CSIS Public Report 2024

Forty years

of national security

Canadian Security Intelligence Service
Service canadien du renseignement de sécurité

Canada

Land acknowledgment

The Canadian Security Intelligence Service acknowledges that its 2024 Public Report was written and published on the traditional and unceded territory of the Algonquin Anishinaabeg People.

ISSN: 1495-0138

Catalogue Number: PS71E-PDF

Published in March 2025

www.canada.ca/CSIS

© His Majesty the King in Right of Canada, as represented by the Minister of Public Safety, 2025.

Aussi disponible en français sous le titre : *Rapport public du SCRS 2024*

Table of Contents

Message from the Director 6

Year in review: Progress in an era of change 8

National security in 2024 12

Highlights 16

Intelligence operations 22

Rising to the challenge: Confronting the contemporary threat environment 26

Forty years of protecting national security: The evolution of the threat environment 29

Foreign interference and espionage 34

Violent extremism 43

Cyber security 48

Advancing the mission: Delivering a digital and data-driven CSIS 52

Economic and research security 54

Counter proliferation 58

Security screening 60

The Integrated Threat Assessment Centre 64

Modernizing policy, partnerships and transparency 66

Modernizing the CSIS Act: Enabling CSIS to better protect Canada and all Canadians 68

Building partnerships through engagement 71

Policy and accountability 76

Workforce and culture 80

The "One Mission, One CSIS" transformation journey 82

Initiatives and updates 84

Message from the Director

Looking back on forty years

1993

Construction begins on CSIS National Headquarters in Ottawa.

The construction is completed in 1995.

Year in review: Progress in an era of change

For 40 years now, the Canadian Security Intelligence Service (CSIS) has protected the safety, security and prosperity of Canada and Canadians through trusted intelligence, advice and action. Yet, as we celebrate this milestone, we face a more complex and challenging national security environment than ever in our history. This year's annual report provides us the opportunity to reflect on the work undertaken to transform and address an evolving environment.

I joined CSIS as Director in October 2024, and since that time, I have had the privilege to witness the dedication, skill, and professionalism at CSIS. From technical professionals finding cutting-edge solutions to enable our investigations, to the regional collectors working to understand the networks that facilitate threat activity, to the analysts who evaluate threats and provide advice to government, CSIS employees are steadfast in their commitment to the mission. I have the good fortune of joining the organization after a history of accomplishments by my predecessors. In particular, I'd like to thank David Vigneault for the leadership, wisdom, and direction that enabled a wealth of transformative accomplishments over the last seven years.

In 2024, two high-profile terrorism-related arrests prevented what were shaping up to be deadly attacks. Canada's National Terrorism Threat Level remains at medium, largely because of mitigation efforts in place through intelligence and law enforcement bodies, but make no mistake, the trajectory of terrorism threat trends is concerning. Our social cohesion has been weakening in recent years, creating cleavages in our social fabric that threat actors seek to exploit. Perhaps most concerning, threat actors are seeking to radicalize younger Canadians, largely through online echo chambers that promote hateful rhetoric and incite others to commit violent acts. CSIS, along with the Royal Canadian Mounted Police (RCMP), joined Five Eyes partners in issuing a joint public statement on youth radicalization, and the collective efforts required to disrupt and counter it. This will remain a challenge for us as a society in the months and years ahead.

As international conflict persists, there are increasing threats from foreign nations seeking to bolster their military and economic goals at the expense of Canadian

Looking back, 2024 was full of major achievements and stark reminders. While we have made impressive strides to invest in our capabilities and modernize our authorities, the high pressure of evolving threats and priorities shows no sign of abating. As we respond to the threats we face, Canada must be clear-eyed on the unique role we play in national and international security and intelligence, while we strengthen ties with European and Indo-Pacific allies and reinforce our North American partnerships.

Dan Rogers
Director of the Canadian Security Intelligence Service

interests. With continued global competition for critical minerals, Canada's potential for prosperity is vulnerable to espionage and foreign interference from states like the People's Republic of China, that seek to acquire the supply chains of the future. Russian aggression extends beyond the current war of aggression in Ukraine, targeting Western states that support the international rules-based order, including through reckless sabotage attempts, and the deceptive evasion of sanctions. CSIS has also seen a concerning trend of states leveraging organized crime networks to conduct threat activity, including transnational repression of legitimate speech in Canada. Indeed, 2024 saw the indictment of two Canadians in the US as part of an alleged murder-for-hire plot on behalf of Iranian intelligence.

As a way to enter Canada and conduct activities on our soil, hostile states, transnational organized crime groups and other threat actors attempt to exploit legitimate avenues—the same ones used by people looking to come to Canada to live peacefully with their families or to start anew. CSIS protects our national security through many efforts, such as the Immigration and Citizenship Screening Program. Through consistent and collaborative partnership with Canadian immigration and border officials, and international partners, we identify and mitigate threats before they enter our border. While the Government of Canada has announced a reduction in immigration targets, CSIS and other immigration partners will continue to treat the high volume of cases awaiting screening with the importance and vigilance needed to maintain our safety.

Throughout 2024, CSIS supported the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions (PIFI) through document production and expert testimony. We welcome the conclusions of the Commission's recently released report, and work is already underway to address conclusions, including those related to intelligence dissemination. The report comes at an opportune moment as CSIS takes over as Chair of the Security and Intelligence Threats to Elections (SITE) Task Force, ahead of high-profile political processes, including the Liberal Party of Canada leadership campaign, a federal election, and anticipated provincial and territorial elections throughout 2025. Foreign states are watching closely for vulnerabilities and gaps in Canada's protection of democratic processes. CSIS will continue to protect Canada's democratic institutions alongside our core partners in a non-partisan manner, consistent with our tradition and that of the broader federal public service. This is why CSIS, along with SITE partners, will continue to engage with political parties and other relevant stakeholders to maintain the confidence of Canadians in our democratic systems.

As states and citizens alike adopt new technology, such as encryption and generative artificial intelligence, Canada must keep pace in understanding the varied impacts, opportunities and risks. These advancements can offer opportunities for Canada's growth, while simultaneously equipping those who would seek to do us harm. In response, CSIS has implemented new processes and structures to review and shift resources as priorities emerge. Our teams work closely with international partners—Five Eye partners, European allies and many others—leveraging relationships built and strengthened over time, and which will be more critical than ever as the geopolitical environment evolves.

This year Bill C-70, *An Act respecting countering foreign interference*, updated the CSIS Act in the most significant way since its creation in 1984. It has provided the basis for some of our operational activities to keep pace with advances in technology and has significantly increased our ability to engage with stakeholders outside the Government of Canada. This report outlines how CSIS has acted quickly to implement these changes, including through the provision of 28 resiliency disclosures to non-Government of Canada partners, including provincial governments and private industry organizations. Importantly, the changes to the CSIS Act also include a requirement for the CSIS Act to be reviewed at least every five years, allowing for Parliament to more regularly consider whether our authorities are appropriate in the face of evolving threats.

Budget 2024 recognized the needs of CSIS in combatting global threats and in keeping pace with technological developments, providing targeted investments over the next eight years to enhance our intelligence capabilities and infrastructure. Upgrading the corporate and technical foundations of our work ensures we are well positioned to understand our vulnerabilities in the new world of security without sacrificing ongoing operational requirements. Our work is 24/7. The world is changing, and the number of threats continues to rise. We continually re-evaluate and re-deploy resources to ensure we remain focused on the highest priorities in safeguarding Canada.

Finally, CSIS' successes have been the result of a dedicated, skilled, diverse, and professional workforce. Our future success depends on our ability to retain these skilled intelligence professionals by ensuring a healthy work environment and culture. At the time of writing, we are about to release our first annual report on addressing misconduct and wrongdoing. It will mark an important step forward in transparency and accountability; however, it also makes clear that further efforts are needed to achieve our goals. We're also about to finalize the establishment of the new CSIS Ombuds, who will report directly to me as Director, with a mandate to further our goals toward a fair and respectful workplace and provide an important resource for all CSIS staff who need advice and support to navigate workplace challenges when they arise.

Looking back, 2024 was full of major achievements and stark reminders. While we have made impressive strides to invest in our capabilities and modernize our authorities, the high pressure of evolving threats and priorities shows no sign of abating. As we respond to the threats we face, Canada must be clear-eyed on the unique role we play in national and international security and intelligence, while we strengthen ties with European and Indo-Pacific allies and reinforce our North American partnerships. Partners and their priorities continue to evolve, and our collective task is not getting simpler.

Continued transparency with Canadians is going to be crucial. New legal authorities under Bill C-70 are enabling us to engage with all sectors of society in new ways. This will also hopefully serve to strengthen the trust Canadians feel toward their institutions' ability to protect our national interests and enduring values. I am confident that CSIS intelligence professionals will continue to meet that challenge.

Dan Rogers
Director of the Canadian
Security Intelligence Service

National security in 2024

Looking back on forty years

1985

Air India Flight 182 explodes off the coast of Ireland, killing all 329 people aboard.

Representing the worst global terrorist event involving an aircraft at the time, this tragic event also remains the worst terrorist attack in Canadian history.

Image source: Andre Durand/AFP via Getty Images

January

Two Canadians indicted in the US for their role in an alleged murder-for-hire plot on behalf of Iranian intelligence.

March

The National Security and Intelligence Committee of Parliamentarians (NSICOP) provides its Special Report on Foreign Interference in Canada's Democratic Processes and Institutions to the Prime Minister.

May

The Foreign Interference Commission releases its initial report featuring preliminary findings and conclusions from the inquiry's first phase.

The National Security and Intelligence Review Agency (NSIRA) publishes its special report on the dissemination of intelligence on People's Republic of China (PRC) political foreign interference from 2018 to 2023.

Charges announced in relation to the homicide of Hardeep Singh Nijjar.

Image source:
Don MacKinnon/AFP
via Getty Images

July

Then Director David Vigneault announces his retirement, and Vanessa Lloyd becomes interim Director of CSIS.

Ahmed and Mostafa Eldidi are arrested on terrorism-related charges for allegedly planning a violent attack in Toronto.

October

Dan Rogers is appointed Director of CSIS.

The RCMP releases a statement concerning violent criminal activity occurring in Canada with connections to agents of the Government of India.

The Government of Canada expels six Indian diplomats and consular officials in relation to a targeted campaign against Canadian citizens threatening public safety in Canada.

Five Eyes partners launch Secure Innovation, a shared security advice initiative for tech companies, researchers and investors.

The Government of Canada designates Samidoun a terrorist entity.

February

Then Director David Vigneault testifies for the first time at the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions (PIFI).

Two years since Russia's full scale invasion of Ukraine.

April

Current and former CSIS executives testify at PIFI.

June

Bill C-70, *An Act respecting countering foreign interference* receives royal assent, significantly amending the CSIS Act.

CSIS and Five Eyes partners release historic joint statement on PRC efforts to recruit current and former western military personnel to bolster the PRC's military.

The Government of Canada designates the Iranian Revolutionary Guard Corps a terrorist entity.

The Government of Canada releases a statement concerning state-driven malicious cyber activity targeting Canada.

Image source:
CFOTO/
Future Publishing
via Getty Images

September

Muhammad Shahzeb Khan is arrested on terrorism-related charges for allegedly planning a violent attack against Jewish communities in the United States.

Then Minister of Public Safety Dominic LeBlanc publicly condemns Russian state-owned media outlet, RT (formerly Russia Today), for committing foreign interference activities against the West.

Current and former CSIS executives testify at PIFI.

November

Media first report on the alleged involvement of Russian intelligence operatives in a plot to ship incendiary devices via air transport to destinations in North America and Europe.

December

The Government of Canada designates militant group Ansarallah (Houthis) a terrorist entity.

Five Eyes security intelligence and law enforcement partners release a joint report on the global rise in radicalization of young people towards violent extremism.

Ahmed Eldidi is charged with offences under the *Crimes Against Humanity and War Crimes Act*.

Highlights

Looking back on forty years

2006

A CSIS investigation plays an integral role in disrupting a terrorist plot targeting multiple locations across Ontario, including the Toronto Stock Exchange.

The individuals involved in the plot later became known as the “Toronto 18.”

Intelligence reports

In 2024, CSIS produced over **1,700** intelligence products.

Warrants and judicial authorizations

Warrants obtained in 2024: **133**

Court orders obtained in 2024: **6**

Assistance orders obtained in 2024: **12**

Threat reduction measures (TRMs)

In 2024, CSIS conducted **2** warranted TRMs

13 non-warranted TRMs

Security screening

Government Screening Program

Requests received in 2024:

138,430

Immigration and Citizenship Screening Program

Referrals received in 2024:

538,100

Investment Canada Act (ICA)

ICA notifications screened in 2024 for national security concerns:

1,220

CSIS partnerships

Domestic arrangements

84 arrangements with domestic partners.

Foreign arrangements

317 arrangements in **158** countries and territories.

CSIS outreach

In 2024, CSIS conducted **103** engagement activities.

In addition, CSIS participated in numerous consultation sessions on Bill C-70 with over **50** partner organizations.

In 2024 CSIS met with representatives of:

- Provincial, territorial and municipal governments
- Indigenous governments and organizations
- Civil society and advocacy organizations
- Research and innovation institutes
- Academia

CSIS resiliency disclosures

CSIS provided 28 resiliency disclosures in 2024 after the coming into force of Bill C-70 in June.

CSIS in the news

Number of articles on CSIS*

2024 **3,809**

2023 **6,298**

*Statistics derived from the Government of Canada NewsDesk media monitoring system.

Access to information and privacy (ATIP)

468 ***Access to Information Act*** **(ATIA) requests**

⇩ **50%**

less than 2023

8,961 ***Privacy Act*** **requests**

⇧ **165%**

more than 2023

For the 2024 calendar year, the **on-time compliance rates** stood at

86% for ATIA requests

90% for *Privacy Act* requests from Canadians only

46% for all *Privacy Act* requests**

**Approximately 95% of all *Privacy Act* requests relate to non-Canadians seeking information on the status of their immigration files.

Number of reviews by NSIRA and NSICOP

Ongoing reviews	18
Completed reviews	10
Requests for information	86

PIFI stats

Over **10,000** classified documents identified for the inquiry

6 current and former senior CSIS executives testified at public hearings

More than **70 hours** of CSIS witness testimony to PIFI

Parliamentary appearances

2024	23
2023	12
2022	13
2021	4

1 Intelligence operations

Looking back on forty years

2001

Terrorists bring down four passenger airliners in the United States, killing nearly 3,000 people including two dozen Canadians.

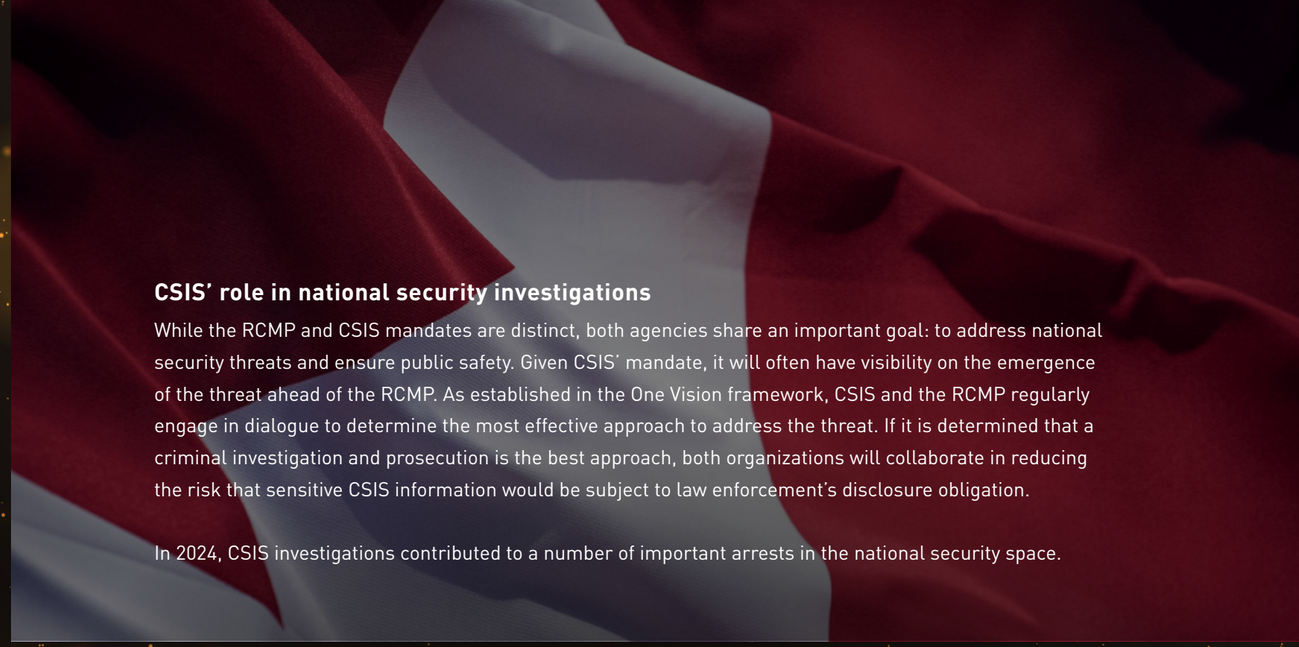
Allies and like-minded partners begin a coordinated international effort to combat terrorism, and in Canada, Bill C-36, the *Anti-terrorism Act* is passed in Parliament on December 18.

