



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

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


| | |
|--|-----------|
| Message from the Director | 6 |
| CSIS 101 | 11 |
| Mandate | 12 |
| Accountability | 12 |
| Partnerships | 13 |
| Duties and Functions | 13 |
| Financial Reporting | 14 |
| The Pandemic | 17 |
| COVID-19 Outreach Initiative | 18 |
| The Four Gates of Economic Security | 19 |
| CSIS Support to the Government of Canada's Pandemic Response | 20 |
| The Threat Environment | 21 |
| 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 |

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



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.

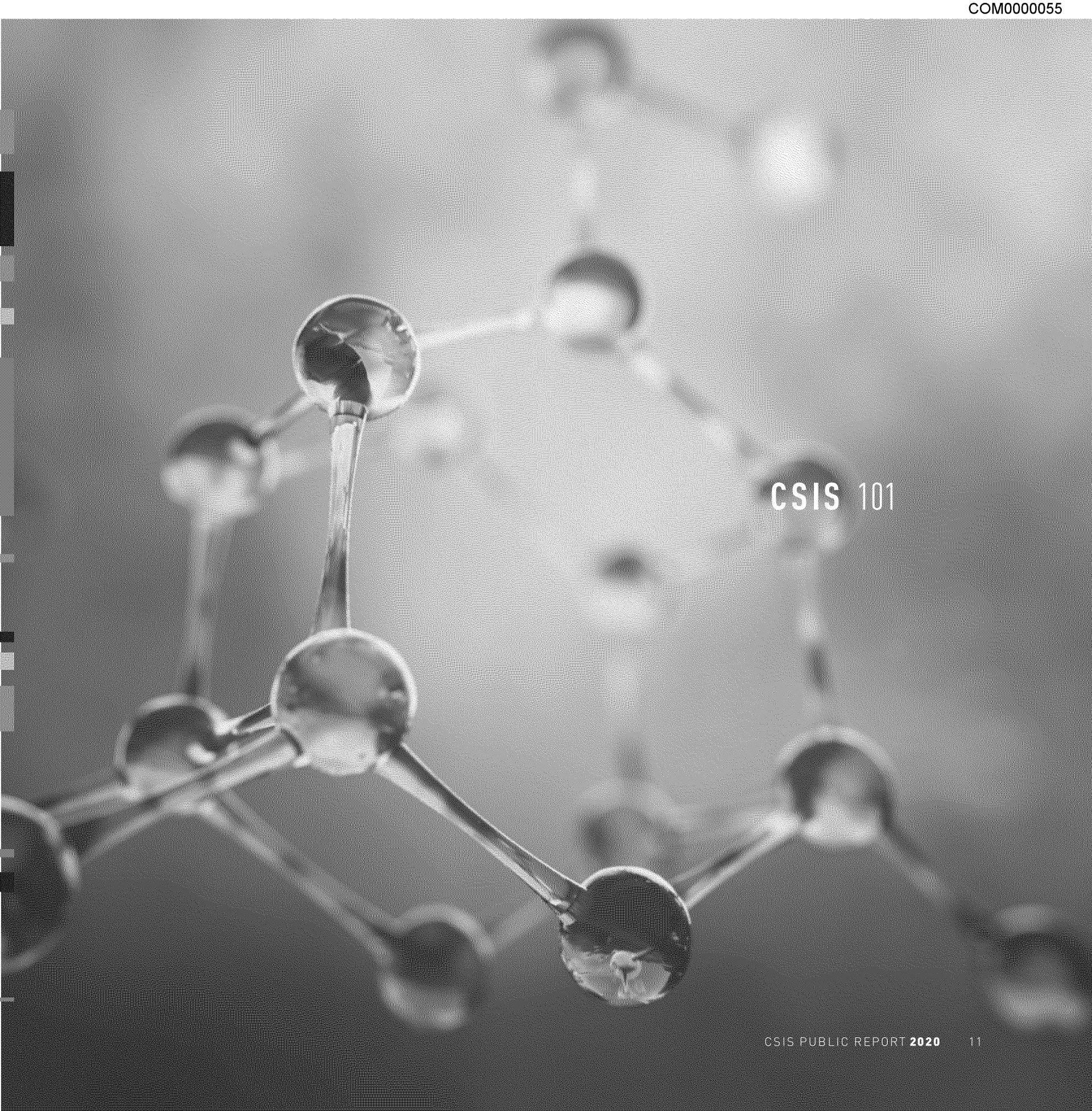
My focus as Director, especially during this pandemic, has been to ensure that all of our employees work in a healthy, safe, and respectful environment. Given our unique mandate, this meant that when much of the world moved to working from home, CSIS employees continued their critical mission in a way 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.



