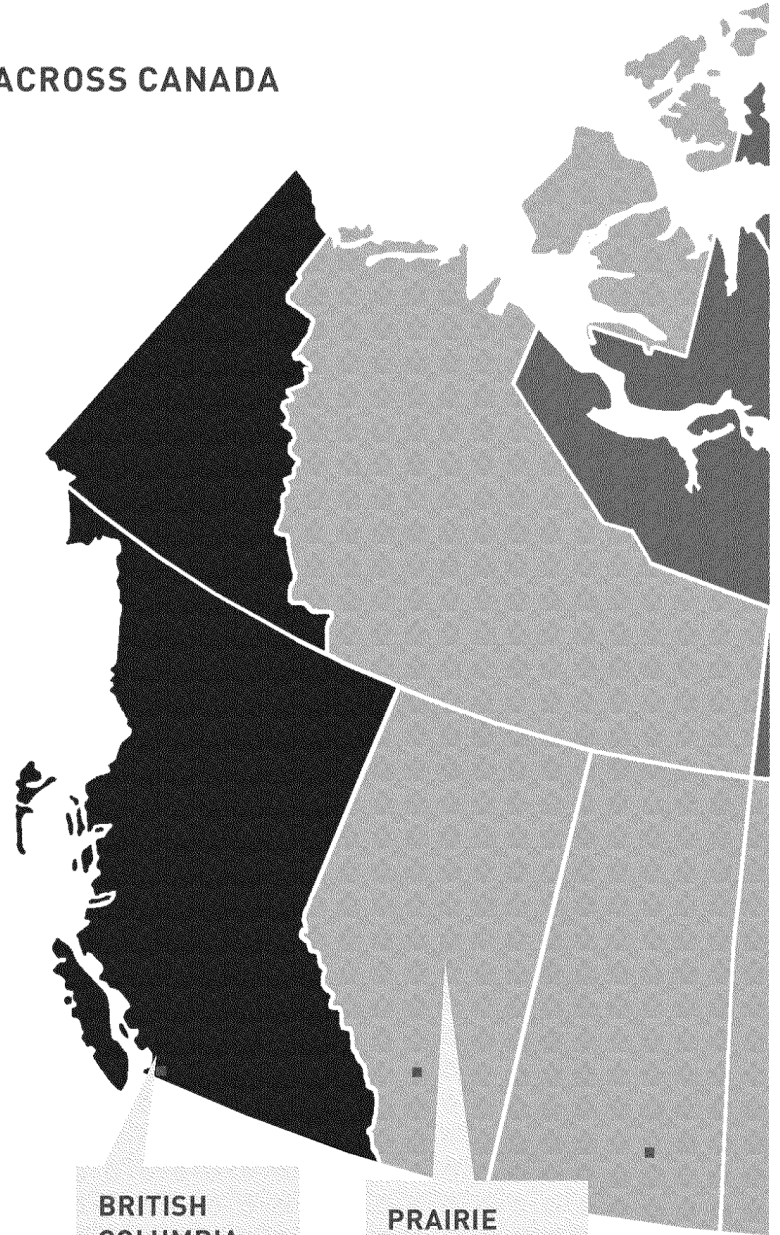
\*Figures have been rounded

\*\*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





## 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





## LEGAL

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

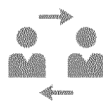
---



## 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.



Canadian Security  
Intelligence Service

Service canadien du  
renseignement de sécurité

UNCLASSIFIED



**FOREIGN  
INTERFERENCE  
THREATS TO CANADA'S  
DEMOCRATIC PROCESS**

Aussi disponible en français sous le titre : *Menaces d'ingérence étrangère visant les processus démocratiques du Canada*

[www.canada.ca](http://www.canada.ca)

Published July 2021

© Her Majesty the Queen in Right of Canada, as represented by the Minister of Public Safety and Emergency Preparedness, 2021.

Cat. No. PS74-17/2021E-PDF

ISBN: 978-0-660-39625-5

## EXECUTIVE SUMMARY

- Activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive, or involve a threat to any person, constitute foreign interference. Examples of foreign interference include attempts to covertly influence, intimidate, manipulate, interfere, corrupt or discredit individuals, organizations and governments to further the interests of a foreign state.
- The Canadian Security Intelligence Service (CSIS) continues to observe steady, and in some cases increasing, foreign interference activity by state actors. Foreign interference directed at our democratic institutions and processes can be effective ways for foreign states to achieve their immediate, medium or long-term strategic objectives. These activities can pose serious threats to Canadians both inside and outside Canada, and threaten Canada's prosperity, strategic interests, social fabric, and national security. Given the nature of today's geopolitical environment, these activities will almost certainly intensify.
- While foreign interference activities can target a range of strategically important political, economic, defence, security, foreign policy and community issues, this report will focus specifically on the foreign interference threat to Canada's democratic process. This report also focuses on CSIS's efforts to counter this threat, although other Government of Canada partners are actively involved in this work.
- Although Canada's electoral system is strong, foreign interference can erode trust and threaten the integrity of our democratic institutions, political system, fundamental rights and freedoms, and ultimately, our sovereignty.
- Foreign interference threats affect all levels of government (federal, provincial, municipal) and target all facets of Canadian society, including civil society, communities, media, voters, political parties, candidates, elected officials and their staff, and elections themselves.
- Foreign states and their proxies use a range of common techniques to further their objectives. This includes human intelligence operations, leveraging state-sponsored or community media, sophisticated cyber tools, and social media. While these techniques are varied and can be difficult to detect, there are indicators that can help increase individual awareness of these threats to avoid becoming a target.
- CSIS is mandated to protect Canada and Canadians against foreign interference, among other threats. To respond to this threat, CSIS works in collaboration with other partners, including the Royal Canadian Mounted Police (RCMP). In addition, CSIS is a core member of the Security and Intelligence Threats to Elections (SITE) Task Force, which coordinates efforts to protect federal elections.
- The nature of foreign interference threats, however, means that all Canadians have a role to play in protecting Canada's democracy and national security, both outside of, and during an election. By raising awareness of these issues, CSIS aims to sensitize Canadians to the threat and help build resilience to protect all that we stand for as a democratic and free Canada.



## INTRODUCTION

Canada is an open and free democracy with a reputation of being a friendly and welcoming country. Not everyone, however, shares these values. Some foreign states, or their proxies, use deceptive, clandestine or coercive means to advance their strategic interests at the expense of Canada's. This is foreign interference and it is a threat to Canada's national security.