Image source: Fabina Sbina/Hugh Zareasky/Getty Images

CSIS investigates activities that fall within the definition of threats to the security of Canada, as outlined in the CSIS Act. Specifically, CSIS is authorized to investigate espionage and sabotage, foreign interference, terrorism and violent extremism, and subversion. Importantly, CSIS is prohibited from investigating lawful advocacy, protest or dissent, except when it is carried out in conjunction with activities that constitute a threat to the security of Canada.

Duties and functions

- **Investigate activities suspected of constituting threats to the security of Canada, report, and advise on these threats to the Government of Canada.**
- **Take measures to reduce threats if there are reasonable grounds to believe the security of Canada is at risk.**
- **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.**
- **Provide assessments by the Integrated Threat Assessment Centre (ITAC) that inform the Government of Canada's decisions and actions relating to the terrorism threat.**



CSIS' role in national security investigations

While the RCMP and CSIS mandates are distinct, both agencies share an important goal: to address national security threats and ensure public safety. Given CSIS' mandate, it will often have visibility on the emergence of the threat ahead of the RCMP. As established in the One Vision framework, CSIS and the RCMP regularly engage in dialogue to determine the most effective approach to address the threat. If it is determined that a criminal investigation and prosecution is the best approach, both organizations will collaborate in reducing the risk that sensitive CSIS information would be subject to law enforcement's disclosure obligation.

In 2024, CSIS investigations contributed to a number of important arrests in the national security space.

Threat reduction measures

CSIS has had the authority to undertake threat reduction measures (TRMs) since 2015. A TRM is an operational action that is intended to reduce a threat to the security of Canada as defined in Section 2 of the CSIS Act. Given its mandate and collection capabilities, CSIS is at times the best placed Government of Canada entity to confront a national security threat.

Generally speaking, TRMs fall into three broad, but non-restrictive categories that include:

Messaging: Directly or indirectly pushing information to a threat actor or person impacted by the threat in an attempt to influence their behaviour or reduce the threat.

Leveraging: Disclosing information to a third party to enable them to take action, at their discretion, against the identified threat-related activities.

Interference: Directly affecting the ability of a threat actor to engage in threat-related activity.

In 2024, CSIS conducted **2** warranted and **13** non-warranted TRMs.

Rising to the challenge: Confronting the contemporary threat environment

As Deputy Director of Operations, Vanessa Lloyd is responsible for directing CSIS' human intelligence collection, intelligence analysis, security screening and threat reduction efforts.

This year's report highlights the persistence of threats that have been investigated by CSIS since our inception in 1984. In some cases, the threat has evolved in how it manifests itself, for example, espionage conducted by foreign intelligence agencies using proxies, or the use of criminal organizations by states to undertake transnational repression. Terrorism threats, which had abated in recent years as a result of purposeful multinational action, are re-emerging in the context of renewed conflict, for example, in the Middle East. New trends such as cyber threats to critical and government infrastructure, are increasing in frequency while others, like economic security, are becoming increasingly complex due to the speed of global innovation combined with increased threat actor focus.

In prior eras, CSIS rose to meet the challenge caused by surges of either espionage or terrorism and most recently, of foreign interference-related activities. In 2024, CSIS actively investigated espionage, foreign interference and terrorist threats, and for the first time in many years, also made concerted efforts to counter sabotage. Overall, threats to Canada's national security have increased and are intensified. Most significantly, CSIS agrees with US and UK intelligence agency statements that never in our combined histories, have we faced threats of such magnitude simultaneously.

As we continue to improve as an organization, the ways in which we respond to protect Canada and its national interest also evolve. In 2024, we built new partnerships, deployed existing tradecraft in new ways and received new legislative authorities, specifically, new judicial authorities to help us address the realities of a digital and data-driven world that transcends geographic boundaries. Additionally, CSIS' collaboration with international partners intensified through coordinated campaigns. We joined together to issue public warnings on intelligence threats,

Overall, threats to Canada's national security have increased and intensified. Most significantly, CSIS agrees with US and UK intelligence agency statements that never in our combined histories, have we faced threats of such magnitude simultaneously.

Vanessa Lloyd
Deputy Director of Operations at the Canadian Security Intelligence Service

to denounce cyber actors and to inform citizens about concerning trends in youth radicalization.

In fact, 2024 saw unprecedented efforts at transparency with Canadians, including on our collaboration with law enforcement on individual cases, joint testimony with government partners before the House of Commons Standing Committee on National Security and the Public Inquiry into Foreign Interference (PIFI), and a public discourse on Canada's response to acts of foreign interference that violated Canadian sovereignty and led to the expulsion of six Government of India officials one year after the Prime Minister's statement on the matter in Parliament.

It was my privilege to speak to Canadians in the company of colleagues from the Canada Border Services Agency, the RCMP, Public Safety, and Immigration, Refugee and Citizenship Canada about CSIS' role in immigration screening in the context of arrests in a terrorism case in summer 2024. Likewise, appearing at PIFI in September provided the opportunity to share with you CSIS' long history of investigating foreign interference, our robust understanding of the threat and the extent of our commitment to address ongoing threat activity in advance of a general election in 2025.

It was also my privilege to serve as interim Director of CSIS, the first woman to fulfill this role, between mid-July and the end of October when we welcomed Dan Rogers to our ranks. My reflection on that assignment and on a year full of challenges and achievements at CSIS evokes enormous pride in its continued contributions to protect Canada and its national interests, as well as concern about the nature and scope of threats we are facing today.

CSIS employees, past and present, come from all backgrounds, and share a common passion: to keep our country secure and defend democracy from those who wish to destabilize it. They work tirelessly to gather intelligence to advise decision makers, and they act decisively to keep Canada safe and prosperous.

It is my hope that this report will foster a continued conversation on how, together with all Canadians, we can improve our country's national security.

Forty years of protecting national security: The evolution of the threat environment

In 2024, CSIS celebrated 40 years of protecting national security as Canada's security intelligence service. This major milestone provoked considerable reflection. How has the threat environment evolved since CSIS' establishment in 1984? How has the threat environment changed, and what remains the same? How did CSIS respond to these threats over the last four decades?

The world was a remarkably different place in 1984 when CSIS was created. The Cold War was still ongoing and conflict between the United States and its allies, and the Soviet bloc represented the greatest threat to international security. At that time, the key national security concern for the Government of Canada was espionage as it sought to stop Soviet bloc nations and other countries conducting espionage activities in Canada from gaining access to sensitive, privileged, and classified information on Canada's military and government sectors. Canada's counter-intelligence efforts throughout the Cold War decades resulted in the removal of around 100 individuals from the country for conducting activities deemed to threaten national security.

Although dangerous, the Cold War threat environment was predictable as it was centered on two main groups of adversarial states conducting espionage activities against one another to gain a strategic military or economic advantage. However, Canada was not immune to terrorism during the Cold War.

In 1985, Canada-based extremists planted and detonated a bomb on Air India Flight 182, killing all 329 people onboard, the majority being Canadian. This tragic event remains the worst terrorist attack in Canadian history and, at the time, was considered the worst global terrorist event involving an aircraft. The failure to disrupt this event provided several hard lessons for CSIS to learn as a young security intelligence service.

The dissolution of the Soviet Union and end of the Cold War in 1991 shifted the threat environment significantly, as the predictably associated with great power conflict was replaced by increasing complexity and volatility. The collapse of the Soviet Union, and later Yugoslavia, created a power vacuum, which led to the emergence of several ethnic and nationalist conflicts within and between newly established nations. Increased violent activity across the globe by transnational terrorist organizations like Al Qaeda posed another significant concern. In response to the changing threat landscape, CSIS reallocated operational resources to meet the Government of Canada's new priority of ensuring public safety. In 1993, CSIS redistributed resources from its Cold War era ratio of 80%/20% in favour of its counter-intelligence program to a more equal ratio of 56%/44% in favour of counter-terrorism. This would prove useful in light of increasingly violent attacks and plots by Al Qaeda, including the 1993 World Trade Centre bombing and the 1998 US Embassy bombings in Dar es Salaam and Nairobi. In 1999, a Canadian nexus to an Al Qaeda plot appeared as Canadian resident Ahmed Ressam planned to bomb Los Angeles International Airport around New Year's Eve, 1999. Thankfully, this plot was foiled by a joint US-Canada investigation into Ressam that included CSIS.

Although public safety was CSIS' primary focus during the 1990s, espionage remained a significant concern, as contrary to observer speculation, espionage activities directed towards Canada by foreign intelligence services did not significantly diminish with the dissolution of the Soviet bloc. In 1996, a CSIS investigation uncovered two Russian illegals living in Toronto under the assumed identities of deceased Canadians to develop their cover legends. The couple was deported from Canada after admitting they were intelligence officers for the Russian Foreign Intelligence Service. In 2020, CSIS acknowledged that it had observed espionage and foreign interference levels not seen since the Cold War.

The rise of information and communications technology in the late 1990s and onwards contributed greatly to the increasing complexity and volatility of the post-Cold War threat environment. The Internet provided terrorist organizations with greater means to organize, direct, and execute terrorist activities, while hostile state actors gained abilities to conduct ever more sophisticated threat activities, such as enhanced targeting of dissidents and critical infrastructure systems. CSIS and its partners understood the necessity of keeping pace with technological change at the time, as falling behind would have significant implications for Canada's national security. This perspective remains true today as the threat environment evolves at an ever more rapid pace with the advent of new technologies like artificial intelligence and quantum computing.

The world forever changed on September 11, 2001. Al Qaeda executed the single largest terrorist attack on US soil via coordinated aircraft hijackings, killing nearly 3,000 people, including 24 Canadians, and injuring countless others. The sheer magnitude of the September 2001 attacks changed the nature of the threat environment in North America, as it demonstrated the ability of terrorist networks to strike, with deadly force, anywhere within its shores. In response, the Government of Canada passed the *Anti-Terrorism Act* to strengthen Canada's ability to combat terrorism by criminalizing the logistical and financial support of terrorist activity in Canada and abroad. Shortly after 9/11, CSIS redirected significant operational resources to address the heightened threat posed by terrorism and intensifying investigations into religiously motivated violent extremism (RMVE) in Canada.

As Canada's military became involved in the US-led War on Terrorism effort in Afghanistan, so too did CSIS. Beginning in 2002, CSIS played a critical role in supporting Canada's combat mission in Afghanistan by collecting information that would save the lives of many Canadian and coalition soldiers, and Afghan civilians.

In 2006, Canada experienced its first instance of 'homegrown' terrorism in the 9/11 era. The public story about the Toronto 18 case began in 2006 with the arrest of a large group of extremists from the Toronto area on suspicion of planning a mass-casualty attack with explosives targeting the Toronto Stock Exchange, CSIS' Toronto office and an unidentified military base. CSIS had been tracking this plot before 2006 as it had been monitoring the suspects closely by using a variety of cutting-edge investigative tools along with more traditional methods such as human sources and physical surveillance. CSIS' investigation, along with the separate, parallel investigation by the RCMP, successfully thwarted the terrorist plot and resulted in the imprisonment of 11 of the original 18.

The elimination of Osama Bin Laden, the architect of the September 2001 attacks, in 2011 symbolized the end of the 9/11 era. However, the rise of Daesh (also known as the Islamic State, ISIS or ISIL) in the 2010s indicated that the RMVE threat would not diminish after Bin Laden's demise. Daesh announced the formation of a so-called caliphate in 2014 after gaining control of significant swaths of territory in Syria and Iraq. Daesh became notorious for committing grotesque acts of violence, including by beheading journalists; conducting a series of prolific terrorist attacks abroad, and attracting thousands of foreign fighters from around the globe. Although Daesh has since lost all of its territories comprising its Middle East caliphate, the group, along with Al Qaeda, still poses a significant threat via its network of provinces, affiliates, related loose online networks, and due to its ability to inspire Canada-based threat actors to commit serious acts of violence, as experienced in Canada in recent years.

The occurrence of ideologically motivated violent extremism (IMVE) activity during the 2010s both globally and domestically led CSIS to establish a greater investigative focus on IMVE. Since 2014, Canada has experienced several IMVE-related attacks, with the most notable being the 2017 Québec City mosque shooting that tragically resulted in the loss of six lives and injury of 19 others by a lone actor. By 2023, IMVE represented approximately 50% of all CSIS counter-terrorism investigations. Lone actor attacks, such as the Québec City attack, characterize the complexity of the contemporary threat environment, as even individuals can have significant impacts on public safety.

1996 - Undercover Russian spies Dmitry Olshevsky and Yelena Olshevskaya are escorted from their deportation hearing in Mississauga.

Image source: Ken Faught/ Toronto Star via Getty Images

In recent years, technology has shifted the threat landscape even further. It is not the same environment CSIS knew in 1984 when it was created. The interconnection of information technology systems and digitization of society has both systematically reshaped human life and consequently revolutionized the threat environment. Now, hostile actors can conduct sophisticated threat activities around the globe at tremendous scales without ever having to step outside their own borders. In terms of espionage, the digitization of information and ubiquity of connected devices has significantly expanded the scope of information vulnerable to collection, while advances in data storage and analytics allow for the stockpiling, analysis, and exploitation of collected data at a scale inconceivable 40 years ago.

During the Cold War period, foreign intelligence services primarily focused targeting efforts on individuals with access to sensitive or classified information, such as Government of Canada employees or researchers working on controlled technologies. Now, foreign intelligence services also target organizations across all sectors and ordinary Canadians through direct or indirect means. Targets include, but are not limited to, tech start-ups and legacy manufacturers; individuals associated with governments at all levels, including federal, provincial, territorial, municipal and Indigenous; students who have had their digital information stolen in a cyber event targeting a university; and patients who lose vital access to healthcare via ransomware targeting a hospital.

While technological advancements have changed how threats to national security can manifest, in general, the key underlying threats facing Canada today remain the same as in decades past. For instance, much like the Cold War period, foreign interference and espionage remain a significant concern. Revelations from testimonies to PIFI concerning the sophistication and level of foreign state interference in our democratic institutions and electoral processes indicate that adversarial states are targeting Canada with far more interest than ever before. Attempts by hostile states to acquire Canadian proprietary information throughout the last four decades signify that economic espionage has remained a key national security threat since CSIS' inception in 1984. The same can be said for violent extremism. Threats posed by violent extremism has ebbed and flowed over the last four decades due to key global events and technological change, however, violent extremists who are driven by a variety of grievances continue to threaten public safety in Canada and around the world with serious acts of violence.

The world has changed considerably in the last 40 years. So has Canada. Major shifts around the world have impacted the threat environment, and while certain threats remain, the rise and dominance of technology and the online ecosystem has given rise to new and rapidly evolving challenges. As a modern intelligence service, CSIS will continue to pivot to address threats posed by hostile actors who seek to undermine the security of Canada and all Canadians.