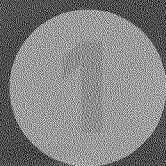
DAVID VIGNEAULT

DIRECTOR, CANADIAN SECURITY INTELLIGENCE SERVICE

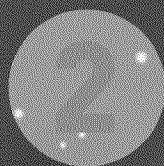


CSIS 101

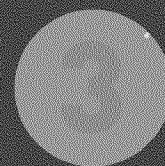
CORE MANDATE



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

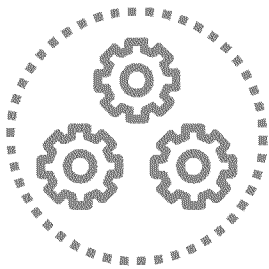
PARTNERSHIPS

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

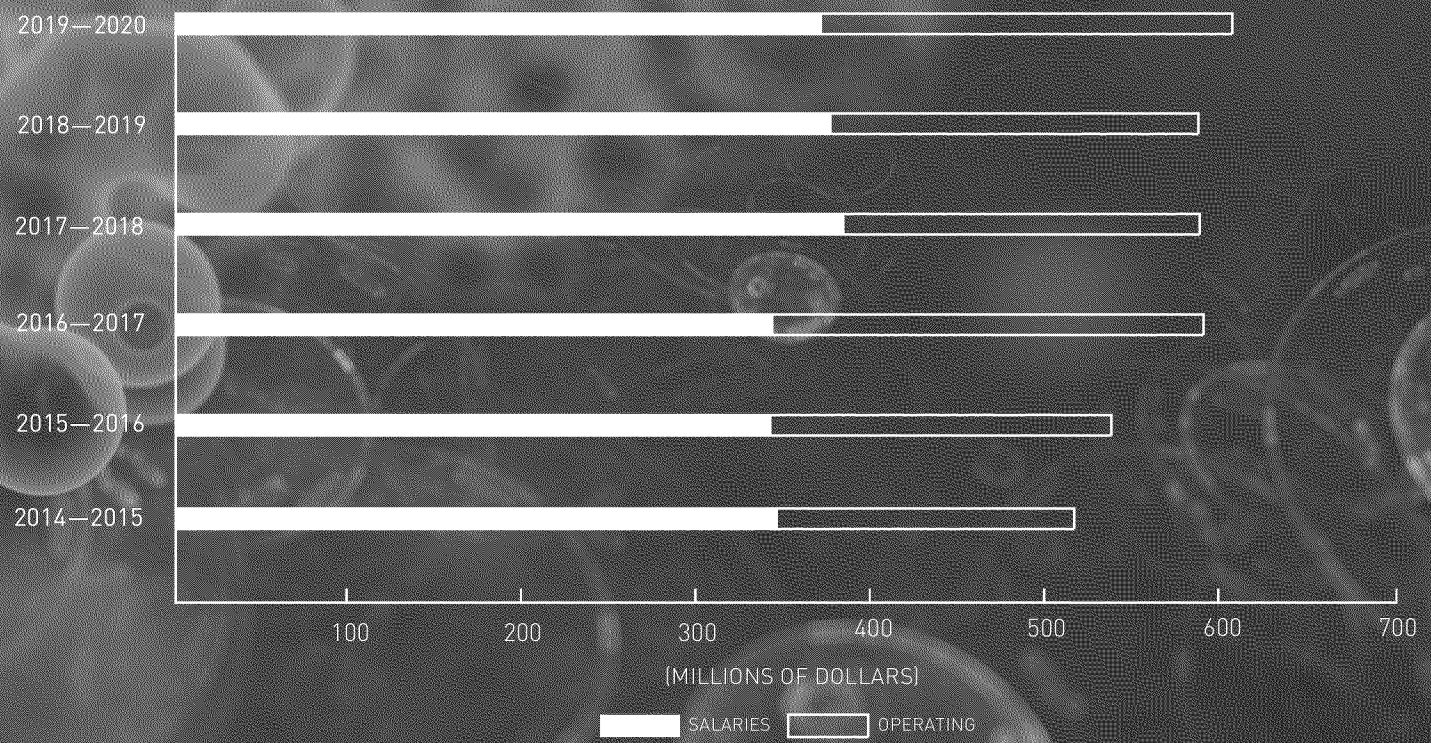
Intelligence
Assessment and
Dissemination