CSIS continues to observe steady, and in some cases increasing, foreign interference by state actors against Canada. Foreign interference targets all facets of Canadian society. One of the key sectors targeted by this activity is Canada's democratic institutions and processes. The purpose of this report is to sensitize Canadians to the nature of foreign interference in this sector and its impact on our democracy. Although Canada's electoral system is strong, foreign interference is a significant threat to the integrity of our democratic institutions, political system, and fundamental rights and freedoms. For instance, certain foreign states and their proxies may use foreign interference to undermine Canada's electoral process, both outside of, and during an election. Such activities may target the Canadian public, media, voters, political parties, candidates, elected officials and their staff, and elections themselves.

As part of its mandate under the *CSIS Act*, CSIS investigates activities which may, on reasonable grounds, be suspected of posing a threat to the security of Canada. CSIS collects and analyzes information to provide advice to the Government of Canada. It may also take reasonable and proportionate measures to reduce the threats it detects. The threats to national security that CSIS is mandated to investigate include espionage, sabotage, foreign influenced activities, terrorism, and subversion.

Foreign interference activities are persistent, multi-faceted, and target all areas of Canadian society. While CSIS is mandated to investigate this threat, everyone has a role to play in protecting Canada's democracy and national security. Together, we can build resilience to ensure that our communities and institutions are not exploited by foreign state actors, and collectively safeguard our democratic values.





## WHAT IS FOREIGN INTERFERENCE?

“Foreign interference” is a commonly used expression which is also referred to as “foreign influenced activities”. The *CSIS Act* defines foreign influenced activities as “activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person”. Broadly speaking, foreign interference includes attempts to covertly influence, intimidate, manipulate, interfere, corrupt or discredit individuals, organizations and governments to further the interests of a foreign country. These activities, carried out by both state and non-state actors, are directed at Canadian entities both inside and outside of Canada, and directly threaten national security.

Foreign interference involves foreign states, or persons/entities operating on their behalf, attempting to covertly influence decisions, events or outcomes to better suit their strategic interests. In many cases, clandestine influence operations are meant to deceptively influence Government of Canada policies, officials or democratic processes in support of foreign political agendas.

This activity can include cultivating influential people to sway decision-making, spreading disinformation on social media, and seeking to covertly influence the outcome of elections. These threats can target all levels of government (federal, provincial, municipal) across Canada.

Foreign interference differs from normal diplomatic conduct or acceptable foreign-state actor lobbying. For instance, lawful advocacy is a healthy part of diplomatic relations. Clandestine or deceptive interference by a foreign state to advance its interests are not. States cross a line any time they, or their representatives in Canada, go beyond diplomacy to conduct activities that attempt to clandestinely or deceptively manipulate Canada’s open democracy and society, including by threats of any kind.

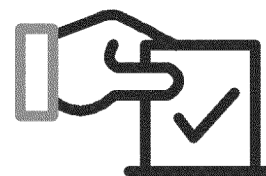
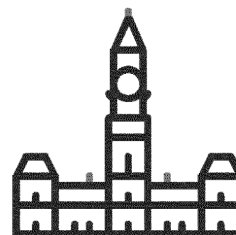
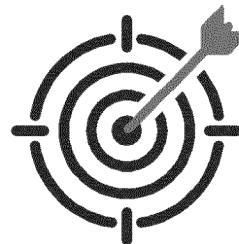
The scale, speed, range, and impact of foreign interference activities in Canada has grown as a result of globalization, technology, and the current geopolitical climate. The changes in how we live our lives in the 21<sup>st</sup> century have provided foreign states with more opportunities to target individuals in Canada through cyber means, including monitoring and harassment.

## WHY IS CANADA A TARGET?

As an open and free democracy with an advanced economy, Canada has long been targeted by foreign states seeking to gain information, covertly influence or leverage individuals and communities to advance their own national interests.

Canada's abundance of natural resources, advanced technology, human talent, and expertise makes it a world leader in many sectors. Canada's close relationship with the United States, its status as a founding member of the North Atlantic Treaty Organization and its participation in a number of multilateral and bilateral defence and trade agreements, as well as the Five Eyes community, has also made it an attractive target for foreign interference. In addition, certain foreign powers are known to leverage Canada's multiculturalism for their own benefit by subjecting Canadian communities to clandestine and deceptive manipulation or threats.

Elections, at any level of government, provide further opportunity for a foreign state to advance its national interests. CSIS has observed persistent and sophisticated state-sponsored threat activity targeting elections for many years now and continues to see a rise in its frequency and sophistication. For instance, CSIS observes social media being leveraged to spread disinformation or run foreign influenced campaigns designed to confuse or divide public opinion, or interfere in healthy public debate.



## WHY DO STATES ENGAGE IN FOREIGN INTERFERENCE TO INFLUENCE THE DEMOCRATIC PROCESSES OF FOREIGN COUNTRIES?

Foreign interference directed at Canada's democratic institutions and processes can be an effective way for a foreign state to achieve its immediate, medium and long-term strategic objectives. The choices that the Government of Canada makes, for example, about military deployments, trade and investment agreements, diplomatic engagements, foreign aid, or immigration policy are of interest to other states. The decisions and policies of provincial and municipal governments are equally important as they determine investments in the economy, infrastructure, resources and the environment, as well as the health and education of citizens and residents. But for some foreign states, the decisions and policy stances of the federal, provincial and municipal governments may negatively affect their core interests. As the world has become ever smaller and more competitive, foreign states seek to leverage all elements of state power to advance their national interests and position themselves in a rapidly evolving geopolitical environment.

### *Immediate Goals*

- Shape narratives around strategic interests (e.g., artificially create perception of support or divisiveness, gain political favour, etc.)
- Covertly influence election outcomes in favour of their preferred candidate or party
- Suppress voter participation
- Reduce public confidence in the outcome of an electoral process

### *Mid-Term Goals*

- Advance strategic priorities that align with their national interests
- Undermine strategic interests of their adversaries
- Discredit democratic institutions
- Erode confidence in democracy

### *Long-Term Goals*

- Achieve economic, intelligence, military, and geopolitical strategic advantage
- Preserve authoritarian regime
- Disrupt the rules-based international order

## WHO ARE THE TARGETS OF FOREIGN INTERFERENCE IN CANADA'S DEMOCRATIC PROCESS?



### *Canadian Public and Voters*

The Canadian public and voters are targeted by foreign interference as they are generally viewed by state actors as vulnerable targets. In particular, elections provide valuable opportunities for state actors to conduct disinformation and interference campaigns; however, such activities are ongoing and are not only observed in the lead-up to, or during, an election.