Foreign interference and espionage

Foreign interference and espionage activities in Canada continue to be pervasive, sophisticated, and persistent. Active targets of these activities include institutions at all levels of government, private sector companies and associations, universities, civil society groups, and ethnic, religious and cultural communities within Canada. Despite increased public awareness in foreign interference and espionage activities in Canada, foreign states remain committed to advancing their interests in ways that are injurious to Canada's national security and social cohesion.

The CSIS Act defines foreign influenced activities as "detrimental to the interests of Canada and clandestine or deceptive, or involve a threat to any person." These activities are also commonly called foreign interference and almost always further the interests of a foreign state to Canada's detriment. Foreign interference undermines Canada's democratic institutions, stifles public discourse, and can involve intimidation or coercion of members of ethnic, religious and cultural communities in Canada. Foreign interference poses a significant threat to Canada's social cohesion, sovereignty, and national security.

The main perpetrators of foreign interference and espionage against Canada include the PRC, India, the Russian Federation, the Islamic Republic of Iran, and Pakistan. During the past year, a number of these states, their intelligence services and other affiliated organizations engaged in a broad range of foreign interference and espionage activities to advance their objectives while undermining Canada's national security, values, and economic prosperity.

When conducting foreign interference and espionage, foreign states may engage in a variety of activities, including:

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.

Malicious cyber activities:
Compromising electronic devices through various means including socially engineered emails, ransomware, and malware.

Information manipulation:
The act of purposely changing, distorting, or controlling information to change the information environment.

Foreign disinformation:
False information that is deliberately created and spread to mislead people, organizations and countries. It is often a part of broader information operations aimed at manipulating audiences.

Transnational repression:
Any efforts undertaken by a foreign state, whether directly or indirectly, to intimidate, influence and/or exact reprisal against individuals or groups living outside their borders. This includes, but is not limited to, acts such as extrajudicial killing, physical assault, unlawful abduction, physical and online surveillance, and obstruction. It could also include pressuring or leveraging a targeted individual's relatives in a foreign state as a means to influence/coerce them.

In 2024 CSIS collaborated with law enforcement to warn private investigator (PI) associations that CSIS and its like-minded foreign partners had observed hostile state actors seeking to hire local PI firms in support of activities incompatible with free and open societies. Such activities include the facilitation of repression and harassment directed by authoritarian governments. PI associations were further warned that hostile state actor engagement of local PI firms can be undertaken deceptively, using alleged financial fraud or marital infidelity as pretexts, or via a third party such as a local law firm.

Protecting National Security in Partnership with all Canadians – Canada.ca

Foreign Interference and You – Canada.ca

From the 1993 CSIS Public Report

Many foreign intelligence services attempt to influence, interfere with or intimidate Canadian ethnic communities. Their purposes vary, but include attempts to ensure that opposition to their governments' policies does not develop in Canada, to recruit agents to operate in Canada and to endeavour covertly to influence Canadian government policy.

Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions (PIFI)

On September 7, 2023, the Government of Canada established PIFI. Justice Marie-Josée Hogue, a judge of the Quebec Court of Appeal, was appointed Commissioner with the agreement of all parties recognized in the House of Commons. The mandate of the Commission was to examine and assess the interference by China, Russia, and other foreign states or non-state actors to confirm the integrity of the 43rd (2019) and 44th (2021) general elections at the national and electoral district levels. The Commission also examined and assessed the flow of information to senior decision-makers, including elected officials, and between the Security and Intelligence Threats to Elections Task Force and the Critical Election Incident Public Protocol panel during the election periods before the 2019 and 2021 elections, and in the weeks following those periods.

The Commission undertook its work in two phases, with the first phase focusing on possible foreign interference activities, and the impact they may have had on the 2019 and 2021 elections. To ensure the Commission had all the necessary CSIS information to enable a comprehensive inquiry, CSIS conducted a thorough collection and production of documents from its operational and analysis holdings to investigate, analyze and advise on the foreign interference threat committed by foreign states or non-state actors related to the 2019 and 2021 elections.

The Commissioner's initial report concluded that while foreign interference occurred during the last two federal elections, it did not undermine the integrity of the electoral system, nor did it impact the outcome of the 2019 and 2021 elections in terms of which party came into power. The report noted that foreign interference is likely to increase and have negative consequences for our democracy unless vigorous measures are taken to detect and counter it.

The inquiry's second phase focused on the capacity of the Government of Canada to detect, deter and counter foreign interference. During this phase, CSIS provided administrative information, including financial and governance information, as it relates to CSIS' capacity to combat foreign interference.

The Commission also heard testimony from diverse community representatives. Maintaining trusted relationships with Canadian ethnic, religious and cultural communities is vital to CSIS' efforts to detect, deter and counter foreign interference, as they are often the first victims. The Commission acknowledged in its initial report that these communities are a common target of foreign interference, and that transnational repression is a real concern.

On January 28, 2025, the Commission released its final report, spanning seven volumes and containing 51 recommendations. The Commission found that certain foreign states are attempting to interfere in Canada's electoral processes and democratic institutions, and that foreign interference had an impact on the electoral ecosystem and has undermined public confidence in Canada's democracy. Despite these findings, the Commission concluded that Canada's democratic institutions have remained robust in spite of attempted foreign interference, and that foreign interference had no impact on the outcome of the 2019 and 2021 federal elections.

Over the course of the inquiry, CSIS identified over 10,000 documents for the Department of Justice to provide to the Commission, and provided more than 70 hours of witness testimony. Additionally, CSIS authored 25 unclassified topical summaries released by the Commission, and contributed to four additional releases. These disclosures facilitated a robust public discussion on national security in Canada and represented the broadest release of intelligence in CSIS' history, demonstrating how intelligence can be safely put into the public domain. With the

inquiry now concluded, CSIS' priority is reviewing the findings and recommendations within the final report, which will guide ongoing efforts to better protect Canada against foreign interference.

People's Republic of China

With one of the world's largest and most active security intelligence systems, the PRC poses the greatest counter-intelligence threat to Canada. Intently focused on ensuring the survival of the Chinese Communist Party (CCP), the PRC Intelligence Services (PRCIS) actively and clandestinely target democratic states around the world. In Canada, they have targeted all levels of government, Canadian citizens, and Chinese communities to advance the PRC's national interests. The Ministry of State Security (MSS) and the Military Intelligence Directorate apply a variety of methods, including leveraging social media and job advertising platforms and offering financial incentives, to recruit individuals to provide the PRC with privileged or classified government documents or proprietary information.

The MSS, the Ministry of Public Security, and the United Front Work Department—the CCP's primary foreign interference administrative arm—also try to recruit people to spy on Canadians who challenge the narratives promoted by the CCP leadership, thereby undermining Canadian values. This kind of foreign interference can include coercing a victim to return to the PRC or threatening their family members in China. The PRC largely targets those it sees as posing a threat to CCP rule, such as human rights activists, political dissidents, journalists, and members of religious and ethnic minority groups. These malign activities compromise the safety, security and rights of Canadians.

In addition to normal diplomatic activity, the PRC employs deceptive and clandestine means to attempt to influence Canadian policy-making at all levels of government (municipal, provincial, federal, Indigenous), and broader civil society, such as non-governmental organizations, media, and academia. Such activity, which seeks to advance PRC national interests while also trying to mask the CCP's hand, aims to weaken Canada's democratic institutions and processes.

CCP-friendly narratives inundate Chinese-language media in Canada. The PRC actively seeks to shape public opinion to gain support for its strategic objectives, while undermining alternative viewpoints, particularly those critical of the CCP. The CCP controls narratives by limiting opportunities for dissenting voices and media organizations to operate in Canada; by providing economic incentives to journalists and media outlets to publish CCP approved content; and by fostering self-censorship through threats and punishments.

The PRC is continually refining and strengthening a suite of national security laws that give the PRCIS extra-judicial and extraterritorial powers. The laws elevate the risk of detention of foreigners who live, visit, or work in the PRC, give the PRC government the ability to control data in China, and require PRC citizens anywhere in the world to assist and cooperate with the PRCIS in support of broadly defined national security work.

The PRC has repeatedly shown that it is willing to use clandestine and deceptive means to acquire intellectual property and emerging technologies, most notably those related to artificial intelligence, quantum computing, biotechnology, and aerospace from Canada and its allies to provide PRC companies and the People's Liberation Army (PLA) with competitive and strategic advantages. With its advanced economy and cutting-edge research expertise, in 2024, Canada was a frequent target of pernicious PRC activities that threatened Canada's economic prosperity.

In 2023 and 2024, CSIS grew concerned about former Canadian Armed Forces pilots employed in the PRC by the Test Flying Academy of South Africa, an entity contracted by the PLA to teach advanced Canadian and North Atlantic Treaty Organization (NATO) fighter pilot tactics, techniques and procedures to PLA pilots. In response, CSIS warned the pilots by letter that such an activity is detrimental to Canada's security interests. In conjunction with its Five Eyes partners, CSIS also issued a historic joint bulletin warning of the PRC's evolving efforts to recruit current and former western service members to bolster the PRC's military.

CSIS assesses that the PRC and CCP organizations will remain an enduring threat to Canada. The PRC's negative perceptions of Bill C-70, *An Act respecting countering foreign interference*, of the establishment of a foreign agent registry, and of Canada's foreign policy initiatives, will likely drive additional concerted foreign interference, disinformation campaigns, and cyber activity in 2025.

Russian Federation

As the war in Ukraine enters its third year and tensions between Russia and NATO member states rise to levels not seen since the end of the Cold War, the Russian Intelligence Services (RIS) and other Russian state actors continue to target Canada, Canadians and Canadian interests. These hostile activities include acts of espionage, sabotage, and foreign influence, all of which pose threats to the security and prosperity of Canada.

The Kremlin believes that it is now engaged in direct conflict with NATO due to the alliances' support to Ukraine. Canada is considered a legitimate target in the Kremlin's eyes and has been the subject of operational planning in relation to potential sabotage operations. Canada is taking all measures necessary to protect the Canadian public and allies from this threat, including intelligence-sharing and close consultation with allied governments. In 2024, CSIS received funding as part of the Government of Canada's overall Security Cooperation Agreement framework guiding support for Ukraine.

The Kremlin has further escalated tensions with the West by sponsoring a series of violent sabotage operations across Europe. Canada's NATO allies have commented publicly that sabotage incidents have increased significantly in Europe since the start of 2024. Operatives, paid by the RIS, are suspected of perpetrating a range of crimes including break-ins and arson at factories and critical national infrastructure, physical attacks and other actions.

Throughout the autumn of 2024 there was widespread media reporting around the world about the potential involvement of Russian intelligence operatives in threats to civil aviation and international supply chains. These hostile actions have resulted in arrests of suspected Russian agents in a number of countries, including Poland and Lithuania, who were involved in efforts to ship incendiary devices to destinations in North America and Europe.

In 2024, CSIS continued to identify foreign interference activities by the RIS targeting the Arctic. In response, CSIS worked to develop and pursue intelligence leads, and engaged with Arctic partners, including Indigenous communities, to counter threats posed by the Russian Federation towards Canada's Arctic sovereignty.

Russia's foreign interference activities aim to disrupt and undermine Western democracies, including Canada, as well as discredit Western policies, partnerships, and alliances. Russia does this through targeting public opinion, and by manipulating and exacerbating existing social divides. These actions further undermine public confidence in political systems and democratic processes in the West, which over time may lead to a shift in public opinion and a wavering in Western support to Ukraine, one of Russia's principal strategic goals.

Russia persistently sponsors disinformation campaigns aimed at discrediting the Government of Canada's position on Ukraine. To counter this threat, Canada has sanctioned over 3,000 individuals and entities in Russia, Ukraine, Belarus and Moldova, including Russian disinformation actors who pose as media pundits, journalists and researchers, and the various arms-length and state-owned institutions that host and support them.

The recent sanctioning and banning of Russian state-owned media outlets in Canada has significantly reduced the means by which Russia traditionally conducts its foreign interference and disinformation operations against the West. However, the Russian Federation has adapted its approach to foreign interference and disinformation in response. Russia relies on online platforms that are controlled by the state and/or the RIS to spread pro-Kremlin narratives, while taking steps to hide such links to the Russian government. Most of the activities conducted by various Russian state-related actors have attempted to discredit and undermine perceived 'hostile' and 'Russophobic' Government of Canada policies against Russia.

Individuals and groups in Canada and elsewhere receive formal or informal direction from Russian government actors to amplify specific narratives to discredit Canada and its allies. When Russia delegates the amplification of divisive issues related to members of Canadian society, the result may mimic an organic public debate process. Wittingly or unwittingly, Western citizens, including Canadians, become disinformation enablers in a multifaceted, complex web of the disinformation networks with hidden links to RIS or Russian state actors, and serve as authenticators of the Kremlin-designed narratives.

Overall, Russia remains willing to engage in increasingly aggressive activities, including spreading malign influence, while accepting a growing risk of collateral damage. For Russia, the effect from these activities far outweighs the potential diplomatic and other consequences associated with them.

India

As PIFI began its first phase of public hearings in March 2024, the extent of the Government of India's involvement in foreign interference became clearer. Indian officials, including their Canada-based proxy agents, engage in a range of activities that seek to influence Canadian communities and politicians. When these activities are deceptive, clandestine or threatening, they are deemed to be foreign interference. These activities attempt to steer Canada's positions into alignment with India's interests on key issues, particularly with respect to how the Indian government perceives Canada-based supporters of an independent homeland that they call Khalistan.

With the re-election of Indian Prime Minister Narendra Modi, India's political course will be a continuation of a Hindu-nationalist policy agenda that has been implemented since Prime Minister Modi was first elected in 2014. Prime Minister Modi and his core ministers and advisers are keen to build India's global influence and counter any activity they consider as 'anti-India,' at home or abroad, in the name of domestic stability and prosperity. With that considered, there is a long history of India arguing that Canada is a haven for 'anti-India' activity, with the separatist Khalistan movement being a particular focus of India's concern, which is rooted in the aftermath of the 1985 Air India bombing and subsequent terrorist activity in India.

The Government of Canada's investigation into the 2023 killing of Canadian citizen Hardeep Singh Nijjar continued in 2024. Four individuals were arrested in May 2024 and charged with first-degree murder and conspiracy to commit murder. Criminal proceedings are ongoing. In mid-October, as part of ongoing RCMP investigations, the RCMP announced that evidence pointed to a link between agents of the Government of India and criminal networks to sow violent activity in South Asian communities in Canada. On October 14, Canada, in the interests of public safety, expelled six Indian diplomats and consular officials in order to disrupt this network. Links between the Government of India and the Nijjar murder signals a significant escalation in India's repression efforts against the Khalistan movement and a clear intent to target individuals in North America.

As PIFI reached the end of its public hearings and South Asian communities in Canada expressed concerns over Government of India pressure tactics and targeting, CSIS noted that this form of foreign interference, called transnational repression, plays a central role in India's activity in Canada. Transnational repression is a well-established tactic for foreign governments to exploit communities they view as their ethnic populations.

Canada must remain vigilant about continued foreign interference conducted by the Government of India, not only within ethnic, religious and cultural communities but also in Canada's political system. CSIS will continue to observe and assess the nature and extent of India's activities in Canada.

Islamic Republic of Iran

In 2024, Iran continued to advance its policy of cementing itself as a regional power and, for the first time in its history, engaged in a direct exchange of fire with Israel. Despite electing a new, more moderate president, Iran continued to support its allies and proxies across the Middle East in Iraq, Syria, Lebanon and Yemen to counter both Israel's military operations in Gaza and Lebanon and, more broadly, the United States and Western interests. The "Axis of Resistance," an Iranian-led regional alliance with Syria, Lebanese Hezbollah, and Iran-aligned non-state armed actors in Iraq and Yemen, conducted multiple military attacks against Israel. In two separate attacks, on April 13 and October 1, 2024, Iran launched more than 500 ballistic missiles, uncrewed aerial vehicles, and cruise missiles against Israel. Despite its efforts to project strength, Iran has suffered numerous losses in 2024, as the capabilities of its regional partners, notably Hamas and Lebanese Hezbollah, have been significantly degraded. The deaths of Hamas leader Ismail Haniyeh and Lebanese Hezbollah leader Hassan Nasrallah, is a significant blow to Iranian interests.