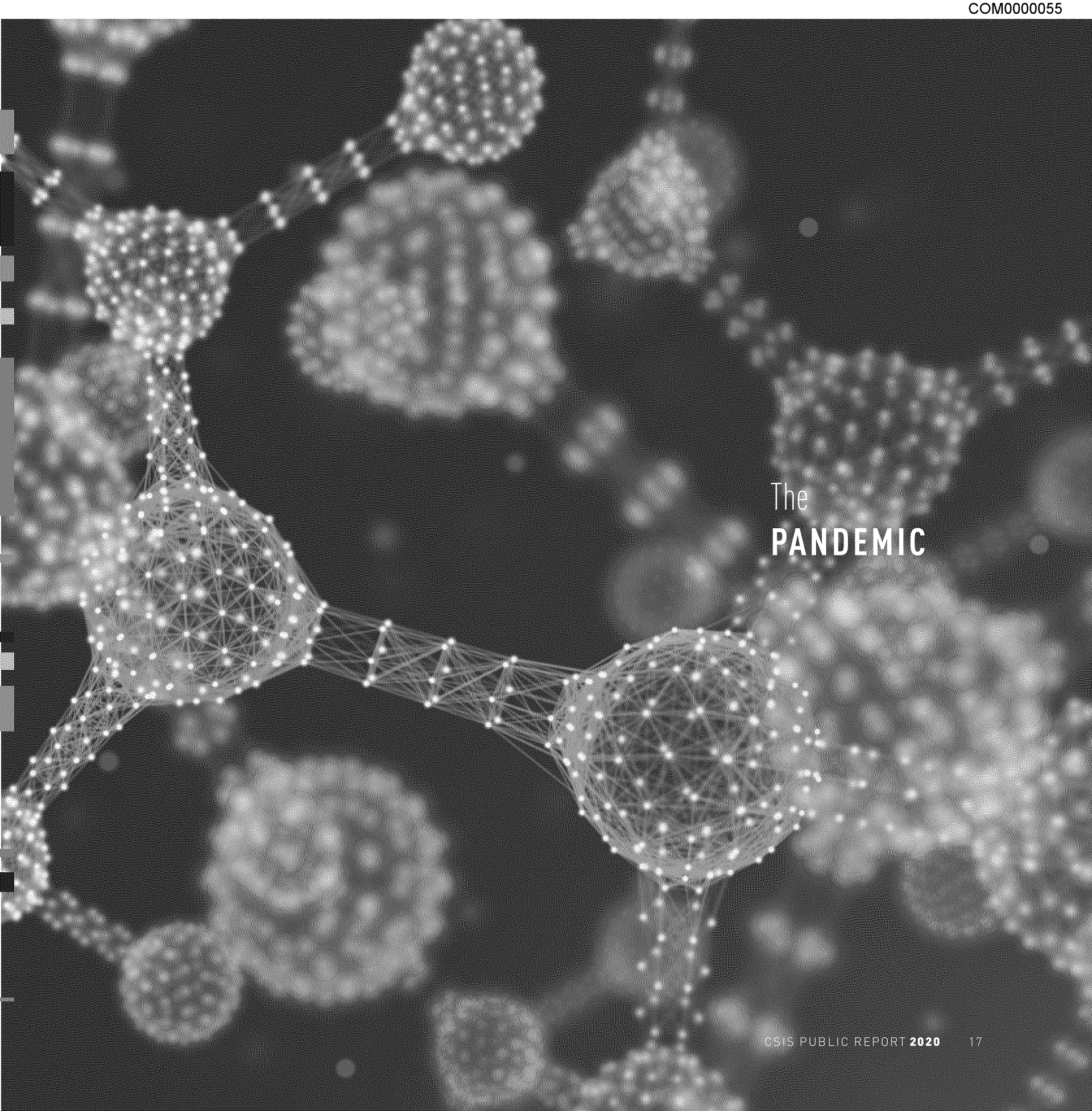
Security
Screening

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.

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.

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).

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.