The targeting and manipulation of diverse Canadian communities are one of the primary means through which states carry out foreign interference activities and undermine Canada's democracy. The impact of this is that communities may fear or resent state-backed or state-linked retribution targeting both individuals in Canada and their loved ones abroad. By exploiting and coercing Canada's communities, foreign states attempt to control messaging that is supportive of Canada's values, policies, or practices; silence dissenting views or opinions of the foreign state or issues that do not support their strategic objectives; and amplify their own favourable messaging. By monitoring and harassing Canada's communities, state actors try to influence public opinion and sow discord. In a democracy where public opinion informs policy development and government decision-making, such influence can alter outcomes and weaken our democratic institutions in the long-term.

State actors may use threats, bribery or blackmail to affect the voting behaviour of individuals inside or outside of communities. Individuals may be threatened or fear reprisal for themselves or their loved ones in Canada or abroad if they fail to comply with publicly supporting a particular candidate or contributing funds to the foreign state's preferred party. While state actors may use coercive techniques to achieve their objectives, they may also use flattery, promise compensation, or appeal to an individual's sense of pride towards another country to elicit the desired behaviour.

Attempts to influence the public are also increasingly observed online, where threat actors have refined their ability to conduct disinformation and foreign interference campaigns. Foreign states attempt to manipulate social media to amplify societal differences, sow discord and undermine confidence in fundamental government institutions or electoral processes. They may use a coordinated approach to amplify a single narrative while also promoting

inflammatory content. Foreign states may also use cyber-enabled tracking or surveillance of dissidents, those who challenge their rhetoric, or do not support their interests in Canada. Such behaviour can lead to threats or blackmail if the individual fails to cooperate.

When communities in Canada are subjected to threats, harassment, intimidation, or other deceptive means by foreign states that are either seeking to gather support or mute criticism of their policies, these activities constitute a threat to the safety of Canadians and to Canada's security. By aggressively conducting such activities, state actors show disregard for Canadian democratic values and open society.



#### *Elected and Public Officials*

Elected and public officials across all levels of government, representing all political parties, are targeted, including: members of Parliament, members of provincial legislatures, municipal officials and representatives of Indigenous governments. Public servants, ministerial and political staff, and others with input into, or influence over, the public policy decision-making process are also targeted by foreign states. State actors may use deceptive means to cultivate a relationship with electoral candidates or their staff in order to covertly obtain information to be used later to their advantage through, for example, threats and blackmail. Alternatively, a state actor may decide to recruit the individual over time in the hopes of greater gains if the individual is elected. After a long period of cultivation there are more opportunities to gain leverage over the official which can be used to pressure the individual into influencing debate and decision-making within government. The individual may also be able to hinder or delay initiatives that are contrary to the foreign state's interest.



#### *Donors, Interest/Lobby Groups and Community Organizations*

State actors may also attempt to covertly mobilize others involved in the democratic process. Donors, interest or lobby groups, or community organizations may be used, wittingly or unwittingly, to carry out interference activities that support a foreign state's preferred candidate, or discredit or attack candidates that threaten their interests. For donors, some may have connections to foreign states or be pressured or coerced into making donations to specific candidates. For the candidate receiving the donations, there may be "strings attached" and an expectation that the candidate will act in the state's best interests.



## *Media*

Foreign states also threaten Canada's democratic process when they attempt to manipulate Canadian media. Both traditional media outlets, such as publications, radio and television programs, and non-traditional media, such as online sources and social media, can be targeted to advance a foreign state's intent. Mainstream news outlets, as well as community sources, may also be targeted by foreign states who attempt to shape public opinion, debate, and covertly influence participation in the democratic process. Considering Canada's rich multicultural makeup, foreign states may try to leverage or coerce individuals within communities to help influence to their benefit what is being reported by Canadian media outlets. These individuals may be knowingly or unknowingly acting on behalf or at the behest of a foreign state.

Another way to influence Canada's media outlets is through funding and advertisements. Foreign states may attempt to invest money, pay for advertisements, or sponsor investigative journalism or interviews that help promote their interests. Such activities could result in content advancing a foreign state's interest being communicated to the Canadian public under the guise of independent media. In addition, foreign states may also acquire media outlets in Canada.

Just as damaging is when foreign states attempt to propagate disinformation, promote divisive and inflammatory content, or discredit credible news sources. These activities undermine legitimate public discourse and erode the public's trust in the media, which is a direct attack on democracy.

## WHAT TECHNIQUES DO FOREIGN STATES USE TO CONDUCT FOREIGN INTERFERENCE?



### *Elicitation*

- Elicitation results when a targeted person is manipulated into sharing valuable information through a casual conversation.
- For example, a threat actor could knowingly seek to provide someone with incorrect information, in the hope that the person will correct them, thereby providing the information the threat actor was actually looking for.
- A threat actor may also share some form of sensitive information with the individual in the hopes that the individual will do the same – a technique referred to as the “give to get” principle.

*How to avoid it: Be discreet, avoid “over-sharing”, and assume public conversations are monitored.*



### *Cultivation*

- Effective threat actors seek to build long-lasting, deep, and even romantic relationships with targeted persons. These relationships enable the manipulation of targets when required, for example, through requests for inappropriate and special “favours”.
- To establish a relationship, the threat actor whose affiliation to a foreign state is not readily known, must first cultivate a target. Cultivation begins with a simple introduction with the end goal of recruitment over time. Shared interests and innocuous social gatherings are often leveraged for cultivation.

*How to avoid it: Be aware and keep track of unnatural social interactions, frequent requests to meet privately, out-of-place introductions or engagements, gifts and offers of all expenses paid travel.*



### *Coercion*

- Blackmail and threats are two of the most aggressive types of recruitment and coercion.
- If a threat actor acquires compromising or otherwise embarrassing details about a target's life, they can seek to blackmail the person.
- Sometimes, blackmail or threats may occur after a long period of cultivation and relationship-building. A threat actor may also attempt to put someone in a compromising situation, just to blackmail the person later.
- Threat actors may also use covert operations, such as intrusions, to steal or copy sensitive information and later use that information to blackmail or threaten the individual.