In June 2024, the Government of Canada designated Iran's Islamic Revolutionary Guard Corps (IRGC) as a terrorist entity under the *Criminal Code*, adding to its previous designation of the IRGC Qods Force (IRGC-QF) in 2012. Between October 2022 and September 2024, Canada has imposed sanctions under the Special Economic Measures (Iran) Regulations against 205 Iranian individuals and 250 Iranian entities linked to systematic and gross violations of human rights in the country.

In 2024, Canadian citizens Damion Ryan and Adam Pearson were indicted by the US Department of Justice for their role in an alleged murder-for-hire plot targeting two residents of Maryland who had previously defected from Iran. The Canadian men were allegedly directed by Iranian-Turkish narcotics trafficker, Naji Sharifi Zindashti, who led a network of individuals that targeted Iranian dissidents and opposition activists for assassination at the behest of Iran's Ministry of Intelligence and Security. This network has carried out numerous acts of transnational repression including assassinations and kidnappings across multiple jurisdictions in an attempt to silence Iran's perceived critics.

CSIS continues to investigate threats to life emanating from the Islamic Republic of Iran based on credible intelligence. CSIS assesses that Iran will continue to use proxies, such as individuals involved with transnational organized crime networks, when it targets perceived enemies living in foreign countries, including Canada. Iranian threat-related activities directed at Canada and its allies are likely to continue in 2025, and may increase depending on developments in the Middle East and the Iranian regime's own threat perceptions.

Pakistan

In May 2024, the PIFI initial report named Pakistan amongst states that have interfered in Canadian democratic processes. In June 2024, NSICOP published its Special Report on Foreign Interference in Canada's Democratic Processes and Institutions, which also highlighted how Pakistan was amongst the countries

to have engaged in foreign interference activities that posed a significant risk to national security, principally by undermining Canada's fundamental institutions and eroding the rights and freedoms of people in Canada.

The Government of Pakistan engaged in foreign interference in previous federal and provincial elections, for example, by attempting to clandestinely affect the selection of politicians and candidates who are perceived to be more pro-Pakistan than pro-India. Between September 2018 and September 2023, CSIS conducted a threat reduction measure to reduce the Pakistan foreign interference threat, which was later assessed as effective.

In addition to interference against Canadian democratic processes, Pakistan engaged in transnational repression by suppressing dissidents and critics in Canada. These activities represent one of the most egregious forms of foreign interference.

Pakistan conducts foreign interference against Canada to promote political, security and economic stability in Pakistan and to counter India's growing global influence. Canada is an attractive foreign interference target due to its significant South Asian community and presence of groups who may be utilized as pro-Pakistan or anti-India proxies. CSIS assesses that Pakistan will continue to target various levels of government as well as ethnic, cultural and religious communities, specifically in relation to electoral nomination processes. They may also target media.

From the 1992 CSIS Public Report

While not as hostile as they once were, Russia's and the People's Republic of China's intelligence services nevertheless remain active against Western interests. Currently, CSIS has identified several countries with known or suspected, undeclared intelligence officers operating in Canada. They conduct activities ranging from monitoring their own citizens to penetrating and coercing Canadian ethnic communities and/or collecting military, economic and technical intelligence.

Violent extremism

Violent extremism, whether it is religiously, ideologically, or politically motivated, continues to pose a significant threat to Canada's national security. The overall violent extremist threat to Canada has remained at a heightened level, as online radicalization has contributed to an increased number of extremists mobilizing to violence, some of whom are youth. Monitoring, investigating, and mitigating these serious threats are a key priority for CSIS and its national security partners.

While only a small number of Canadians are actually willing to engage in extremist violence in support of a cause, their actions continue to have devastating consequences on national security. The collective threat posed by religiously motivated violent extremism (RMVE) and ideologically motivated violent extremism (IMVE) grew during 2024.

Religiously motivated violent extremism

RMVE encourages the use of violence as part of a spiritual struggle against a perceived immoral system. Like other terrorist movements, RMVE actors utilize violence to intimidate or compel a desired action, or to restrain a government from taking an action.

In 2024, multiple RMVE adherents were arrested in Canada for terrorism-related offences. They were mainly motivated by the conflicts in the Middle East, inspired by Daesh, and planned to carry out an attack either alone or as part of a small group. These actors were planning to use low-sophistication means of attack against soft targets: a person or group, place, or thing that is easily accessible to the public and generally left unprotected.

CSIS counter-terrorism investigations resulted in two high-profile arrests in summer 2024 of Daesh-inspired individuals. In July, father and son duo, Ahmed and Mostafa Eldidi, were arrested while allegedly in the advanced stages of planning a mass casualty attack in the Toronto area. In September, Muhammad Shahzeb Khan, a Pakistani citizen living in the Toronto area, was arrested while attempting to illegally cross into the United States to allegedly conduct a mass casualty attack against Jewish people in New York City. Khan allegedly planned on using firearms in an attack around the anniversary of the October 7, 2023, Hamas attack on Israel. CSIS is proud to have played an integral role in preventing these serious acts of terrorist violence from occurring in Canada and the US.

RMVE organizations will continue to take advantage of geographic safe havens provided by poor governance and regional conflicts to plan, enable, direct and conduct acts of terrorism. As international counter-terrorism pressure diminishes in areas of Africa, the Middle East and Afghanistan, we can expect a resurgence of terrorist activities against Western interests. The ongoing conflict in Gaza has the potential to inspire an entire new generation of RMVE adherents, and has already done so to some extent, as a pillar of the Daesh narrative in particular. CSIS is increasingly concerned by Daesh's reach into Canada and Western countries and the growing potential of Daesh-enabled or directed attacks in Canada and Western countries.

CSIS assesses that RMVE actors will continue to pose a domestic threat to Canada in 2025. Pro-RMVE content online will almost certainly continue to radicalize individuals with ties to Canada and it is highly likely that international conflicts, in particular the current conflict in the Middle East, will continue to contribute to and drive RMVE radicalization in the coming years. In response, CSIS will continue to investigate and reduce the threat activities of violent extremists in close collaboration with law enforcement partners to protect public safety.

Canadian extremist travellers

Canadian extremist travellers (CETs) are individuals who hold Canadian citizenship, permanent residency or a valid visa for Canada, and are suspected of having travelled abroad to engage in terrorism-related activities, such as individuals who travelled to Syria and Iraq in the 2010s, and in recent years to join Daesh. Although the current CET threat posed to Canada is primarily religiously motivated, individuals may elect to leave Canada to engage in terrorist activity abroad for ideological or political reasons as well.

CSIS continues to pursue a number of investigations against CETs who have travelled abroad and joined violent extremist organizations in a number of regions including the Middle East and Africa. CSIS is aware of a small number of Canadians who aspire to travel to join RMVE groups in the Middle East, Afghanistan, and Africa.

In 2024, while no CET returned to Canada, six Canadian children were repatriated to Canada from an internally displaced persons camp in Syria.

Ideologically motivated violent extremism

The IMVE threat is complex, constantly evolving, and fueled by entities (individuals, cells, groups, or networks) driven by a range of influences rather than a singular belief system. Extreme racist, anti-gender and identity, and anti-authority views combined with personal grievances can result in an individual's willingness to incite, enable or mobilize to violence.

CSIS classifies IMVE into four general categories:

1. Xenophobic violence, which includes racially-motivated and ethno-nationalist violence.
2. Anti-authority violence, which includes anti-government and anti-law enforcement violence.
3. Gender identity-driven violence, which includes violent misogyny (including incel movement), anti-2SLGBTQIA+, and anti-gender driven ideology violence.
4. Other grievance-driven and ideologically motivated violence.

There is no single worldview and no single radicalization pathway for IMVE, as they are often as unique as the individual. Rather, threat actors are increasingly driven by a range of often seemingly contradictory grievances, ideas and highly personalized narratives from across the traditional left/right-wing ideological spectrum and are often deeply intertwined with conspiracy theories. CSIS also notes the ideological mixing of these diverse grievance narratives within the IMVE landscape and across the IMVE/RMVE divide add to the complexity and challenge for security intelligence services to understand, assess and articulate this threat from a national security perspective. One result of this complexity is the chaotic nature of online spaces, which continually attempt to desensitize individuals to extreme racism, sexism, and anti-government rhetoric. While an increasingly vague ideological foundation based on the mixing of beliefs and grievance narratives is not a new concept, CSIS notes that this 'hybrid ideology' is more prevalent and remains a national security threat. As such, CSIS faces a new range of complex and often confusing threats, including those posed by accelerationist and occult networks (AONs).

AONs are IMVE networks that combine a variety of extremist beliefs, including militant accelerationism (advocating for the violent destruction of society), neo-Nazism, and satanic occultism. These networks are active on numerous public and private online platforms, which they use to glorify and promote a range of threat behaviours that include acts of serious violence, child sexual exploitation and child sexual abuse material, sextortion, self-harm, arson, and animal abuse. Violent online groups, including AONs, utilize online platforms and applications such as Discord, Telegram, Roblox and Minecraft to deliberately target, victimize and recruit vulnerable children and youth between the ages of 8 and 17 years old. Although AONs engage in acts that are both vile and criminal, CSIS assesses that national security threats posed by AONs emanate from the fringes of the networks, as opposed to the networks in their entirety, via individuals who are planning or plotting to engage in serious acts of extremist violence and those who seek to inspire others to engage in extremist violence.

The greatest threat of IMVE radicalization comes from anonymous, public and private transnational online spaces. CSIS also assesses that IMVE threat actors come in two forms: those who mobilize or attempt to mobilize to violence, and those whose primary objective is not to engage in violence, but rather to inspire others to engage in acts of serious violence. CSIS is aware

of several IMVE threat actors who were not actively organizing a mass casualty attack. However, through their words, propaganda, and/or support to listed terrorist entities, CSIS assesses that their intent was to inspire others to commit acts of serious violence. CSIS notes that some IMVE threat actors can both engage in serious violence and attempt to inspire future attackers, often through the release of a manifesto.

Politically motivated violent extremism

Politically motivated violent extremism (PMVE) encourages the use of violence to establish new political systems or new structures or norms within existing systems. PMVE actors engage in the planning, financing and facilitating of attacks, globally, in order to establish new political systems or entities.

Since the mid-1980s, the PMVE threat in Canada has manifested primarily through Canada-based Khalistani extremists (CBKEs) seeking to use and support violent means to create an independent nation state called Khalistan, largely within Punjab, India.

Some Canadians participate in legitimate and peaceful campaigning to support the Khalistan movement. Non-violent advocacy for an independent state of Khalistan is not considered extremism. Only a small group of individuals are considered Khalistani extremists because they continue to use Canada as a base for the promotion, fundraising or planning of violence primarily in India. While there were no CBKE-related attacks in Canada in 2024, ongoing involvement in violent activities by CBKEs continues to pose a national security threat to Canada and Canadian interests. In particular, real and perceived Khalistani extremism emerging from Canada continues to drive Indian foreign interference activities in Canada.

CSIS also continues to monitor emerging threats and contribute to the Government of Canada terrorist listing process. In October 2024, the Government of Canada listed Samidoun (also known as the Palestinian Prisoner Solidarity Network) as a terrorist entity under the *Criminal Code*. Samidoun is associated with and advances the interests of the Popular Front for the Liberation of Palestine (PFLP), a Palestinian organization and listed terrorist entity since 2003. In December 2024, the Government of Canada also listed Ansarallah (Houthis), a Yemen-based group, as a terrorist entity. Ansarallah attacked dozens of maritime vessels in the Red Sea in the past year and is closely linked to the IRGC-Qods Force and Hezbollah, two other listed terrorist entities in Canada.

Youth radicalization

In recent years, Canada has seen a growing trend of youth (some as young as 13) involved in select counter-terrorism investigations. The online environment's anonymous and permissive nature has made it easier for young people, who are often more vulnerable to radicalization, to access extremist content, on a wide variety of platforms, including gaming and social media, bypassing traditional gatekeepers like parents and educators. Youth radicalization is a complex, individualized process driven by a range of factors. These can include a quest for significance, intergenerational conflict, cultural identity issues, cultural integration conflicts, mental health concerns, traumatizing events, and personal grievances. Exposure to moderately objectionable material containing extremist narratives can rapidly escalate into support for violence.

Youth are capable of taking on key roles in extremist activities, including the creation and distribution of violent extremist content, the radicalization and recruitment of others, the leadership of violent extremist groups, and the planning and perpetration of terrorist attacks. Identifying the threat posed by a minor at an early stage can enable timely interventions, such as redirecting them to countering violent extremism programs or providing access to mental health services, thereby preventing escalation and potential law enforcement involvement.

CSIS will maintain and strengthen its collaboration with domestic and international partners to prevent and counter the radicalization of youth.

In February 2024, an Ottawa youth was arrested and charged with three terrorism-related offences, including knowingly facilitating terrorist activity by seeking to acquire a prohibited firearm. The youth is the co-conspirator of another Ottawa youth arrested in December 2023 on terrorism-related offences and who was subsequently charged in February 2024 with two additional terrorism-related offences in relation to their planning of a terrorist attack in Ottawa. A CSIS investigation into the plot played a significant role in preventing the attack.

In December 2024, Five Eyes security intelligence and law enforcement partners, including CSIS and the RCMP, released a joint report titled *Young People and Violent Extremism: A Call for Collective Action*. The report highlights the increasing concern among Five Eyes partners regarding the radicalization of young people towards violent extremism, including those who support, plan, or carry out terrorist activities. The report highlights real world examples from Five Eyes countries concerning the radicalization of young people to shed light on the severity of this increasing threat. ■

From the 2000 CSIS Public Report

Terrorism in the years ahead is expected to become more violent, indiscriminate, and unpredictable than in recent years [...] There will likely be terrorist attacks whose sole aim would be to incite terror itself. A hardening attitude and willingness on the part of certain terrorist organizations to directly support terrorist operations in North America reinforce the belief that Canadians, now more than ever, are potential victims and Canada a potential venue for terrorist attacks.

Cyber security

Canada's strong democratic institutions, advanced economy, innovative research sectors, and leading academic institutions make Canada an attractive target for cyber-enabled espionage, sabotage, and foreign influenced activities, all of which pose significant threats to Canada's national security. Cyber-enabled foreign interference activities targeting Canada will continue to increase in breadth and sophistication.

CSIS' role in cyber security

Working closely with trusted domestic and foreign partners, CSIS actively takes steps to investigate and reduce threats to the security of Canada posed by hostile cyber actors, including those in the PRC, Russia, and Iran. To do this, CSIS employs the entirety of its investigative techniques, including the use of dedicated human sources, warranted collection opportunities, and other covert methods. When appropriate, CSIS also takes steps to reduce threats to the security of Canada and Canadian critical infrastructure using its threat reduction mandate.

CSIS routinely provides high-quality intelligence assessments to our government partners, allowing them to make informed policy and operational decisions. CSIS also shares these assessments and investigative leads with our trusted foreign partners in order to assist them in ensuring the integrity of the global information infrastructure, upon which Canadian security relies.

In recent years, in addition to its traditional covert intelligence work, CSIS has also assumed a vital public facing role in the cyber domain. CSIS efforts have assisted to harden the Canadian cyber ecosystem and reduce the attack surface for hostile actors. Close collaboration with industry sectors, Indigenous groups, and governments, along with presentations and panel discussions at cyber industry and academic conferences, helps the whole-of-government approach to build awareness and resilience to an ever-growing cyber threat environment.

Canada's cyber threat environment is continuously changing and adapting with the development of new technologies. To counter these threats, the Government of Canada and civil society must continue to collaborate to mitigate them.