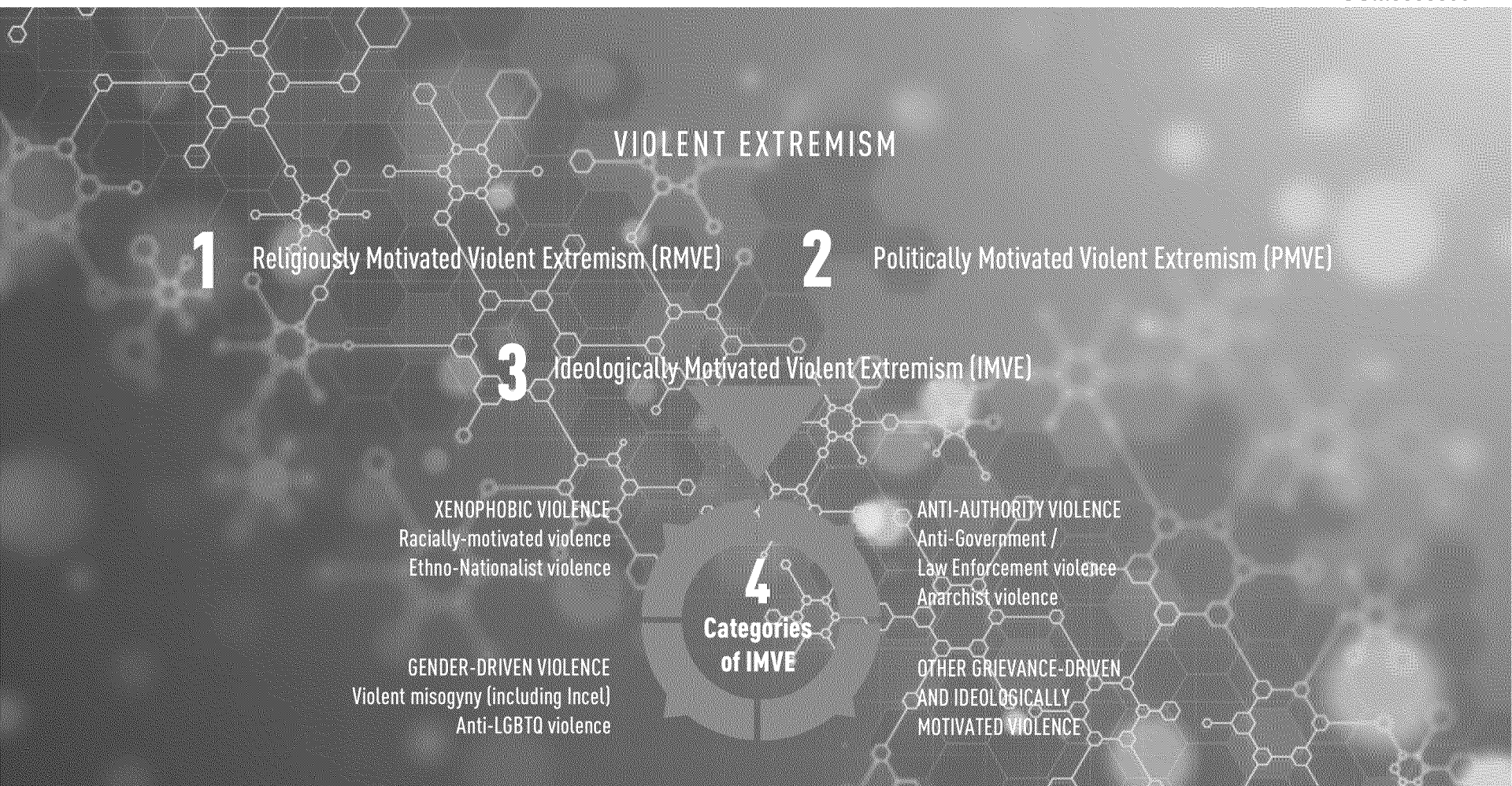
Threat actors have also compromised third-party vendor software or equipment in order to conduct cyber-operations against that vendor's clients. In 2020, a state-sponsored cyber threat actor modified an update mechanism for a popular brand of network management software which allowed the actor to gain 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

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

GOVERNMENT SCREENING PROGRAMS

| REQUESTS RECEIVED* | 2019–2020 |
|---------------------------------------|------------------|
| 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 |
| TOTAL: | 167,210 |

*Figures have been rounded

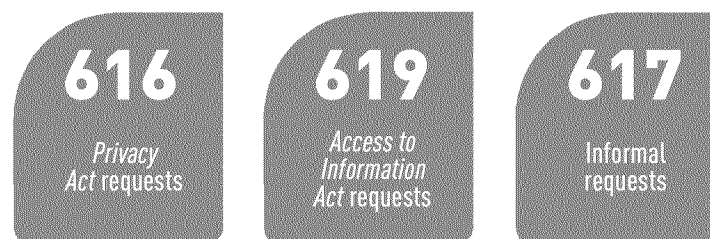
**Individuals claiming refugee status in Canada or at ports of entry