*How to avoid it: Avoid sharing compromising details or personal information with untrusted individuals, both in-person and online.*



### *Illicit and Corrupt Financing*

- Threat actors can use someone as a proxy to conduct illicit financing activities on their behalf.
- Inducements may occur innocuously via a simple request for a favour. For example, a threat actor may ask a target to "pay someone back" or relay money to a third party on their behalf.
- Political parties and candidates may also receive funds (e.g., donations) seemingly from a Canadian, though this may have originated from a foreign threat actor.

*How to avoid it: Be aware of inappropriate requests which involve money, and question the source of suspicious donations or "gifts".*



### *Cyber Attacks*

- Threat actors can compromise electronic devices through a range of means. Socially-engineered emails (i.e., spear-phishing emails) can trick the recipient into clicking a specific link thereby sharing details about their devices, or can potentially introduce harmful malware into their systems.
- These cyber attacks enable threat actors to collect potentially useful information (e.g., voter data, compromising information about a candidate) that can be used in a foreign influenced operation.

*How to avoid it: Use strong passwords, enable two-factor authentication, and don't click on links or open attachments unless you are certain of who sent them and why.*





### *Disinformation*

- Threat actors can manipulate social media to spread disinformation, amplify a particular message, or provoke users (i.e., “troll” users) when appropriate to serve their interests. A growing number of foreign states have built and deployed programs dedicated to undertaking online influence as part of their daily business. These online influence campaigns attempt to change voter opinions, civil discourse, policymakers’ choices, government relationships, the reputation of politicians and countries, and sow confusion and distrust in Canadian democratic processes and institutions.

*How to avoid it: Be critical of what you are consuming online, careful what you share (or repost from others), and take note of unexpected online interactions.*



### *Espionage*

- While distinct threats, foreign interference and espionage are often used together by foreign actors to further their goals. For instance, information collected or stolen through espionage can be very useful in planning and carrying out a foreign influence or public disinformation campaign.

*How to avoid it: Follow security of information protocols, don’t disclose information to individuals who don’t have a reason to access it, and be discrete about how you handle sensitive information.*

## WHAT ARE THE GOVERNMENT OF CANADA AND CSIS DOING TO PROTECT AGAINST FOREIGN INTERFERENCE?

The Government of Canada has a fundamental responsibility to protect Canada's national security and the security of Canadians. It has measures in place to ensure the integrity of our political system, both during and outside of an election. Canada's electoral process is paper-based and there are procedural mechanisms in place to protect against voter fraud, such as having to prove identity and address prior to voting in a federal election. In addition to these safeguards, Elections Canada has a number of other legal, procedural, and IT measures in place that provide very robust protections for Canadian federal elections. The Communications Security Establishment (CSE) also takes measures to prevent cyber threats. At the provincial and territorial level, the Canadian Centre for Cyber Security (Cyber Centre) also provides advice and guidance to election bodies.

CSIS contributes to a whole-of-government approach to protect Canadians from national security threats, including foreign interference. CSIS has longstanding investigations into specific threat actors who are believed to be targeting Canada and Canadians through clandestine, deceptive or threatening means. CSIS advises the Government of Canada of these threats, and is able to take lawful measures under its threat reduction mandate to mitigate threats to the security of Canada.

Foreign interference can manifest through various means, including cyber means. The increasing interconnectedness of the world presents cyber actors with more opportunities than ever to conduct malicious activity. CSIS actively investigates cyber threats and works in collaboration with key partners. While CSIS, CSE, the Cyber Center, the RCMP and other key government partners have distinct and

separate mandates, they share a common goal of keeping Canada, Canadians, and Canadian interests safe and secure online.

In the lead up to the 2019 Federal Election, the SITE Task Force was created to protect Canada's federal election. As an active partner in SITE, CSIS works closely with CSE, the RCMP and Global Affairs Canada to share information on election security and inform decision-making when there are incidents of foreign interference in elections. Now seen as a model for our allies on how different departments can work together to ensure free and fair elections, SITE's efforts continue today.

Canada's democratic institutions and processes are strong and the Government of Canada actively works to ensure their continued protection. However, keeping Canada's democratic institutions, political system, and democracy safe requires a national security-aware population. This means that all citizens need to know about the threats to Canada's democracy and be equipped to protect themselves from foreign interference. We all have a role to play in protecting Canada's democracy.



## HOW TO REPORT FOREIGN INTERFERENCE

The Government of Canada has mechanisms in place to report foreign interference.

Information related to espionage or foreign interference may be reported to CSIS by contacting 613-993-9620 or 1-800-267-7685, or by completing the web form at [www.canada.ca/en/security-intelligence-service/corporate/reporting-national-security-information.html](http://www.canada.ca/en/security-intelligence-service/corporate/reporting-national-security-information.html).

In addition to their local police, any individual in Canada who is concerned that they are being targeted by state or non-state actors for the purposes of foreign interference should contact the RCMP's National Security Information Network at 1-800-420-5805, or by email at [RCMP.NSIN-RISN.GRC@rcmp-qrc.gc.ca](mailto:RCMP.NSIN-RISN.GRC@rcmp-qrc.gc.ca).



## ANNEX: KEY TERMS AND DEFINITIONS

**Clandestine or Covert:** Activities that are conducted in secret or not out in the open.

**Censorship:** The suppression of speech, public communication, or information. This may be done on the basis that the information is harmful, obscene, or politically inconvenient depending on perspective.

**Coercion:** The use of threats, force, or manipulation to compel individuals to act in ways that further their objectives.

**Covert Influence:** Foreign states who use deception or power to secretly affect, control or manipulate their adversaries to further their own state's objectives.

**Cultivation:** As part of a long-term recruitment plan, individuals who are in a position of influence, or have knowledge or access to information, are actively sought after. In a process known as cultivation, the individual is groomed for an eventual request or "favour".

**Deception:** When threat actors cause an individual to believe something that is not true in order to further their objectives.

**Discredit:** Threat actors may cause others to question or refuse to believe in an individual or something that the individual said or did in order to further their objectives.

**Disinformation:** The deliberate spread of false or manipulated information with the intent to mislead others.

**Interference:** Foreign states who use deception or power to secretly hinder or impede their adversaries to further their own state's objectives.