State-sponsored cyber activity

PRC state cyber actors continue widespread cyber espionage against a range of sectors and targets within Canada, including government, academic institutions, private industry and civil society organizations. Cyber espionage targeting Canadian and allied entities is conducted to provide the PRC government with strategic military, political, or economic advantages over its adversaries. In one such example made public in 2024, PRC cyber threat actors targeted members of the Inter-Parliamentary Alliance on China in 2021, including multiple Canadian members of Parliament.

The digital infrastructure used by these threat actors came into focus in 2024, with Canada joining international partners in warning the public about a PRC-based company, Integrity Technology Group, that controlled a network of compromised, internet-connected devices (commonly known as a botnet) being used for malicious cyber activity. The devices in the network, dubbed Raptor Train by the cyber security industry, were located throughout North America, South America, Europe, Africa, Southeast Asia and Australia. Activity on the network was consistent with the tactics, techniques and procedures associated with Flax Typhoon, a PRC cyber threat actor known to target entities in North America, Southeast Asia, and Africa, including government agencies, the education sector, critical manufacturing, and information technology organizations. In cooperation with foreign and domestic partners, CSIS worked to mitigate the threat posed by this botnet to Canadians.

The PRC's military, police, and intelligence services are supported by a large number of private sector information security companies that provide novel capabilities and personnel to develop malicious cyber capabilities. Combined with the PRC national security laws, CSIS assesses that Canadian businesses that partner with such entities, and Canadians who work with them, risk indirectly bolstering the military and intelligence cyber capabilities of the PRC to the possible detriment of the security interests of Canada and its allies.

CSIS continues to be concerned with the activities of PRC cyber actors targeting North American critical infrastructure in order to pre-position disruptive capabilities. Pre-positioning occurs when a threat actor covertly accesses internet-connected devices and leverages techniques to maintain a network presence by blending in with legitimate network activity. While the direct threat to Canada's critical infrastructure from PRC state-sponsored actors is likely lower than that to US infrastructure, the interdependence between both countries' sectors infer that a major disruption to the US would likely affect Canada as well.

Russia continues to conduct disruptive cyber activities against its adversaries and coordinates with non-state groups to conduct malicious cyber activity against Ukraine and NATO allies, including Canada.

From the 2000 CSIS Public Report

A principal factor currently underlying all security issues is the impact of technological change. The reliance of modern countries on the unimpeded and secure flow of information electronically has created vulnerabilities within their information infrastructure that are serious enough to raise international security concerns. The already complex investigation of threats posed by terrorism and intelligence activity is further complicated by the adoption of cyber technology by foreign intelligence organizations and terrorist groups.

In 2024, CSIS alongside its foreign and domestic partners, participated in a cyber disruption operation against a Russian General Staff Main Intelligence Directorate (GRU)-controlled botnet of hundreds of compromised routers around the world, including in Canada. The botnet was believed to be used by Advanced Persistent Threat 28 (APT28) to conceal and otherwise enable a variety of malicious cyber activities. These activities included spear-phishing and similar credential harvesting campaigns against targets of intelligence interest to the Russian government.

Iran continues to combine offensive cyber operations with cyber-enabled influence operations in the pursuit of its geopolitical goals. While Canada is not a high priority target for Iranian cyber activity, Canadians are targeted for opportunistic credential harvesting, phishing attacks, and exploitation. Iran also uses malicious cyber activity to repress and manipulate Canada-based dissidents.

More broadly, as of late 2023, Iran-aligned cyber actors have been targeting Western critical infrastructure. Iran-aligned cyber groups, such as the IRGC-linked CyberAv3ngers, have used a variety of different techniques and are attempting to compromise high-value organizations across multiple different critical infrastructure sectors, including healthcare and public health, government, information technology, engineering and energy sectors.

Non-state cyber actors

Non-state actors continue to play a prominent role in the cyberspace threat landscape. Ransomware campaigns continue to pose a threat to Canadian critical infrastructure and sensitive information. Cybercriminals are typically opportunistic actors who operate for financial gain. However, their malicious cyber activity can constitute national security threats in certain circumstances, such as when they disrupt the operations of critical infrastructure or other sensitive sectors. State actors have, and will likely continue to, leverage or condone non-state actor ransomware campaigns that advance their geopolitical interests. Ransomware campaigns may also involve threats to leak data on the dark web in order to induce victims into paying ransoms, putting Canadian personal identifiable information at risk.

The commercial proliferation of cyber capabilities enables an ever-growing array of actors to conduct malicious activities, including those who undermine democratic values and exert foreign influence. This not only serves to equalize competition in cyberspace for those who can afford to purchase off-the-shelf capabilities, but will also further complicate attribution efforts. The services offered by these companies range from defensive, meaning penetration testing and vulnerability analysis, to more offensive techniques, such as lawful intercept solutions or computer network exploitation suites. Open-source reporting suggests that multiple authoritarian regimes have leveraged such tools to target lawyers, journalists, politicians and human rights defenders, including in Canada. ■

Advancing the mission: Delivering a digital and data-driven CSIS

As Assistant Director of Technology, Jacqueline Mayda is responsible for supporting the enablement of CSIS' operational functions and enhancing the operational effectiveness of the organization through technology.

As the threat environment evolves and the demand for CSIS intelligence increases, CSIS operations, systems and processes need to keep pace, which is why success depends on CSIS being digital and data-driven.

CSIS uses a variety of collection methods to monitor activities suspected to constitute a threat to national security, and derive intelligence that is comprised of useful actionable information. Information is composed of data. Therefore, CSIS must have the required tools and capacity to examine and cross reference data in an effective manner to ensure it remains one step ahead of threat actors.

Understanding how to treat and utilize massive amounts of data to extract value is a dilemma that most modern organizations must deal with. However, with CSIS there are added complexities. As a covert intelligence organization, we must protect our employees and sources. Our data must not be traceable back to their origin, as failing to ensure this could result in lives being put at risk, and could compromise operations protecting national security.

CSIS must conduct its duties in a digital environment where traditional methods of conducting intelligence operations have become increasingly difficult and dangerous. To ensure the quality of its intelligence, CSIS must continue adapting and modernizing its operations. Here are a few examples of how we are doing that:

- We have operationalized a suite of digital security risk mitigation measures to protect CSIS from malicious cyber activities that aim to steal classified data, disrupt operations, or manipulate intelligence.

- We are working with domestic and international intelligence partners to collect, share, manage, store, and process vast amounts of data from various sources to help protect domestic and international security. Under an overarching project called Data Fuelled Intelligence, CSIS is consolidating existing data while increasing the variety and volume of data analysis to support the provision of superior, actionable intelligence assessments.

- Recognising the opportunities associated with artificial intelligence (AI), we are implementing AI pilot programs across CSIS in a manner consistent with the Government of Canada's guiding principles on the reasonable use of artificial intelligence to support our mission.

- We have assembled elite Computer Network Exploitation teams to drive success in this highly specialized discipline that has emerged as a critical component of modern intelligence gathering, enabling the covert collection of vital information from computer systems.

As both the digital and threat environments continue to evolve, so too will CSIS to meet the threats and opportunities associated with them. Going forward, CSIS will continue to prioritize the advancement of its digital and data-driven capacities in a prudent, legal and ethical manner to ensure it remains one step ahead of Canada's adversaries. ■

As the threat environment evolves and the demand for CSIS intelligence increases, CSIS operations, systems and processes need to keep pace, which is why success depends on CSIS being digital and data-driven.

Jacqueline Mayda
Assistant Director of Technology at the Canadian Security Intelligence Service

Economic and research security

As a trading nation and global leader in the research and technology sector, Canada is a prime target for hostile state actors, including the PRC, Russia, and Iran, who seek to acquire sensitive research and technology to advance their own strategic political, economic, and military interests. Threats to economic and research security are increasingly complex and multifaceted in nature as hostile states continue to take advantage of weaknesses in Canada's legal and regulatory frameworks to undermine Canadian interests.

Trade and investment

Threats to Canada's economic security continue to be shaped by increasing geo-economic competition. In addition to attempts to acquire Canadian technology and data, hostile state actors continue to seek privileged knowledge of Canada's plans, priorities, and intentions for navigating this environment, including advance knowledge of Canadian policy and regulatory decision-making.

Foreign interference by hostile state actors in Canadian supply chains and international trading relations represents a threat to Canada's national security and prosperity. As global trading relationships adapt to geo-economic competition and new forms of globalization, hostile state actors have sought to overtly and clandestinely undermine Canada's efforts to increase its resiliency to economic security threats. Examples of such interference activities include employing proxy influence actors, economic coercion, supply chain manipulation, and disinformation/misinformation campaigns. While such interference has been observed in multiple sectors of the economy, including interactive digital media and emerging technologies, CSIS notes that of Canada's natural resources sector, which includes critical minerals and agricultural exports, in particular has been targeted due to the strategic relevance it has for both Canada and its trading partners.

In an effort to increase awareness and build resilience, CSIS has briefed various provincial and territorial partners using section 19 of the CSIS Act. CSIS has worked closely with the territorial governments and Indigenous local governing bodies in the Arctic. These briefings and corresponding unclassified materials prepared have resulted in additional requests for engagement including further briefings.

In 2024, CSIS engaged on a regular basis with the Canadian Chamber of Commerce, the national organization connecting businesses of all sizes, from all sectors of the economy and in every federal riding across the country. Engagement with the Chamber allows CSIS to brief a wide spectrum of Canadian businesses on economic threats.

CSIS continues to support the national security review of foreign direct investment in Canada under the *Investment Canada Act* (ICA). In collaboration with the other members of the Canadian security and intelligence community, CSIS continues to provide Government of Canada policymakers with intelligence to inform their decisions on mitigating national security risks posed by foreign investment. In 2024, CSIS screened 1,220 ICA notifications for potential national security concerns.

Research security

CSIS contributes to and supports Government of Canada efforts to strengthen research security and ultimately safeguard Canadian research and industry. CSIS supports Government of Canada partners in reviewing federal research funding for national security consideration through the National Security Guidelines for Research Partnerships and the Policy on Sensitive Technology Research and Affiliations of Concern. Furthermore, CSIS aims to increase awareness of threat activity targeting Canada's research sector through engagement with universities, academics, research associations, and companies.

Sensitive technology

Sensitive technology consists of advanced and emerging technologies, such as quantum computing, artificial intelligence (AI), biotechnology and others, the transfer of which could cause injury to Canada's national security and defence through degradation of Canadian or allied military or intelligence capabilities, or enhancement of adversarial military or intelligence capabilities. Sensitive technology can also comprise technologies that are important to Canada's development and economic competitiveness in the global market. These technologies are often characterized by rapid growth, high potential for disruption, and significant investment. CSIS focuses on, amongst other areas, the exploitation of economic activities by hostile state actors to acquire access to and transfer of sensitive technologies, expertise, data, and other strategic resources to advance their own military, intelligence, or addressing economic capabilities at the expense of Canadian and allied interests.

Five Eyes economic security initiative - Secure Innovation

Following the 2023 Emerging Technology and Securing Innovation Security Summit at Stanford University in Palo Alto, California, the domestic security intelligence services of the Five Eyes international intelligence alliance, launched the Secure Innovation initiative in October 2024.

From the
1993 CSIS
Public Report

Studies conducted by CSIS in 1990-91 led to the observation that a small group of leading-edge companies in Canada had been targeted by foreign intelligence services between 1980 and 1990. In fact, in a more recent case of economic espionage, which involved support from a foreign government, a Canadian company lost a major contract after precise information contained in the company's tender was passed to an offshore competitor.

Secure Innovation is a shared security advice initiative to help protect emerging technology companies, researchers, and investors from a range of threats, particularly those from hostile state actors.

CSIS and its Five Eyes partners have committed to work collaboratively against hostile state actors that target and steal technology and research from Five Eyes economies. Secure Innovation provides the tech sector with a set of cost-effective measures that companies can take to better protect their ideas, reputation and future success. Businesses in Australia, Canada, New Zealand, the UK, and the US can take advantage of a collection of Secure Innovation resources, guidance and products, which are now available across all Five Eyes countries. CSIS will continue to engage with its Five Eyes partners on this important initiative, and will seek to release additional resources in the future to assist our community partners, businesses, and academia in mitigating the threats to Canada's economic security.

Critical infrastructure

All ten sectors of Canada's critical infrastructure (finance, energy and utilities, food, transportation, government, information and communications technology, health, water, safety and manufacturing) represent high value targets for threat activities, such as foreign interference, espionage and sabotage, including for the purposes of intentional service disruptions and intellectual property theft. For example, a former Hydro Québec employee was charged with economic espionage on behalf of the PRC, and is accused of having provided his research on battery and electric vehicle technology to entities in the PRC, harming Hydro Québec's prosperity.

To counter the evolving threats to the financial sector, CSIS collaborates with partners, including the Financial Transactions and Reports Analysis Centre of Canada, the Office of the Superintendent of Financial Institutions, and the Department of Finance, to collect, analyse and advise on national security threats.

Given the interconnected nature of Canada's critical infrastructure, a disruption in one sector, such as the energy and utilities sector, can have cascading effects on other key sectors. Russia has previously targeted foreign critical infrastructure via malicious cyber activity, targeting Ukraine's electrical grid in 2015 and 2016, and its largest telecommunications provider, Kyivstar, in December 2023, disrupting the mobile signal and Internet for over 23 million Ukrainians for days. These activities indicate that Russia has the capability to disrupt the critical infrastructure of other countries in a similar fashion. To help mitigate this threat activity from occurring in Canada, CSIS assists in the prevention of hostile state actors from accessing or impacting Canada's critical infrastructure. CSIS continues to work with critical infrastructure providers and organizations to address security concerns.

Secure Innovation: Security advice for emerging technology companies and researchers – Canada.ca

Secure Innovation: Security advice for emerging technology investors – Canada.ca

Counter proliferation

CSIS' counter-proliferation efforts substantially reduce the risk of Canadian technology and research being utilized to advance the military capabilities of adversarial foreign states. In response to CSIS' efforts, adversarial states are applying increasingly complex strategies to mask their illegal procurement activities.

CSIS actively investigates efforts by adversarial foreign states and state-affiliated actors to illicitly procure a range of sensitive technologies, services, research and intellectual property in Canada to advance their own weapons of mass destruction (WMD) programs. The proliferation of chemical, biological, radiological, and nuclear weapons, or WMDs, and their associated delivery vehicles constitutes a global challenge and a threat to the security of Canada and its allies.

CSIS monitors developments in the weapons and WMD programs of adversarial foreign states to support Canada's export controls and sanctions. CSIS' monitoring work also supports Government of Canada efforts to assess and understand the adversary advanced conventional weapon and WMD threat to Canada.

In its attempt to procure foreign technologies for its war effort against Ukraine, the Russian Federation continues to challenge Government of Canada export controls and sanctions. Russia applies a complex strategy to hide its illicit procurement activities by falsifying shipping documents and by rerouting shipments through a vast international network of intermediaries. Russia uses equally complex methods to mask payments for these imports.

Much like Russia, Iran continues its attempt to evade Government of Canada export controls and sanctions. CSIS engages with Canadian companies to prevent Iran's procurement of technologies that are critical for the development of advanced conventional weapons. This collaboration has helped curb Iran's ability to conduct and support destabilizing activities, such as conducting direct attacks against Canada's regional partners, providing weapons to Russia for its war against Ukraine and arming militia groups for attacks against Canadian and partner forces in the Middle East. CSIS also continues to monitor Iran's WMD programs and actively investigates attempted procurement of Canadian technology to further Iran's WMD programs.

CSIS activities also include monitoring the development of emerging and sensitive technologies, and their potential security implications. CSIS actively investigates Canadian exports suspected of contributing to the development of sensitive technologies by adversarial foreign states.

As a leader in key space technologies, such as communications, robotics and radar satellites, Canada is vulnerable to threats from hostile state actors who seek access to these technologies for their own military and economic advantage. In an effort to access sensitive technologies, hostile state actors employ individuals who exhibit the willingness and ability to damage Canadian space interests for the benefit of adversarial foreign states. CSIS is aware of such individuals.