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

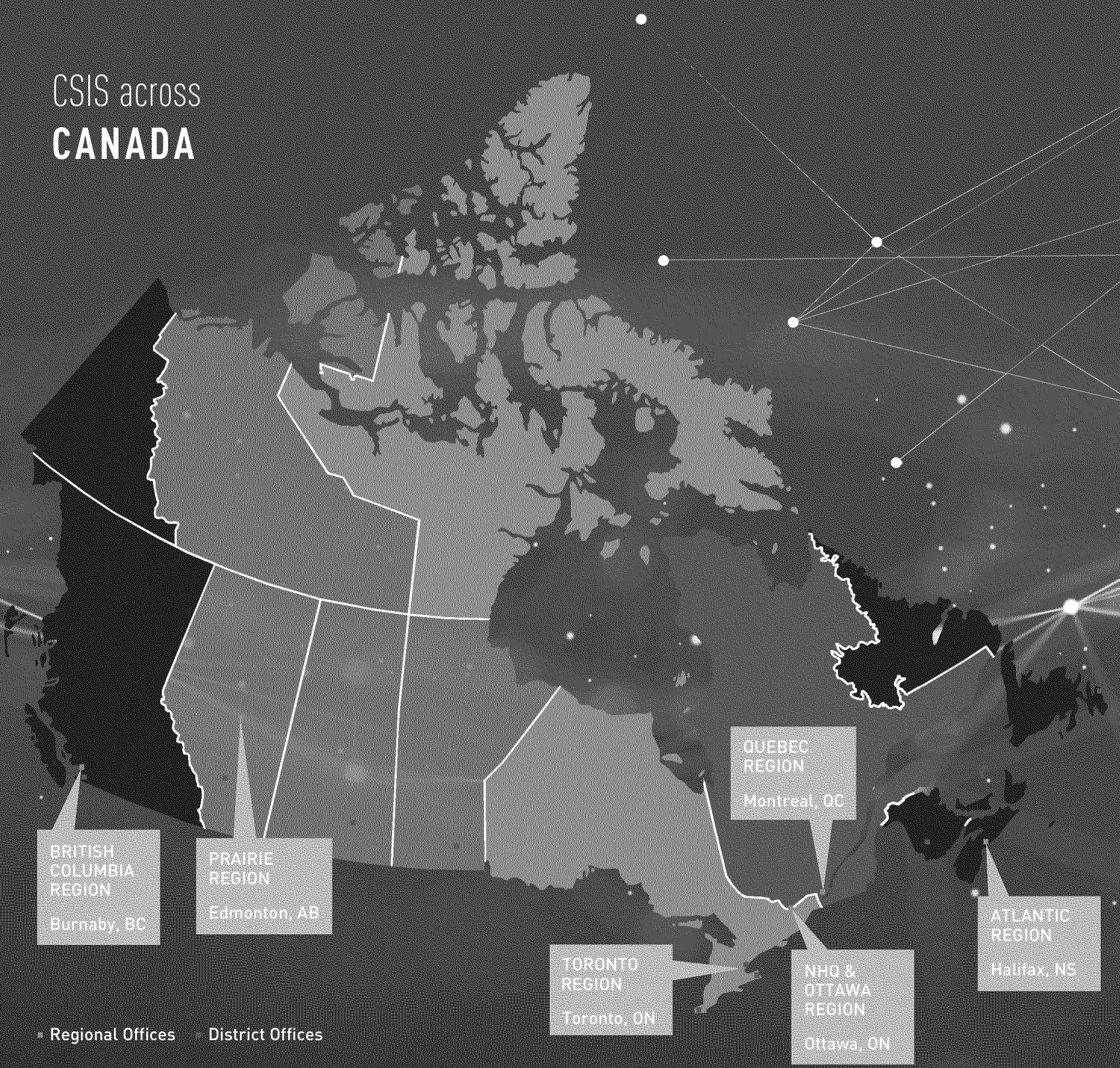
Protecting Canada's national security and that of its citizens is a critical job — and how CSIS employees conduct themselves and interact in the workplace is just as important. 2020 marked an important step in the organization's commitment to providing a healthy and respectful workplace for all of our 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