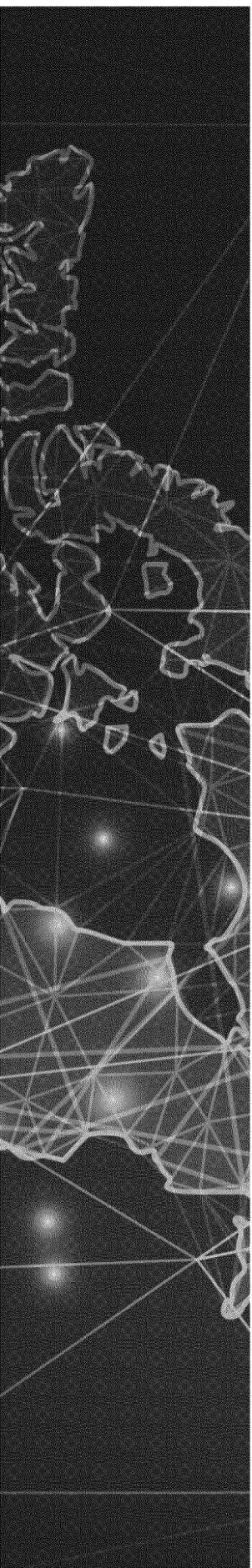
**Manipulation:** A form of coercion where individuals or information are controlled to shape behaviour, outcomes or decision-making processes.

**Misinformation:** The spread of false information without the intent to deceive or mislead. This is communication between people that contains incorrect facts.

**Propaganda:** An organized program of publicity using selective information to propagate a doctrine of belief, often in a misleading or dishonest way.

**Proxy:** An individual or entity that is not directly linked to a foreign state, but acts on its behalf.

UNCLASSIFIED



**Recruitment:** Typically after a process of successful cultivation, individuals will be asked to complete a “favour” for a threat actor. Some individuals may be compensated with money, assets, or career progression for assisting the threat actor, while others may not be aware that they have been recruited.

**Subversion:** Activities that attempt to undermine, overthrow, or destroy the power and authority of an established system or institution.

**Threats:** A form of coercion where threat actors express their intention to damage an individual’s reputation or property, or inflict injury upon an individual, or their loved ones, if they fail to act in ways that further their objectives.

UNCLASSIFIED



Canadian Security Intelligence Service  
Service canadien du renseignement de sécurité



# FOREIGN INTERFERENCE AND YOU

A SAFE, SECURE AND PROSPEROUS CANADA THROUGH TRUSTED INTELLIGENCE AND ADVICE.  
DES RENSEIGNEMENTS ET DES CONSEILS FIABLES POUR UN CANADA SÛR ET PROSPÈRE.

UNCLASSIFIED

FOREIGN INTERFERENCE AND YOU

## /// WHAT IS FOREIGN INTERFERENCE?

Foreign interference is deliberate and covert activity undertaken by a foreign state to advance its interests, often to the detriment of Canada's. The CSIS Act describes Foreign-Influenced Activities, which is another term for Foreign Interference, as "activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person".

Foreign interference is distinct from normal diplomatic conduct or acceptable foreign state lobbying; it is purposely covert, malign, and deceptive. States cross a line anytime they go beyond diplomacy to conduct activities that attempt to threaten our citizens, residents and institutions, or to compromise our way of life, undermine our democratic processes, or damage our economic prosperity.

## /// FOREIGN INTERFERENCE AIMS

Foreign governments engage in foreign interference activities in Canada and target Canadians to advance their interests, sometimes at our expense, in an effort to achieve geopolitical, economic, military and strategic advantage. They seek to sow discord, disrupt our economy, bias policy development and decision-making, and to influence public opinion. In many cases, clandestine influence operations are meant to support foreign political agendas or to deceptively influence the targeted country's policies, officials, research institutions or democratic processes.

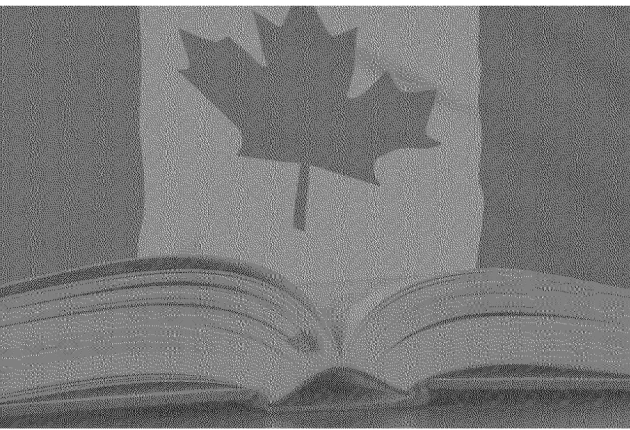
## /// THE NATIONAL SECURITY THREAT

Foreign interference is a complex national security threat. It poses a significant threat to the integrity of our political systems, democratic processes, social cohesion, academic freedom, economic prosperity and challenges Canadians' rights and freedoms. In short, and as described by the National Security and Intelligence Committee of Parliamentarians, foreign interference threatens the fundamental values of our country and our national security.

CSIS has observed and investigated multiple instances of foreign states targeting Canada and Canadian interests through the use of human intelligence operations, state-sponsored or foreign influenced media, and sophisticated cyber techniques. Traditional interference through human intelligence operations remains the greatest danger, but interference through hostile cyber activity is a growing concern.

## /// CANADA AS PERMISSIVE TARGET

As an advanced economy and an open and free democracy, Canada has long been targeted by hostile states seeking to acquire information, intelligence and influence to advance their own interests. These activities pose strategic, long-term threats to Canada's interests, jeopardize our future prosperity, and have a corrosive effect on our democratic processes and institutions.



The Committee believes that these states target Canada for a variety of reasons, but all seek to exploit the openness of our society and penetrate our fundamental institutions to meet their objectives. They target ethnocultural communities, seek to corrupt the political process, manipulate the media, and attempt to curate debate on postsecondary campuses. Each of these activities poses a significant risk to the rights and freedoms of Canadians and to the country's sovereignty: they are a clear threat to the security of Canada. [Source: [Annual Report 2019](#), National Security and Intelligence Committee of Parliamentarians, p. 77.]

## /// WHO AND WHAT IS TARGETED?

Canada's fundamental institutions (e.g. academia, free press, democratic institutions), governance processes, and diverse Canadian communities are all active targets of foreign interference activities.