In 2024, CSIS significantly increased the number of security briefings provided to space stakeholders. These briefings raised awareness of the increasing threats to the Canadian space sector and sought to harden the Canadian space sector against espionage and sabotage perpetrated by adversarial foreign states, including Russia and China.

From the 1994 CSIS Public Report

> **As Canada is an internationally recognized leader in many high-technology sectors (such as nuclear, chemical, electronics and aerospace sectors), it has been, and will remain, a lucrative target for clandestine and illicit procurement activity.**

Security screening

Through its Government Security Screening, and Immigration and Citizenship Screening programs, CSIS serves as a line of defence against those who could threaten Canada's national security by obtaining access to Canadian government information, assets and facilities, or by seeking status in Canada via an immigration process. The line between threat actors and civil society continues to blur as the world becomes evermore interconnected, leading to a significant increase in both volume and complexity of the files referred for security screening.

As part of an overall evaluation to assist federal government departments and agencies in deciding to grant, deny or revoke security clearances, the CSIS Government Security Screening (GSS) program provides security assessments to help prevent individuals of concern from gaining access to classified or sensitive information and assets, as well as sensitive sites such as airports, marine and nuclear facilities. The decision to grant, deny or revoke clearances ultimately rests with each department or agency, and not with CSIS. In the face of increasing threats of foreign interference from hostile state actors, GSS has implemented additional measures to highlight and raise awareness of the risk of such threats. These initiatives enable sponsoring departments and agencies to make more informed, risk-based decisions regarding security clearances and site access clearances. In 2024, CSIS received 138,430 requests for GSS.

The Government of Canada's Immigration and Citizenship Security Screening (ICS) program is a trilateral program that relies on close collaboration between Immigration, Refugees and Citizenship Canada (IRCC), the Canada Border Services Agency (CBSA) and CSIS. The program is a critical function of Canada's national security and focuses on the admissibility of foreign nationals and permanent residents as it pertains to national security, human or international rights violations and organized criminality, as outlined in the *Immigration and Refugee Protection Act*. Under this program, IRCC and CBSA can refer applications to CSIS for security screening assessments on persons applying for refugee status in Canada, temporary resident visas, permanent residency, and citizenship applications. As part of the program, CSIS provides security advice to CBSA and IRCC regarding persons who are attempting to obtain entry to or status in Canada, and who may represent a threat to national security. The advice is provided through CBSA to IRCC, which takes CSIS' advice into consideration when making the final decision on the inadmissibility of an applicant. In 2024, CSIS received 538,100 security screening referrals from IRCC and CBSA.

CSIS undertakes the security screening for all asylum claimants (also known as front-end security screening). The volume of in-Canada asylum claimants has rapidly increased over the last five years and continues to grow every year, creating pressures at ports of entry and leading to delays in process and other strains on the asylum system.

In late 2024, the Government of Canada committed to lower immigration targets over the next three years. CSIS recognizes that the immigration levels of the current and past years, coupled with the multiple commitments by the Government of Canada to world events have led to record high immigration applications and security screening referrals received by CSIS. There continues to be high volumes of applications awaiting security screening, however, CSIS and its security screening partners will continue to take the time required to ensure the safety of Canadians and Canada.

In 2024, CSIS continued its participation on IRCC's Digital Platform Modernization (DPM) projects. DPM will allow IRCC, CBSA and CSIS to pivot towards a more robust digital and evidence-driven immigration system that includes updated business processes, policy enhancements, and a new digital technology platform. For CSIS, these modernization efforts will enhance and improve the conduct of security screening and the delivery of security advice to both CBSA and IRCC.

In late 2023, the intense fighting between Israel and Hamas raised the prospect of broader crisis in the Middle East. In response, the Government of Canada implemented measures by way of a public policy to help Canadians and family members get to safety, including through assisted departures via the Rafah border crossing between Gaza and Egypt when it was open. In December 2023, the public policy aimed to provide temporary resident status to 1,000 eligible applicants from Gaza, which was subsequently increased to 5,000 in August 2024. CSIS has been actively engaged in screening foreign nationals with ties to Canada who are escaping the conflict. In light of the security risk presented by a territory that is governed by a listed terrorist entity, CSIS has been closely screening all applicants, which has led to a significant increase in resource demands on screening staff to ensure due diligence. In addition to prioritizing applicants from Gaza, CSIS also proactively prioritized applications from Lebanese nationals in the event that the Hezbollah-Israel conflict in Lebanon expanded and triggered an evacuation of Canadian citizens and other foreigners.

CSIS was involved in the immigration and citizenship screening of father and son Ahmed Eldidi and Mostafa Eldidi, who were arrested in July 2024 and charged with nine offences related to support to terrorist activity on behalf of Daesh. CBSA and IRCC referred the files to CSIS for security screening, and both men were cleared in all cases based on the information CSIS received at the time. In response to the arrest of Ahmed and Mostafa Eldidi, and public questions concerning existing immigration processes, then Public Safety Minister Dominic LeBlanc ordered a review of the Government of Canada's immigration screening process. IRCC, CBSA and CSIS are currently undertaking this review.

In December 2024, Ahmed Eldidi was additionally charged with offences related to crimes against humanity and war crimes for allegedly dismembering a prisoner of Daesh in 2015. ■

Immigration and Citizenship Screening program

Requests received in 2024*

Permanent residents inside and outside Canada	22,500
Refugees (front-end screening**)	151,400
Citizenship	319,700
Temporary residents	44,500
Total:	**538,100**

Government Screening program

Requests received in 2024*

Federal government departments	63,800
Free and Secure Trade (FAST)	7,400
Transport Canada (Marine and Airport)	47,300
Parliamentary Precinct	2,300
Nuclear facilities	14,600
Provinces	70
Others	1,900
Foreign screening***	420
Major events	640
Total:	**138,430**

* Figures have been rounded.

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

*** Security assessments to provincial and foreign governments, as well as to international organizations, when Canadians seek employment that requires access to sensitive information or sites in another country.

The Integrated Threat Assessment Centre

The Integrated Threat Assessment Centre (ITAC) (previously the Integrated Terrorism Assessment Centre) is a specialized organization in the Canadian intelligence community, responsible for providing timely, relevant and objective assessments based on all-source information and intelligence that enable decision-makers and security partners to safeguard Canadians and advance Canadian interests at home and abroad.

ITAC actively monitors intelligence collected by partners and a variety of open sources of information, leading to recommendations to the Director of CSIS on the National Terrorism Threat Level (NTTL) and various products focusing on data, trend analysis and strategic assessments. Although its assessment mandate is distinct, ITAC operates as a component of CSIS and is accountable to the Director of CSIS. ITAC reflects the clients it serves by integrating representatives from traditional and non-traditional partners. Representatives from policing, security intelligence, signals intelligence, border security and other communities come together to provide foresight on converging topics such as terrorism, technology, hostile state activity, climate change and food insecurity.

ITAC has evolved considerably since its inception in 2004, and when its mandate was focused on terrorism starting in 2011. In 2024, ITAC's mandate grew beyond terrorism and violent extremism to include the assessment of all types of national security threats relating to public officials. In response to Government of Canada priorities, ITAC provides strategic assessments to educate federal public officials on the threat of violence, espionage and foreign interference, and to inform protective security postures. With this expansion of its mandate, along with the celebration of its 20th anniversary in 2024, ITAC has reverted to its original name: the Integrated Threat Assessment Centre.

In addition to these developments, in line with recent changes to the CSIS Act, ITAC will also begin to provide unclassified information to a broader spectrum of clients in 2025 to help build resiliency against threats to the security of Canada.

The National Terrorism Threat Level

Over the course of 2024, mitigation measures undertaken by police and security intelligence partners ensured that the NTTL remained at Medium, meaning that a violent extremist attack in the next six months was a realistic possibility.

In 2024, global events, such as the ongoing conflict in the Middle East and the Russia-Ukraine war, contributed to individualized grievance narratives and extremist groups' efforts to influence Western audiences through propaganda. These factors have aggravated the violent extremist landscape and driven threat activities; however, mitigation measures have thus far prevented Canada from experiencing attacks like those seen in other democracies. Over the course of 2024, the most likely terrorism scenario was assessed to be a lone actor motivated by a personalized worldview.

In 2025, this trend is expected to continue, as extremists of various ideologies are galvanized by a broad spectrum of issues and crises amid social polarization and misinformation/disinformation.

In advance of a federal election in 2025, ITAC remains focused on assessing potential national security threats to public officials. While the threat environment for public officials remains dynamic, the vast majority of violent threats ITAC has noted have been unrelated to national security.

2 Modernizing policy, partnerships and transparency

Looking back on forty years

2023

Then Director David Vigneault and fellow Five Eyes counterparts participate in a historic joint public appearance to discuss threats posed to Five Eyes economies by foreign adversaries.

Modernizing the CSIS Act: Enabling CSIS to better protect Canada and all Canadians

As Deputy Director of Policy and Strategic Partnerships, Nicole Giles is responsible for strategic policy development, legislation and strengthening CSIS' relationships and engagement with oversight bodies, foreign partners, and Canadians.

This was an important year for CSIS. Not only did we celebrate 40 years of protecting national security, but our legislation, the CSIS Act, received the most significant updates since its enactment in 1984. We recognised that the Act had aged, and that we needed to better equip CSIS in the face of an increasingly complex threat environment and rapid technological change.

As Deputy Director of Policy and Strategic Partnerships, I had the honour of directing the effort to modernize the CSIS Act. This was truly a team endeavour. Its success is owed to the contributions of individuals from across CSIS, the Government of Canada, and Canada. Many Canadians played a key role by taking the time to provide their diverse perspectives on the proposed modifications to the CSIS Act. A total of 360 Canadians provided written submissions and CSIS met directly with over 200 stakeholders, representing a wide-range of interests—provincial, territorial and Indigenous, business, academic, and ethnic, religious and cultural—from Whitehorse to Halifax, and many cities in between. Throughout the process, Canadians generally noted the need for changes to the CSIS Act, and agreed that existing gaps were problematic. Many indicated that the proposed amendments could better equip CSIS and the government to respond to national security threats such as foreign interference, and their input ultimately informed the amendments proposed by the government to the CSIS Act in Bill C-70, *An Act respecting countering foreign interference*.

On June 19, 2024, Bill C-70 received royal assent, helping fill a number of key gaps in CSIS' authorities. Bill C-70 also provided the government with stronger measures to protect national security through amendments to the

With these amendments, CSIS is better able to equip a broader range of national security stakeholders, operate in a digital era, and respond to changes in the threat environment, while remaining accountable to all Canadians.

Nicole Giles
Deputy Director of Policy and Strategic Partnerships at the Canadian Security Intelligence Service

Security of Information Act, the *Criminal Code*, and the *Canada Evidence Act*, as well as via the establishment of a foreign influence transparency registry.

With these amendments, CSIS is better able to equip a broader range of national security stakeholders, operate in a digital era, and respond to changes in the threat environment, while remaining accountable to all Canadians.

With the amendments to information disclosure, CSIS can now share information with entities or persons outside the Government of Canada to proactively build resiliency to threats. This ability will help build society-wide resilience by increasing our partners' ability to understand and recognize threats, and to protect their people, information, assets, as well as Canada's interests. In 2024, CSIS conducted 28 resiliency briefings since the Act came into force, and we are continuing to deliver resiliency briefings in 2025. We have moved quickly to share threat information with provincial and territorial governments, Indigenous organizations, religious and community groups, and national advocacy organisations like the Business Council of Canada, a network composed of chief executives from Canada's leading enterprises across the private sector.

Our new legislative amendments also provide CSIS with expanded judicial authorizations modeled on authorities routinely relied on by Canadian law enforcement and intelligence services in other democracies. For instance, CSIS now has the ability to request a single-use warrant to conduct a one-off investigative technique, such as examining the content of a USB key that may contain information that advances a national security investigation. The single-use warrant is less intrusive than a traditional warrant as it does not authorize ongoing collection, but like all warrants and orders, it still requires Federal Court approval and remains subject to robust oversight by the Minister and the National Security and Intelligence Review Agency.

The amendments to CSIS' dataset regime increase the efficiency of the collection and use of datasets, and the retention timeline from 90 to 180 days for CSIS to decrypt, translate and evaluate datasets before seeking permission from the Minister of Public Safety to retain them. This is an important change as datasets can vary in size from a few entries to billions of records.

In addition, the amendments to the CSIS Act closed a technical gap to allow CSIS to collect information from within Canada that is located outside Canada, when the information is about the activities of foreign individuals in Canada.

I've said before that whole-of-society threats require whole-of-society responses. The process to modernize the CSIS Act demonstrates how effective a whole-of-society response can be. This is what separates us from our adversaries, and makes us stronger.

Building partnerships through engagement

CSIS' outreach and engagement activities aim to develop relationships with, work alongside, and learn directly from Canadians to build a whole-of-society approach to mitigate national security threats.

Academic outreach

In 2024, CSIS' academic outreach program continued to bridge the worlds of academia and intelligence through roundtable events, workshops, and via the production of commissioned papers. By drawing regularly on experts and taking a multidisciplinary approach, CSIS plays an active role in fostering a clearer understanding of security issues, a process that benefits both CSIS' experts, as well as the researchers and specialists that collaborate with us.

In 2024, CSIS continued to deliver its flagship academic outreach program: the Expert Briefing series, which hosts leading academics and researchers for briefings usually attended by over 500 Government of Canada participants per session. The 2024 series touched on topics including the threat and implications of increased Russia-China coordination, supply chain vulnerabilities in hardware, moral injury and its potential impact on intelligence officers, and the psychology of ideologically motivated violent extremist actors.

In October 2024, CSIS hosted the University of Waterloo's Institute of Quantum Computing (IQC) for a discussion with Government of Canada officials on the state of quantum research and development

in Canada. The meeting was the latest in a series of engagements between CSIS and IQC, including CSIS participation on a panel discussion at Quantum Connections hosted by IQC in May 2024. By encouraging exchanges and collaboration with critical strategic sectors, CSIS is better informed and can leverage the expertise of Canada's rich research sector while increasing resiliency to malicious actors.

In June 2024, CSIS organized a workshop for international partners headquartered at the North Atlantic Treaty Organization (NATO) in Brussels, Belgium. This first-of-its-kind event brought together representatives from all NATO member states to discuss pressing intelligence threats to the alliance, focusing on a solutions-oriented approach to our greatest adversaries. International cooperation and alliances are more important than ever as we face a multi-faceted threat environment. CSIS looks forward to continuing to build on these efforts with NATO and other partners in 2025.

To recognize CSIS' 40th anniversary, CSIS was a key sponsor of a conference organized by the University of New Brunswick entitled "Canadian Intelligence History at the Crossroads: Historical Reflections on the Occasion of CSIS' 40th Anniversary." Offering commentaries on Canadian intelligence history from leading academics, the event sought to explore CSIS' recent past and inspire a new generation of intelligence history scholars. CSIS was pleased to host the conference's second day, where CSIS Deputy Director, Policy and Strategic Partnerships, Nicole Giles offered the keynote address reflecting on the past, present and future of intelligence history, and encouraging the next generation of practitioners to learn from our past so as to shape our future.

Engagement activities

CSIS' stakeholder engagement program continued to expand and deepen relationships with key stakeholders across the community advocacy, academic, and private sectors; and with Indigenous partners across Canada.

CSIS continued to engage various stakeholders in early 2024 as part of the public consultations on Bill C-70: *An Act respecting countering foreign interference*. Insights gleaned from these consultations were incorporated into the legislation, and proved critical to the successful passage of the Bill. Through the modernized authorities resulting from *An Act respecting countering foreign interference*, CSIS has been able to quickly deliver national security resiliency briefings to key partners across all sectors of society, helping protect key national security interests from threats of espionage, foreign interference, and extremist violence.

In July 2024, CSIS was invited to present at the 42nd Annual Meeting of the Federal-Provincial-Territorial Ministers Responsible for the Status of Women to provide information about the threats from incel and gender-based violent extremism, as well as an overview of CSIS' various activities with government and civil society partners to combat such threats. CSIS also provided expert advice to Government of Canada funding advisory boards working with civil society and community organizations to counter violent extremism.