■ Regional Offices ● District Offices

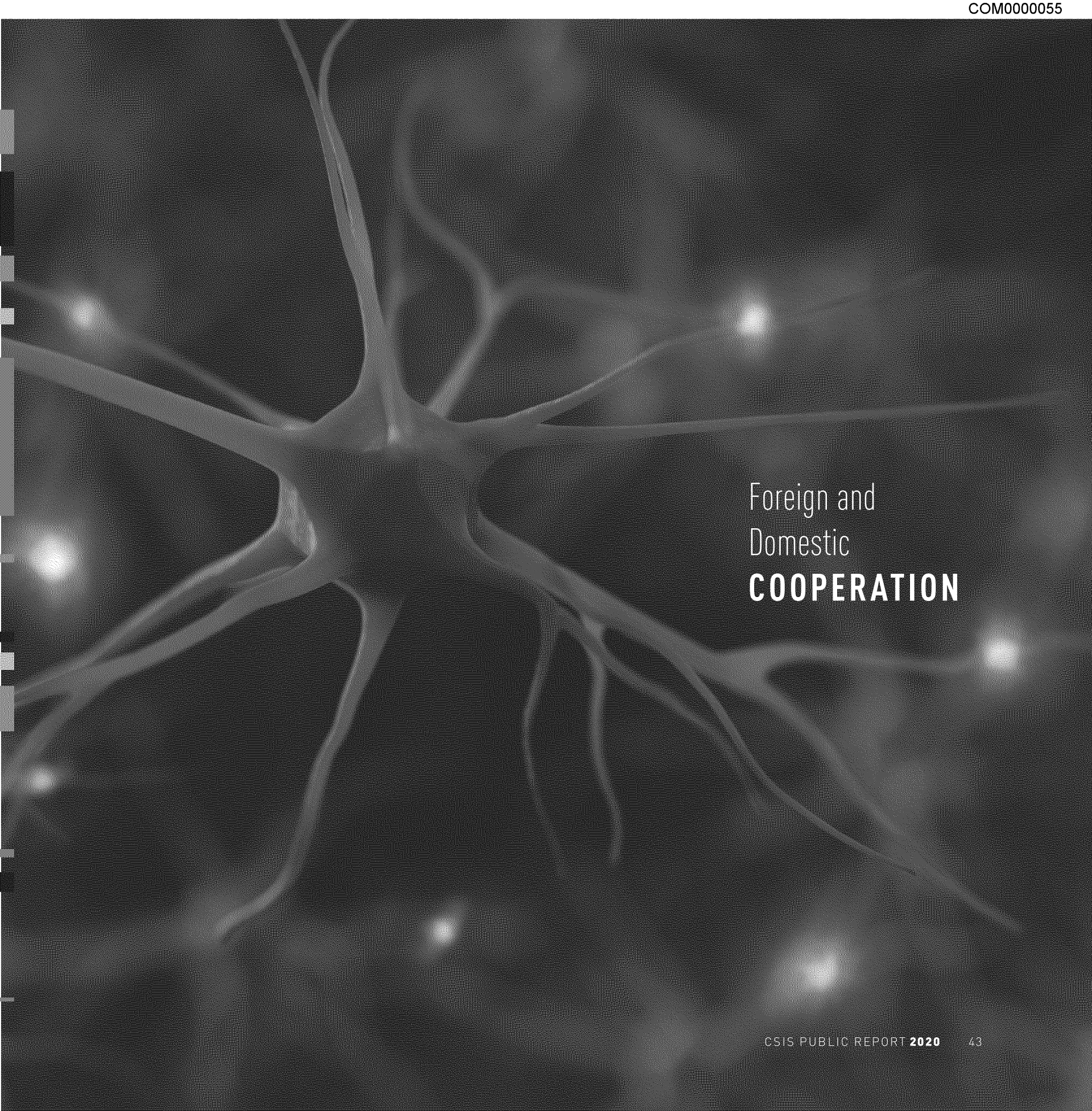
INTERNATIONAL

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 "outposts," are essential 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 global presence. CSIS has forged over many years, and collect information on threats to the world. 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 Canadian security have a nexus to someone or something elsewhere in the world — whether that be an

philosophy, a terrorist actor or a foreign station investigate these threats before they reach Canada's borders.

In 2020, CSIS's international work was impacted by the pandemic. Many countries instituted severe measures in response to the spread of the virus including border closures, travel and meeting restrictions, lockdowns, and curfews. While these measures presented challenges, CSIS employees displayed great ingenuity and resilience to maintain communication with important partners and sources. Despite the difficulties presented by the pandemic, CSIS's intelligence continued to flow, including the sharing 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.