On university campuses, foreign states may seek to exert undue influence, covertly and through proxies, by harassing dissidents and suppressing academic freedoms and free speech that are not aligned with their political interests. Similarly, these actors may attempt to influence public opinion and debate in Canada through interference in our press or online media.

Elected and public officials across all levels of government, representing all political parties, are targeted: Members of Parliament, members of provincial legislatures, municipal officials and representatives of Indigenous governments. Public servants, Ministerial and political staff, and others with input into or influence over the public policy decision-making process are also attractive targets.

Hostile foreign actors also target the fabric of Canada's multicultural society, seeking to influence Canadian communities, including through threats, manipulation and coercion. Some of these communities are vulnerable targets of foreign interference from states seeking to exploit them in various ways to advance the foreign state's interests, sometimes to the detriment of Canadian values and freedoms.



UNCLASSIFIED

FOREIGN INTERFERENCE AND YOU

## FOREIGN INTERFERENCE IN ACADEMIA AND RESEARCH

Foreign actors may seek to interfere in academia through a range of actions, such as:

- covertly influencing research agendas or peer review processes
- exerting economic pressure to achieve desired outcomes
- introducing or obscuring conflicts of interest or military ties
- recruiting researchers and staff for interference activities or talent programs, and
- direct foreign investment or other legal funding arrangements where the objectives of the investment or details about the funding are deliberately obscured or misrepresented.

In trying to influence public debate at academic institutions, foreign states may sponsor specific events to shape discussion rather than engage in free debate and dialogue. They may also directly or indirectly attempt to disrupt public events or other on-campus activities they perceive as challenging their political positions and spread disinformation, undermining confidence in academic discourse and expertise.

## COMMON TECHNIQUES

- Foreign interference techniques or activities can include (but are not limited to): elicitation, cultivation, coercion, illicit financing, cyber attacks, intimidation and disinformation.
- Elicitation results when a targeted person is manipulated into sharing valuable information through a casual conversation.
- Cultivation is a technique of building long-lasting relationships with targeted persons to enable manipulation and facilitate threat activities.
- Blackmail and threats are two of the most aggressive types of recruitment and coercion. Intimidation is also commonly used to silence dissent, including on university campuses, and to instill fear and compliance among various Canadian communities.
- Threat actors can use individuals as a proxy to conduct illicit financing activities or to make a donation to a political party or candidate.
- Cyber attacks such as spear-phishing can be used to introduce malware into your system as a means of collecting information to support foreign interference activities.
- Disinformation can be used by foreign actors to influence public opinions, perceptions, decisions and behaviours. A growing number of states have built and deployed programs dedicated to undertaking online influence as part of their daily business. Adversaries use online influence campaigns to attempt to change civil discourse, policymakers' choices, government relationships, and the reputation of politicians and countries both nationally and globally.

## ONLINE INFLUENCE



A growing number of states have built and deployed programs dedicated to undertaking online influence as part of their daily business. Adversaries use online influence campaigns to attempt to change civil discourse, policymakers' choices, government relationships, and the reputation of politicians and countries both nationally and globally. They try to delegitimize the concept of democracy and other values such as human rights and liberty, which may run contrary to their own ideological views. They also try to exacerbate existing friction in democratic societies around various divisive social, political, and economic issues. While online foreign influence activities tend to increase around elections, these ongoing campaigns have broadened in scope since 2018, expanding to react and adapt to current events, shifting their content strategies around trending news stories and popular political issues [Source: 2020 National Cyber Threat Assessment, Canadian Centre for Cyber Security].

## /// WHAT CAN YOU DO?

### **Individuals:**

- Be aware of the threat; increasing our collective resilience against foreign interference is a shared responsibility.
- Do your due diligence before sharing information or entering into arrangements, know your partners and assess the risks of any partnership in advance.
- Be cyber safe.
- Remember to always verify the credibility of your information sources to ensure that you are receiving accurate information.
- Report suspicious activities and any incidents of intimidation, harassment, coercion, or threats to CSIS or to your local law enforcement authorities.

### **Organizations:**

- Don't be a permissive target for foreign interference. Protect yourself, your organization, your reputation and your work by being aware of the threat and doing your due diligence.
- Develop policies, procedures and processes for dealing with instances of foreign interference. Make these public to ensure that potential threat actors are aware that you will not tolerate foreign interference activities.
- Provide awareness materials or training on associated policies and procedures to all employees.
- Inform any prospective partners, employees, and investors of your position and policies.
- Protect your reputation by publicly affirming your values and ethics and describing measures and policies that you are taking to advance and protect them.





## CONTACT US

CSIS takes all allegations of foreign interference seriously. These activities constitute a threat to our national security and sovereignty, and the safety of Canadians. If you have been targeted or have concerns or other information to report, please contact CSIS by telephone (1-800-267-7685) or through our website. Canada.ca <https://www.canada.ca/en/security-intelligence-service/corporate/contact-us.html>

ISBN: 978-0-660-39473-2  
Catalogue number: PS74-16/2021E-PDF  
Aussi disponible en français et autres langues.  
Also available in French and other languages.

# Remarks by Director David Vigneault to the Centre for International Governance Innovation

---

From: Canadian Security Intelligence Service

## Speech

**Ottawa - February 9, 2021** - Good afternoon everyone. It's a pleasure to be here with you today. I recognize the challenges of organizing events like this in our new normal and would like to express my sincere gratitude to the Centre for International Governance Innovation for doing so. It's a bit unusual for me today as the tables have turned. You can see me and I cannot see you. Usually, I'm the one on the outside looking in.

I have often commented on the need for a sophisticated dialogue on national security issues - one framed in a Canadian context. These issues are far too important to be left to the agencies alone and that is precisely why we need you to be involved. We need to engage with each other more, break down traditional siloes, and integrate our thinking. I am pleased to see that CIGI has recently launched a research project that will serve to begin addressing this gap in a meaningful way.

There is a lot of uncertainty in our world today, much has changed at such a rapid pace. Undoubtedly, this will continue into the foreseeable future.

The COVID-19 pandemic has had a profound impact on every aspect of our lives. Despite this stress, CSIS remained vigilant of national security threats, both old and new, and carried out its mission to protect Canadians. As all of us adjusted to the new environment, so

did threat actors. CSIS pivoted in part by stepping out of the shadows to shine a brighter light on threats to Canada's national security.