CSIS has been working with Canadian businesses and business associations, including the Business Council of Canada (BCC) as well as the Canadian Chamber of Commerce, to enhance communication between the public and private sectors, as well as to build resiliency and minimize security threats. This past year, CSIS travelled to London to meet with MI5's National Protective Security Authority and to Washington to meet with the FBI's Domestic Security Alliance Council, as well as the Cybersecurity and Infrastructure Security Agency, in partnership with private industry leaders with the BCC. These joint engagements provided opportunities to learn best practices on sharing information between the public and private sectors, as security agencies work with private industry to mitigate against threats, especially where critical infrastructure is concerned. CSIS has already had robust and regular engagements with businesses and business associations

"The Business Council of Canada is proud of the strategic partnership it has forged with CSIS to enhance the Canadian private sector's awareness of, and resiliency against, malicious threat activity targeting Canadian businesses in every sector and region of our country. Through increased information sharing and collaboration, Canadian businesses have been able to better protect their employees, customers, and the communities in which they operate."

Goldy Hyder
President and Chief Executive Officer,
Business Council of Canada

"As Canadians, we are concerned about foreign government interference that undermines our democratic processes and intimidates our citizens. At the same time, as Asian Canadians marginalized by systemic anti-Asian racism, we must ensure that security-related laws and policies do not become tools of oppression that target and deny the rights of Asian and racialized communities. We support CSIS' focus on combating racially-motivated hate and threats, and urge CSIS to continue building trust with Asian Canadian communities through meaningful engagement to protect Canada's democracy and values of inclusion and equity."

Amy Go
President, Chinese Canadian
National Council for Social Justice

"Collaboration with external partners is vital for national security. Civil society and the private sector face direct threats and also hold key pieces of the security puzzle. The workshops, briefings, and outreach by CSIS' Academic Outreach and Stakeholder Engagement are critically important in furthering Canada's national security."

Maria Robson-Morrow
Intelligence Project,
Belfer Center for Science and International Affairs at the Harvard Kennedy School

"It remains crucial for CSIS to continue in its positive efforts to repair trust and build meaningful relationships with Canadian Muslim communities."

Amira Elghawaby
Canada's Special Representative
on Combatting Islamophobia

"When we began planning a conference on Canadian intelligence history in 2022 we were unsure what support, if any, we would get from the government. Over the next two years, however, CSIS proved to be our strongest advocate. The success of the conference reinforced my firm belief that intelligence history is at its strongest when historians and practitioners work together to both share and compare our understandings of the past."

Sarah-Jane Corke
Associate Professor, University of New Brunswick

to deliver threat briefings to support informed decision-making, including to the Canadian Chamber of Commerce and to the BCC's National Security Working Group and National Security Executive Network.

Indigenous, Arctic and Northern engagement

In 2024, CSIS continued engagements with Arctic and Northern partners, including governments, communities, Indigenous groups, local leadership, and research institutes. This engagement work in the region is focused on ensuring partners have relevant information to build and maintain resiliency against current and emerging threats. Throughout the year, CSIS officials traveled to Nunavut, the Northwest Territories, the Yukon, and Nunavik (Northern Quebec), in addition to hosting senior officials and leadership from key Northern and Indigenous partner organizations at our headquarters. These various activities have considerably advanced CSIS objectives to build meaningful partnerships in the Arctic and North that help inform CSIS' understanding of the region's dynamics and to contribute to a safer, and more secure and prosperous environment for its residents and all Canadians.

In addition to continuing to develop relationships with First Nations, Inuit, and Métis organizations and governments, CSIS continued to work with Indigenous partners in 2024 to implement the *United Nations Declaration on the Rights of Indigenous Peoples Act*, the Government of Canada's legislation to implement the United Nations Declaration on the Rights of Indigenous Peoples (UN Declaration). CSIS is the only intelligence service in the world to have made UN Declaration commitments. In June 2024, CSIS released a publication detailing our UN Declaration Act commitments and providing highlights of their implementation at CSIS.

In early 2024, as part of our UN Declaration Act Action Plan commitments, CSIS worked with the Métis Nation British Columbia to develop a training video on Métis history, culture, and perspectives, to assist in cultural competency training for CSIS officers.

In June 2024, CSIS took over as Chair of the Five Eyes Indigenous Network, a position CSIS will hold until June 2025. The Network was created to consider Indigenous perspectives and security intelligence outcomes affecting Indigenous Peoples across Five Eyes countries. CSIS looks forward to continuing to work with Indigenous and international partners through this initiative into 2025. ■

Image source:
Shaun Vincent, artist;
Department of Justice

Policy and accountability

Protecting national security and Canada's interests requires CSIS to be a policy-driven organization that is accountable to Canadians and Parliament.

Lawful Access Advisory Committee

For law enforcement and national security agencies in Canada, lawful access is essential in the prevention, investigation, and prosecution of serious offences, and in the investigation of threats to the security of Canada. Lawful access entails the collection of data, such as documentation, computer data, and other information from telecommunications companies to investigate suspected threats to Canada's national security in a legal and ethical manner that protects the rights and freedoms of Canadians. However, no centralized program exists in Canada that fully addresses lawful access requirements and initiatives responsible for coordinating, developing, implementing, or maintaining lawful access systems. The rapid evolution of technology has also increased the complexity and inefficiencies that impact the ability of law enforcement and national security agencies to keep investigative capability up to date.

As part of the RCMP' and CSIS' ongoing effort to address lawful access challenges, the Lawful Access Advisory Committee (LAAC) was created in 2023. LAAC is an advisory body composed of senior level lawful access representatives from Canadian telecommunications companies, all levels of law enforcement, CSIS and other federal departments. LAAC provides a collaborative forum for members from both government and private industry to identify and openly discuss challenges pertaining to lawful access, and develop potential solutions to address challenges in a way that ensures full and fair representation for all stakeholders.

External review and oversight

CSIS is dedicated to upholding the highest standards of transparency and accountability, ensuring that its operations comply with Canadian law, including the CSIS Act and the *Canadian Charter of Rights and Freedoms*, adhere to direction from the Minister and the courts, and align with Government of Canada policies.

External review by the National Security and Intelligence Committee of Parliamentarians (NSICOP) and the National Security and Intelligence Review Agency (NSIRA) provides CSIS with findings and recommendations that offer opportunities for improvement. CSIS carefully considers each recommendation, and when in agreement, takes action to implement change when feasible. Independent external review also fosters a culture of compliance, transparency, and continuous improvement at CSIS while keeping Canadians informed of key national security issues. To this end, CSIS has been responding publically to review body recommendations since 2022.

CSIS devotes significant attention to the review process. In 2024, there were a total of 28 national security reviews involving CSIS by NSICOP and NSIRA. Of these reviews, 18 are ongoing. CSIS received 86 requests for information and briefings from review bodies. CSIS actively engages in fact checking and the redaction of reviews for public release to ensure balance between public interest, national security and the protection of classified information, such as human source information. CSIS welcomes external review as an investment in ensuring CSIS remains accountable in fulfilling its requirements as Canada's security intelligence service.

Since 2018, CSIS has received 136 non-binding recommendations from review bodies. Of these, CSIS has accepted 106 and partially accepted 19. In the past year, CSIS received 8 final NSIRA reports. CSIS responds publicly to all recommendations it reviews. For example, on NSIRA's review of the dataset regime, CSIS agreed with most recommendations even as CSIS had a different perspective on several key issues. The implementation of recommendations is an important way to ensure CSIS remains compliant with the law and is continuously improving, leading to better national security outcomes for Canadians. Even where CSIS disagrees, the publication of responses to review body recommendations supports transparency and can enrich the national security conversation in Canada.

Under the NSIRA Act, anyone can submit a complaint to NSIRA about a CSIS activity or the denial of a security clearance. There has been a 200% increase in complaints in 2024 compared to 2023. Of the complaints received in 2024, 77% are allegations of delays related to the processing timelines of CSIS' security screening of immigration applications. While there are high volumes of applications awaiting security screening, CSIS continues to take the time required to carefully screen applications to ensure the safety of Canadians and Canada. Application processing is not expedited in response to complaints. CSIS takes NSIRA's findings and recommendations on complaints seriously and implements changes quickly when necessary. Of the four complaint investigations concluded in 2024, NSIRA found all allegations against CSIS to be unsupported.

The Intelligence Commissioner (IC) provides an important additional layer of oversight and accountability for CSIS. The IC reviews decisions of the Minister of Public Safety on classes of datasets, and approves the retention of a foreign dataset under Section 11.17 of the CSIS Act. The IC also approves the categories of acts and omissions that designated CSIS employees can commit while in the function of their duties that would otherwise constitute offences. With the goal of further

increasing transparency, the office of the IC and CSIS work together in a way that protects against national security injury to publish IC decisions on its website. In 2024, the IC rendered six decisions involving CSIS.

For CSIS, protecting privacy and personal information is foundational. CSIS limits the collection, use, retention and disclosure of personal information to what is necessary and proportional to meet our mandate. CSIS collaborates closely with government agencies to develop and refine privacy standards that meet the evolving needs and expectations of Canadians. CSIS engages with the Office of the Privacy Commissioner and the Treasury Board Secretariat to identify and implement best practices in privacy protection, ensuring CSIS programs are aligned with the principles of the *Privacy Act*. In the past calendar year, CSIS has completed its review of 12 privacy breaches (6 founded but non-material, 2 unfounded, 4 underway); 32 privacy breaches related to non-compliance (12 founded but non-material, 3 unfounded and 17 in progress), conducted 28 privacy needs assessments (16 completed, 12 currently underway) and is currently drafting 13 new privacy impact assessments.

Operational policy

CSIS continues to focus on modernizing its policies and procedures to reflect the requirements of a modern intelligence service. A series of new operational policy documents have been published over the past year, with an emphasis on improved operational decision-making, managing investigative activities, and enhancing disclosure of information and intelligence. Responding to the Ministerial Direction on Threats to the Security of Canada directed at Parliament and Parliamentarians, issued to CSIS in 2023 also required updated guidance and improved interdepartmental coordination.

Prior to *An Act respecting countering foreign interference* receiving royal assent, CSIS began developing a rigorous and carefully considered plan to implement new and expanded authorities under the CSIS Act in a way that prioritizes the safety, security, and privacy of Canadians, including through the articulation of functional guidance. CSIS is also developing new and updated guidance for employees to support its ability to operate lawfully in a modern data-dominated threat landscape, while respecting the Charter, *Privacy Act* and Canadians' privacy. CSIS is taking a careful and deliberate approach to ensure the effective and compliant implementation of these new authorities. Throughout this process, CSIS will remain fully transparent and accountable to the Minister, the Federal Court, as well as oversight and review bodies.

CSIS is also implementing new judicial authorizations authorities in cooperation with Public Safety and the Federal Court. This includes validating and revising existing multi-step warrant processes as needed, along with accompanying internal approvals and prioritizations, as well as collaborative review with Public Safety and legal counsel, before seeking the Minister's approval and submission to the Court. In implementing these authorities, CSIS will ensure that the rigorous processes through which Canadians' privacy and rights are safeguarded remain central.

Justification Framework

The Justification Framework provides legal authority for CSIS employees who are designated by the Minister of Public Safety and persons acting under their direction, such as human sources, to engage in activities that would otherwise constitute offences. This means that when a CSIS employee, or human source acting at their direction, engages in activities with a suspected terrorist in the hope of gaining their confidence, they are protected from criminal liability. For example, the very act of providing direction to a human source operating covertly within a suspected terrorist entity could potentially engage terrorism offences in the *Criminal Code*. Another example is providing electronic items, such as a cell phone, to enable the human source's access to vital information or to contact CSIS.

As a first layer of accountability, the Framework requires the Minister of Public Safety to determine, at least once a year, the classes of acts or omissions that designated CSIS employees may be justified in committing or directing another person to commit, and this determination is only valid after it is reviewed and approved by the Intelligence Commissioner. As a second layer of accountability, and as an added layer of transparency, Section 20.1(24) of the Justification Framework also requires the Minister to publicly release certain information. The following table provides the information required to fulfill Section 20.1(24), by fiscal year:

Justification Framework table	2021–2022	2022–2023	2023–2024
Number of emergency designations under s. 20.1(8)	0	0	0
Number of authorizations to direct the commission of acts or omissions under s. 20.1(12)	172	173	178
Number of directions under s. 20.1(15)(b)	0	0	0

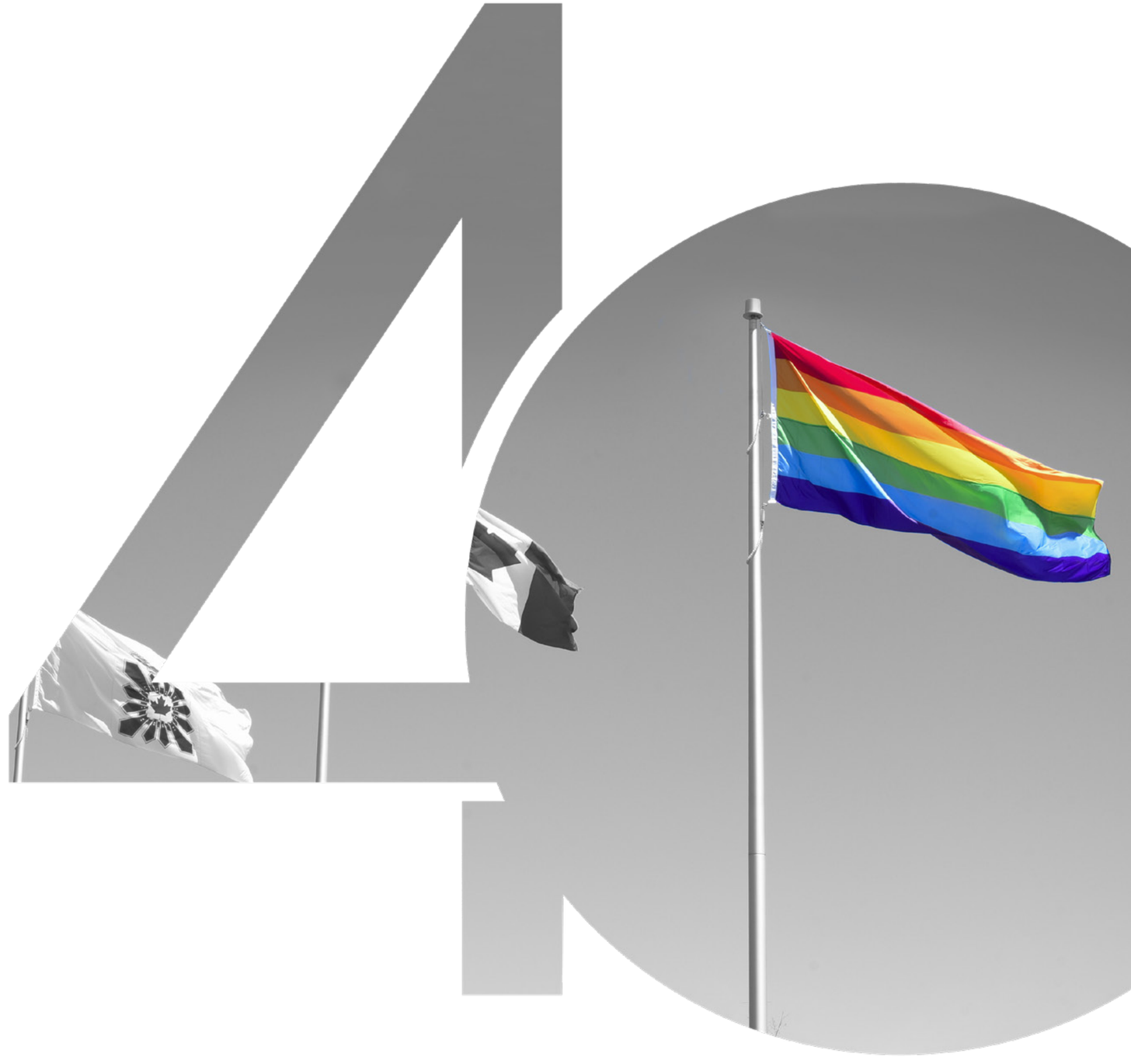
Since the coming into force of the Justification Framework, the authorizations granted were in support of information and intelligence collection activities relating to espionage/sabotage, foreign interference, and terrorism as defined in paragraphs (a), (b), and (c) of the definition of threats to the security of Canada in Section 2 of the CSIS Act. During the same time, the majority of the acts or omissions that were directed to be committed under those authorizations were related to terrorism as defined in paragraph (c) of the definition of threats to the security of Canada in Section 2 of the CSIS Act, and as such could constitute terrorism-related offences under the *Criminal Code*. ■

3 Workforce and culture

Looking back on forty years

2018

The Pride flag is raised for the first time at CSIS National Headquarters.