The fluid and rapidly evolving environment created by COVID-19 has created a situation ripe for exploitation by threat actors seeking to cause harm or advance their own interests. With many Canadians working from home, threat actors are presented with even more opportunities to conduct malicious online activities.

For instance, we've seen the continued use of online platforms by violent extremists to recruit others and to spread their hateful messaging, anti-authority narratives and conspiracy theories about the pandemic to rationalize and justify violence. We are also seeing an increase in the exploitation of cyber tools to steal sensitive information, conduct ransomware attacks and cause disruption. In addition, we remain aware of the efforts of state adversaries to spread disinformation about pandemic responses in an attempt to discredit government efforts and diminish confidence in vaccine rollout efforts.

With the world becoming ever smaller and more competitive, states are naturally seeking every advantage to position themselves as leaders in the 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. While not new, this has accelerated during the global pandemic and will continue to do so as we attempt to emerge from an event that has shattered national economies.

From a national security perspective, the threat from hostile activity by state actors in all its forms represents a significant danger to Canada's prosperity and sovereignty.

For instance, espionage can have a profound impact on the security of our research and development, and ultimately, the success of our companies. By subverting our ability to innovate and commercialize research, espionage results in lost jobs and diminished economic growth.

Foreign interference, on the other hand seeks to undermine our institutions, threatens our democratic system and our citizens. Above

all, this activity erodes our sovereignty and undercuts our societal norms.

Together, this one – two punch contributes to a complex environment full of other threats.

With that in mind, I would like to turn to providing you with an update about the threats we are currently facing.

Violent extremism continues to represent a deeply concerning threat to public safety, and a significant area of focus for CSIS.

The threat landscape surrounding religiously, politically, or ideologically motivated violent extremism continues to evolve and has increased in complexity. Threat actors who commit violent acts are more often no longer influenced by a singular and definable belief system, but a range of very personal and diverse grievances and narratives.

Today, threat actors leverage a range of readily available communication tools and platforms that enable them to communicate securely with one another. They use these tools to spread and amplify extremist messaging, recruit others, and finance and plan activities all without getting off their living room couch.

For example, we've seen Canadians move from supporting Daesh to violent misogyny within a short period of time.

CSIS is seeing a rise in the threat from ideologically motivated violent extremism or IMVE. Indeed, since 2014, Canadians motivated in whole or in part, by their extreme views in this sphere have killed 21 and wounded 40 on Canadian soil. In 2019, two IMVE groups were added to Canada's list of terrorist entities for the first time, with another four being added just last week.

This issue is broad and complex. It represents a societal problem that will require a holistic approach involving all elements of civil society to address it. As with religiously motivated violent extremism, CSIS plays a key role, alongside intelligence and law enforcement partners, in that broader government response.



While violent extremism remains an ongoing threat to our safety and a significant preoccupation for CSIS, the greatest strategic threat to Canada's national security comes from hostile activities by foreign states. While we focus on protecting our citizens, we bear witness to hostile states leveraging all elements of their state apparatus to advance their national interests at Canada's expense.

Historically, spies were focused on obtaining Canadian political, military and diplomatic secrets. While these secrets are still attractive, today our adversaries are more focused on intellectual property and advanced research held on computer systems in small start-ups, corporate boardrooms, or university labs across the country.

State cyber actors will continue to target sensitive and proprietary data that resides on these networks – some of which remain relatively open and accessible. They will continue to deploy tradecraft that is highly-creative and deceptive to gain access to data that holds strategic and tactical value.

These actors are able to leverage emerging technologies such as bulk data collection or AI-powered analytics to their advantage. With full integration, they pull from common data pools to identify threats and vulnerabilities. Without strong defences to protect our citizen's data, it is easily accessed and can be used to drive the further development of AI capabilities.

For instance, in 2020, global news sources revealed that Zhenhua Data Technology which primarily serves China's military and intelligence services had been gathering sensitive data on 2.4 million individuals for several years. Approximately 20% of this data was not publically available and likely accessed via cyber-espionage.

Canadian companies, in almost all sectors of our economy, have been targeted. They have been compromised and have suffered losses from human and cyber enabled threats. CSIS has observed persistent and sophisticated state-sponsored threat activity for many years now and we continue to see a rise in the frequency and sophistication of this threat activity. CSIS actively investigates this daily, from coast to coast to coast and abroad.

In particular, I would cite Canada's biopharma and health sector; artificial intelligence; quantum computing; ocean technology; and aerospace sectors as facing particularly severe threat activity.

Emerging technologies in these sectors are also among the most vulnerable to state-sponsored espionage given that they are largely developed within academia and small start-ups. They're attractive targets because they may have less security awareness or protections in place. They are also more likely to pursue financial and collaboration opportunities, which can, and sadly are, exploited by other countries.

Our investigations reveal that this threat has unfortunately caused significant harm to Canadian companies. Collectively, it jeopardizes Canada's knowledge-based economy. When our most innovative technology and know-how is lost, it is our country's future that is being stolen.

Our adversaries do not play by globally-accepted rules.

Some countries do not reciprocate Canada's openness and support for a level playing field and others are aggressively advancing their own economic, intelligence and military state interests, at our expense. This is no longer traditional private commerce.

This is state capitalism and it creates a skewed playing field in which our private sector is always at a disadvantage.

Employees, former employees, students, professors, contractors, business associates, or any individual with inside knowledge of – or access to – an organization's systems can be targeted by hostile intelligence services to wittingly or unwittingly steal sensitive information.

An insider acting at the behest of a threat actor can compromise a system and cause damage, or open a backdoor to allow access from across the street or across the ocean. They can steal information outright, and walk it out the door on a flash drive.

It is no secret that we are most concerned about the actions by the governments of countries like Russia and China. But we should also

not discount that threat activity evolves and can originate from anywhere in the world.

China is an important actor on the world stage and a partner for Canada on some important fronts. Canada and Canadians have benefited for decades from relationships with Chinese researchers, scholars, artists, business people, and others; and our cultural mosaic is all the richer because of the presence of Chinese-Canadians across Canada, in large cities and in small towns dotting every corner of this country.

To be clear, the threat does not come from the Chinese people, but rather the Government of China that is pursuing a strategy for geopolitical advantage on all fronts – economic, technological, political, and military – and using all elements of state power to carry out activities that are a direct threat to our national security and sovereignty. We all must strengthen our defences.

I will now focus on the threat of foreign interference.

Foreign interference has always been present in Canada, but its scale, speed, range, and impact have grown as a result of globalization and technology. We are increasingly seeing social media being leveraged to spread disinformation or run influence campaigns designed to confuse or divide public opinion, interfere in healthy public debate and political discourse, and ultimately create social tensions.

Efforts by foreign states to target politicians, political parties, and electoral processes in order to covertly influence Canadian public policy, public opinion and ultimately undermine our democracy and democratic processes represent some of the most paramount concerns. Our electoral system has been shown to be resilient, but we must also work hard to keep it that way. Vigilance is the best defence.

A number of foreign states engage in hostile actions that routinely threaten and intimidate individuals in Canada to instill fear, silence dissent, and pressure political opponents. One notable example of this is the Government of China's covert global operation, known as Operation Fox Hunt which claims to target corruption but is also

believed to have been used to target and quiet dissidents to the regime.

Those threatened often lack the resources to defend themselves or are unaware that they can report these activities to Canadian authorities, including us. Moreover, these activities are different from the norms of diplomatic activity because they cross the line by attempting to undermine our democratic processes or threaten our citizens in a covert and clandestine manner.

Today, I felt it was important to provide you with this update on the threat environment, given the significance of the changes. The world has changed significantly and so have the threats, in short order.

What has not changed, and must not, is how innovative and dedicated CSIS employees are. The high quality of our investigations, our analysis, the advice we provide and our decisiveness around taking action to address the threats has not changed.

However, we need to ensure that CSIS authorities continue to evolve so that they are able to address the challenges of the significantly more complex environment around us. Today's threats manifest themselves in vastly different ways than they did in 1984, when the CSIS Act was enacted.

An Act better suited for the threats of the Cold War era greatly impedes our ability to use modern tools, and assess data and information. We need laws that enable these types of data driven investigations, carefully constructed to reflect the values we share in our democracy, including assurances of robust privacy protections.

Our Act enables advice to government but limits our ability to provide relevant advice to key partners, including many of you listening today. Our Act sets technological limitations on intelligence collection that were not foreseen by the drafters of the legislation in 1984 and unduly limit our investigations in a modern era.

These are simply a few examples of the challenges of our authorities. At CSIS, we take our social license with Canadians very seriously.

Contrary to many of our adversaries, CSIS operates in a democracy governed by the rule of law, not by the law of the rulers. We strive for the best in accountability and see a healthy discussion on the expectations that Canadians have of their national security agencies, and whether the laws have kept pace, as a meaningful contribution to that accountability. We need your help as advocates and partners in this effort.

I would like to take this opportunity to elaborate further on that need for strong partnerships.

Whether we're talking violent extremism, espionage, or foreign interference, no single government department or agency can deal with these threats alone. If we want to be effective in countering modern threats, we must build strategic partnerships – within and outside government. Partnerships facilitate information sharing, consultation, the pooling of resources or expertise, and joint actions.

I'm seeing this happen in real-time with the pandemic. By sharing what we know about a number of related issues, CSIS has increased and deepened its cooperation with partners like the Public Health Agency of Canada. We're also working closely with partners like Innovation, Science and Economic Development Canada to raise awareness of foreign investments that could impact our national security. We are doing as much as we can to harden the target.

I talked about how we stepped out of the shadows during the pandemic. Immediately, we saw that Canadian universities, medical research institutes, pharmaceutical companies, and others involved in the national response to the pandemic were facing an elevated level of risk to their cyber security. CSIS worked closely with its partners in universities, alongside the Canadian Centre for Cyber Security, to respond accordingly.

The need for partnerships also extends outside our borders, especially among the Five Eyes, the G-7 and other like-minded liberal democracies. It's only through the mobilization of like-minded partners that we can raise the cost to hostile states.

Keeping Canada safe requires a national security-literate population. By this I mean a citizenry that understands the key dilemmas Canada faces, and recognizes the need to adapt and respond in a thoughtful, meaningful, and timely way.

I encourage you to consider CSIS a partner and to contact us for information, advice, or support as your companies, universities, and associations navigate increasingly complex geopolitical waters.

You may think to yourself: “I’m not a national security person. I’m a scientist, a business person, an academic and so on. I’m not interested in geopolitics.”

Well, I can say with some confidence that geopolitics is interested in you.

And it’s important that you know how you can be at risk and how you can protect your interests.

When you reach out to us, you’ll appreciate the expertise and dedication of CSIS employees. As Director of the Service, I take the greatest pride in the quality of our workforce. People truly are CSIS’s most valuable resource.

As Canada’s security and intelligence service, CSIS must reflect the society it protects. Just like the people of Canada, we’re a diverse and inclusive workforce. Our diversity allows us to better understand communities and helps us maintain the bond of confidence and trust that needs to exist between civil society and intelligence agencies. In exchange for the trust that Canadians place in us, we commit to high standards of accountability.

My remarks today have painted a picture of the key threats we all need to be aware of and have a role in countering.

I can assure you that CSIS, along with Government of Canada and international partners, are actively investigating, monitoring and, disrupting harmful threat actors when our lawful mandates allow.

This builds on active efforts undertaken by the Government of Canada to protect Canadians and their interests; for example, we have increased scrutiny of all foreign direct investments under the national

security provision of the *Investment Canada Act* and there is ongoing work of the Security and Intelligence Threats to Elections Task Force to counter foreign interference against threats to elections. Moreover, we have sought to identify new sectors for focused outreach to private companies, associations and academics to help them understand how to protect their intellectual property.

I would like to conclude today, by asking some questions that I would like all of you to consider.

For instance, what are the national security implications of Canada's economic recovery post-pandemic?

What expectations do citizens have regarding how Canadian authorities should use powerful data driven technologies for the public good?

How do we prevent our data and research from inadvertently advancing hostile foreign military, intelligence and commercial interests?

These are just a few questions that we're slowly coming to ask of ourselves and of Canadians.

There is no greater responsibility for a government than the protection of its citizens. In today's dynamic threat environment, government, civil society and the private sector must work together to harden the targets and protect our national interests. I ask all of you to work with CSIS in advancing this call to action to protect the security of Canadians and the health of our economy for our future and that of our children. I'm an optimist. I know we can do it. We must!

Thank you Aaron, and everybody online for listening. I'll stop here, and I'll be pleased to take questions.