The "One Mission, One CSIS" transformation journey

As Deputy Director of Administration, Jerome Laliberté is responsible for leading critical functions within CSIS' internal security program, corporate services, finance, strategic planning, and organizational transformation.

While we have spent this 40th anniversary year reflecting on our past, we have also kept an eye on our future. The One Mission, One CSIS strategy launched in 2022 marked a transformative step forward for CSIS. Designed to address an increasingly complex and rapidly-changing world, this strategy ensures that we remain agile, innovative, and effective in protecting Canada's security and prosperity.

Understanding that transformation is a continuous process is central to the strategy. By emphasizing adaptability, bold thinking, and calculated risk-taking, our way forward has clear direction as we navigate an evolving world.

The One Mission, One CSIS strategy is anchored in three foundational pillars: people first, mission focus, and digital and data-driven intelligence.

Firstly, our people are our greatest strength. Prioritizing diversity in all forms ensures a workforce reflective of Canada, which is crucial for delivering on our mission. Expanding professional development opportunities through learning paths, job shadowing, mentoring, and coaching programs empowers employees to grow their skills and take on leadership roles at all levels, and it fosters a culture of accountability, collaboration and innovation at CSIS.

Strengthening this pillar remains a priority as we create a culture where collaboration and recognition are central to how we work.

Secondly, a renewed focus on mission excellence is helping us adapt to evolving threats and opportunities. Streamlined intelligence operations make us more agile in addressing security challenges. We have focused on integrating expertise and fostering collaboration across disciplines for faster, more responsive decision-making. These efforts will position CSIS to address both traditional and emerging security challenges with greater precision and speed.

While we continue to make these changes internally, our threat environment continues to evolve around us. As such, we will continue to develop and employ foresight strategies to look at emerging risks and trends as well as strengthen partnerships in Canada and abroad in order to safeguard Canada's security.

Finally, digital and data-driven intelligence is critical in today's world. Advanced analytics and artificial intelligence will help us identify threat-related patterns and operate more efficiently.

Through additional funding announced this past year, CSIS can further invest in cutting-edge tools that enhance our ability to collect, process, and analyze data with precision. We are equipping our workforce with the tools and training to tackle emerging challenges with resilience and innovation. These investments support timely, actionable intelligence for decision-makers, and enhance our ability to protect Canadians.

While progress is clear, the journey is ongoing. Transformation is not an endpoint but a process of growth, learning, and adaptation. Moving forward, we remain committed to uniting as one team, strengthening our culture, and embracing bold innovation.

The work to date on our One Mission, One CSIS transformation has laid a strong foundation for our future. Together, we will build on this progress by continually renewing our strategies and evaluating outcomes in order to navigate the complexities of an ever-changing world. By staying true to our mission and values, we will ensure a safer, more secure, and prosperous Canada for generations to come.

While progress is clear, the journey is ongoing. Transformation is not an endpoint but a process of growth, learning, and adaptation. Moving forward, we remain committed to uniting as one team, strengthening our culture, and embracing bold innovation.

Jerome Laliberté
Deputy Director of Administration at the Canadian Security Intelligence Service

Initiatives and updates

CSIS continues to consolidate efforts and make important strides in becoming the inclusive and people-focused organization that our diverse employees expect and deserve.

Diversity, Equity and Inclusion Strategy

In 2024, CSIS advanced implementation of its Diversity, Equity, and Inclusion (DEI) Strategy and three-year action plan. Overall, 96% of the 45 commitments adopted have progressed, and 38% are completed. Implementation of the strategy and action plan depends on multiple stakeholders from across the organization, and progress is shared with employees, as well as posted to the CSIS website. Active and engaged CSIS Diversity Committee members continue to provide important guidance and recommendations to management, which contributes to employee-led changes at CSIS.

In support of creating an inclusive workplace free of bias and systemic barriers, CSIS undertook an in-depth review of hiring, recruiting, and promotion processes and policies using gender-based analysis plus (GBA Plus). Recommendations stemming from this review are under discussion with stakeholders to update tools and policies and ensure systemic bias is avoided, and inclusive language and principles are meaningfully integrated throughout the talent acquisition and career progression processes. This work will continue into 2025. Other measures implemented include the establishment of a dedicated lactation room, and the expansion of multi-faith prayer rooms to accommodate greater participation during religious holidays. The organization also expanded mandatory DEI training requirements for all employees, including a learning path specifically tailored to CSIS executives.

CSIS 2023–2025 Accessibility Plan

Throughout 2024, CSIS has continued efforts to become increasingly accessible and barrier-free. With the support and guidance of our Accessibility Committee stakeholders and diverse employees with disabilities, the organization has progressed 95 of the 102 commitments (42 of which are completed) in its 2023–2025 Accessibility Plan.

Notable advances include a streamlined process for requesting ergonomic equipment; publishing products using file types that allow users to make the product most accessible to them (such as font changes); and learning opportunities for HR and other employees to increase understanding of accessibility requirements. Mandatory learning paths that include accessibility, unconscious bias, barriers, and overall inclusion have been approved for all employees, including executives.

Employee Retention and Attraction plan

In early 2024, CSIS launched the Employee Retention and Attraction (ERA) plan with the goal of enhancing employee satisfaction, reducing turnover, and fostering a culture where everyone feels valued, safe and motivated. To achieve this, CSIS focused primarily on three areas: leadership, career growth and development, and culture. It invested in a leadership development program, including 360° leadership assessments for executives, to equip them with the skills, knowledge and mindset to lead teams and transformation effectively. CSIS emphasized leadership accountabilities for people management in our talent and performance management program and made sure employees at all levels were aware of their roles and responsibilities, and had tools to do their part in supporting a thriving workplace.

In 2024, CSIS' Chief Culture Officer (CCO) focused on promoting and supporting an environment of engagement, openness and inclusivity. The CCO communicated widely to increase reflection and conversations across the organization about desired behaviours. To strengthen and nurture organization values, beliefs and practices, CSIS' Values and Ethics team evaluated the organization's values and ethics training program, identifying needed enhancements. This work, including developing targeted case studies, continues into 2025.

The retention rate has improved, returning to pre-pandemic levels. As of December 2024 (Q3), annual attrition was at 3.3%, lower than it has been at Q3 since 2018. The ERA plan is being updated for 2025 with new measures to further foster a more supportive and engaging workplace that attracts and retains top talent.

CSIS Ombuds Office

In early December 2023, the former Director of CSIS, David Vigneault, announced the creation of an independent CSIS ombuds office. The purpose of the Ombuds Office is to better support all CSIS employees, augment existing mechanisms, and help build a strong culture of trust and respect with CSIS employees at all levels. The creation of the Office also responds to an earlier recommendation from the Clerk of the Privy Council for all departments to establish an ombuds-type function to provide employees with a trusted space to discuss harassment without fear of reprisal, and to help navigate existing systems.

The Ombuds will report directly to the Director of CSIS, and the Office will be independent and separate from all other CSIS business lines and reporting structures. The Ombuds Office will adhere to the four key principles of all ombuds: informality, independence, impartiality and confidentiality. They will analyse trends and patterns to identify systemic issues and provide an overview and recommendations to the organization, as well as an annual public report summarizing issues based on anonymous aggregate data.

The CSIS Ombuds Office will also include the delivery and monitoring of internal conflict management services, and will undertake employee exit interviews.

CSIS' commitment to this initiative is steadfast, and various key aspects of the project have been completed to date. The establishment of the ombuds office was led by the CSIS Deputy Director of Policy and Strategic Partnerships to ensure separation between the office and CSIS' human resources functions. The recruitment process itself was led by an independent recruitment firm.

Wrongdoing Report

At the end of 2023, the former CSIS Director announced that CSIS would produce an annual report addressing misconduct and wrongdoing to ensure transparency, to hold the organization to account, and to clearly demonstrate that inappropriate behaviours are being and will continue to be addressed. The first *Addressing misconduct and wrongdoing at CSIS* report will be published in 2025, and will provide complete statistics for both 2023 and 2024.

For 2024, we have seen an increase in reporting from employees, which is indicative of the willingness of employees to use the internal mechanisms available to them. In 2024, there were 50 new cases related to breach of conduct and 33 new occurrences related to harassment and violence, representing a total increase of 63% over 2023. A total of 34 cases were closed in 2024, with 33 deemed founded. (Note: some cases that were closed were carried over from 2023.) In these cases, the appropriate disciplinary or administrative measures were taken, ranging from verbal warnings to dismissal.

Advancing values and ethics

In 2023, a renewed conversation around values and ethics in the public service began, led by John Hannaford, Clerk of the Privy Council. During the pandemic, the public sector faced a level of complexity not previously experienced by public servants. The public service also onboarded thousands of public servants during this time. With the last update to the Public Service Code of Conduct dating back to 2012, and to ensure a consistent application of values and ethics in discussions, actions and behaviours of public servants, further efforts were made by a team of senior officials to reinvigorate the conversation and ensure that all public servants understand the fundamental role they play in serving Canadians and upholding public trust.

CSIS has its own complimentary Code of Conduct that constitutes the basis for its employees' actions and behaviours in the workplace. We are proud to say that the CSIS Code of Conduct features prominently in the recruitment and onboarding process for new employees, and active employees are required to sign an annual affirmation reiterating their commitment to the Code of Conduct. Furthermore, CSIS' "Stop, Reflect, Inquire" method and annual attestation were featured in PCO's report *Continuing Our Dialogue, Positioning for the Future* as best practices. Then interim Director, Vanessa Lloyd, spoke about these best practices and their contribution to decision-making at CSIS in October 2024 at the Government of Canada's Values and Ethics Symposium.

CSIS representation on the Human Resources Council

In 2024, the Government of Canada Human Resources Council (HRC) selected CSIS Chief Human Resources Officer Renée de Bellefeuille to become Chair. As Chair, she provides leadership across many of the HRC's engagements and partnerships, and ensures the Council fulfills its mandate to support and empower the HR community across the federal public service, including heads of Human Resources and therefore their deputy heads in fulfilling their responsibilities in human resources management.

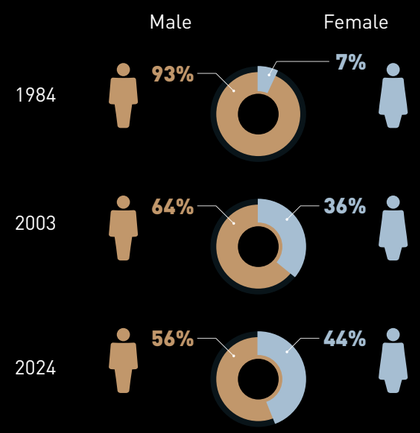
Employee networks

CSIS places great value on its employee-led networks, which serve to unite employees and amplify their unique perspectives across the organization. Employee networks are very active and include the Black Women's Network; the Black, Indigenous and Persons of Colour (BIPOC) Network; the CSIS Women's Network; the Pride Network; the Women in IT Plus (WiT+) Network; the Indigenous Network; the Jewish Network; the Latin American Network, and the Young Professionals Network. Networks are a crucial platform for collaboration, and there are many inspiring examples of network-led community building initiatives designed to educate and immerse employees in common experiences. CSIS strongly endorses the networks' collective dedication to creating an inclusive environment where everyone feels valued, respected, and empowered to share and celebrate their diversity in an increasingly vibrant and dynamic workplace.

Employee demographics

	Representation (2023)	Representation (2024)	Objective by March 31, 2027
Persons with disabilities	**7.1%**	**7.5%**	**9%**
Indigenous Peoples	**2%**	**2.3%**	**3.4%**
Racialized groups	**20.7%**	**21.3%**	**24.9%**
Women in science and technology	**18.8%**	**18.6%**	**24.9%**

Intelligence officer demographics



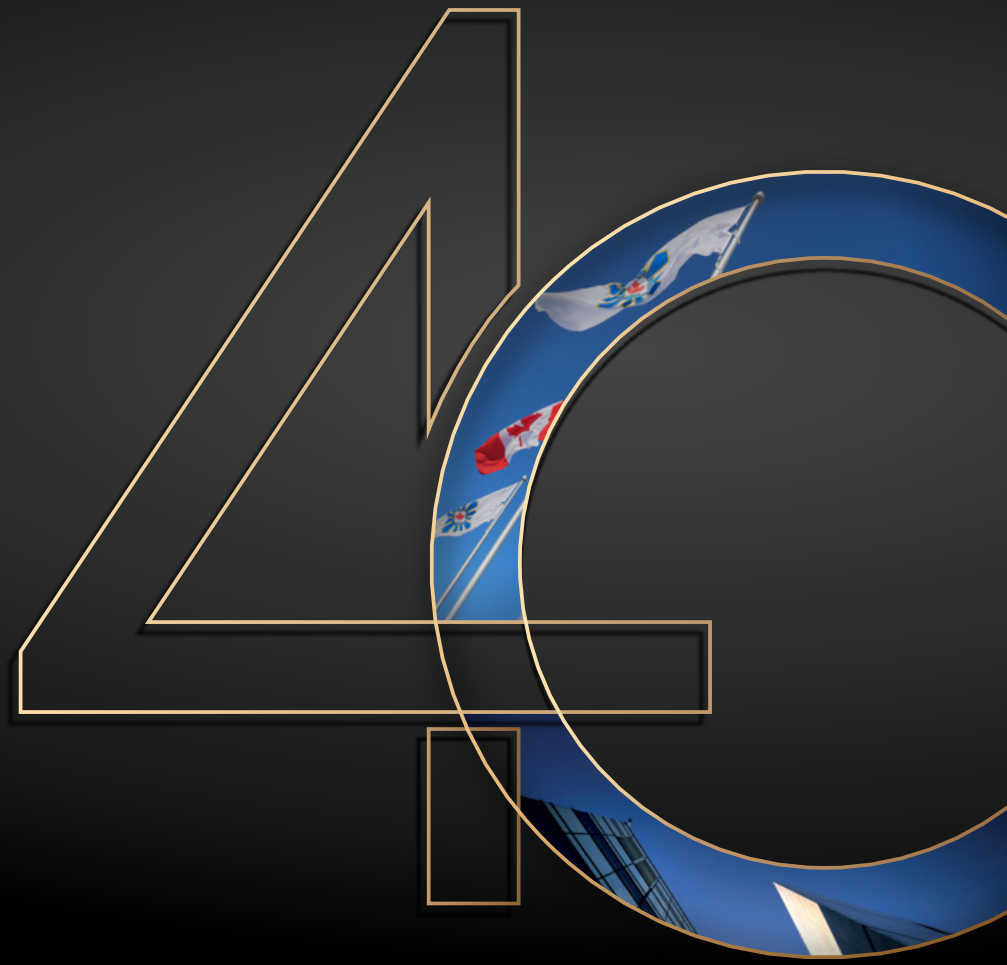
Expenditures

	2021–2022	2022–2023	2023–2024
Salaries	**$404,107,049**	**$415,818,326**	**$557,907,209**
Operating	**$238,065,778**	**$256,628,550**	**$270,508,389**

*Salary costs include employee benefits payments.

Forty years

of national security



For more information contact us at:

PO Box 9732 STN T

Ottawa ON K1G 4G4

Canada

Telephone: 613-993-9620

TTY and or TDD: 613-991-9228

To access the web links,
consult the CSIS Public Report online at
https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-public-report-2024.html